Benämning	*Rapport*	Ansvarig	*Beatrice Fossmo*	Skapat	*2016-09-29 12:52*
Projekt				Senast sparat	*2016-10-26 09:18*
Revision	*2*	Filnamn	*Slutrapport_0.2*		

SLUTRAPPORT

VLL - FÖRSTUDIE INFORMATIONSSÄKERHET

Delges Margit Håkansson, Staben för verksamhetsutveckling
Josefin Leijon, landstingsjurist och personuppgiftsombud

Sammanfattning

Informationssäkerhetens mål inom VLL är att informationshanteringen ska bidra bland annat till patientsäkerhet och patientintegritet, men också att alla verksamheter inom VLL ska kunna lita på att informationen finns där när de behöver den, att de kan lita på att informationen är korrekt och att bara den som behöver den tar del av informationen. Oavsett om informationen på något sätt härrör patient eller ej. Informationssäkerhetsarbetet måste utgå ifrån **ett riskhanteringsperspektiv**.

Den samlade bilden av informationssäkerhetsarbetet och säkerhetsläget i VLL är att **det pågår aktiviteter** på olika håll i organisationen, starkast på kris- och katastrof samt IT säkerhetsområdet, men **utan koppling till en sammanhållen strategisk informationssäkerhet**.

Detta kommer av att det **saknas en ledare för informationssäkerhetsarbetet**. Arbetsuppgiften är inte tilldelad någon specifik medarbetare, följaktligen ramlar frågan "mellan stolarna" och VLL får ingen styrning i frågan.

Idag genomförs riskanalyser av olika slag inom VLL, ur patientsäkerhetsperspektivet, ur beredskapsperspektivet, ur IT-säkerhetsperspektivet; men någon **riskhantering inom informationssäkerhetsområdet förekommer inte.**

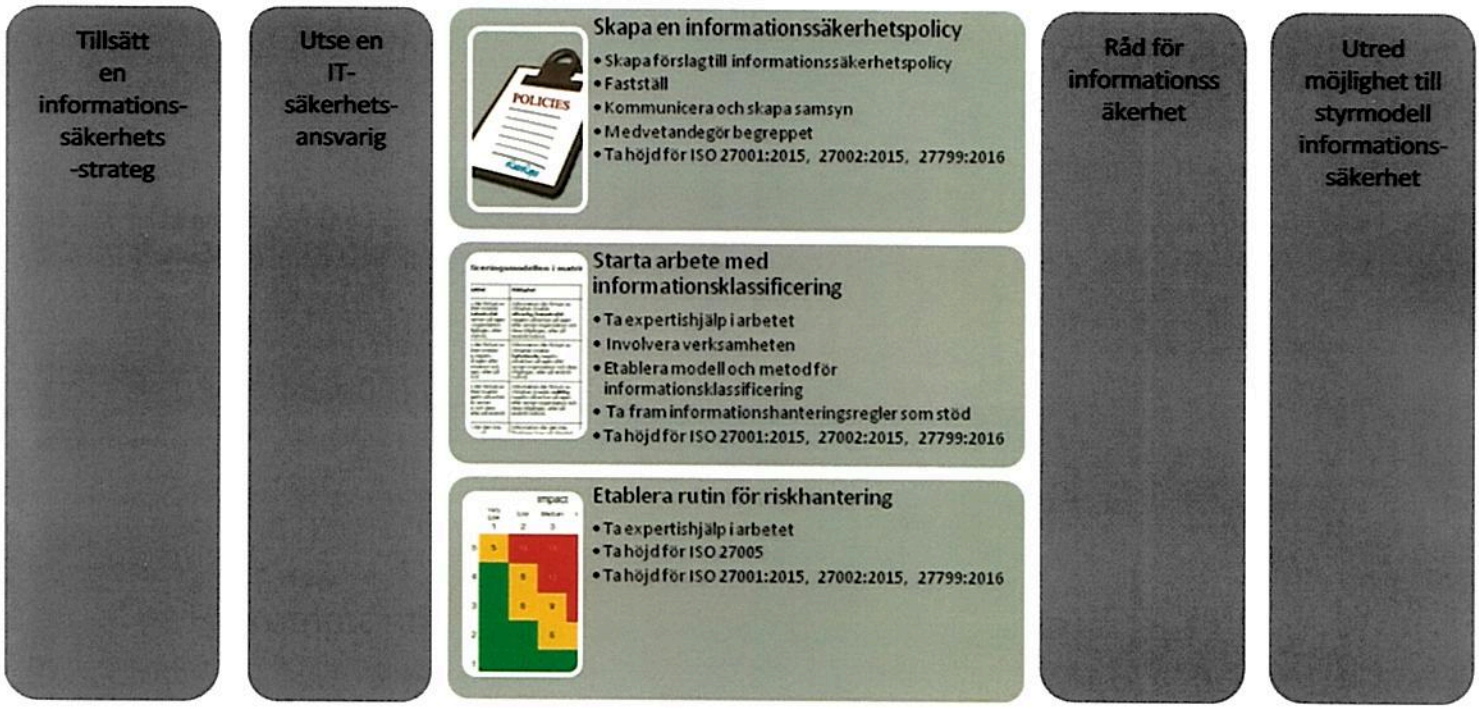
Det finns idag **ingen informationsklassificeringsmetod eller -modell** inom VLL.
Det innebär att det finns risk för att VLL dels inte lever upp till legala eller intressenters krav, men även att information inom VLL kan komma obehöriga till del, kan bli förvanskad och inte kommas åt när den behövs för att utföra en arbetsuppgift.
Klassificeringen ligger ju till grund för vilka skyddsåtgärder som ska utformas och vilka rutiner som ska gälla, dvs hur informationen får hanteras, lagras, distribueras och avvecklas.

Ett lyckat informationssäkerhetsarbete **måste alltid ses utifrån en verksamhetsnytta** och bidra till att landstinget bland andra krav uppfyller kravet på **patientsäkerhet och patientintegritet**. Därför måste informationssäkerhetsarbetet bedrivas i **nära samverkan med verksamheten**.

Förstudien som denna rapport redovisar, visar tydliga tecken på att **det måste genomföras åtgärder** inom organisation för informationssäkerhet, inom ramverk, riskhantering, informationsklassificering och styrning av åtgärder.

Atea Sverige AB
Gräddvägen 7
906 20 Umeå
Tel: 090-71 28 00
Fax: 090-71 28 01
Org nr: 556448-0282
www.atea.se

Rekommendationer & förslag till handlingsplan



Följande rekommendationer ges till VLL för att informationssäkerhetsarbetet ska kunna etableras och upprätthållas.

- **Anta en separat informationssäkerhetspolicy** som noggrant beskriver begreppet informationssäkerhet, målen med arbetet samt hur ansvarsfördelningen inom VLL ser ut. Kommunicera informationssäkerhetspolicyn.
  - **Medvetandegör begreppet** informationssäkerhet inom VLL, använd inte begreppet Säkerhet som ett samlingsnamn – det förvirrar.
  - Ta höjd för **ISO 27001, 27002, 27005 samt 27799**

- Starta arbetet med att ta fram **en metod och modell för informationsklassificering** för att identifiera och värdera informationen inom VLL.
  - Förslagsvis börjar VLL med de **verksamhetskritiska processerna** och informationstillgångarna inom dessa. Absolut avgörande är att involvera verksamheten i detta arbete.
  - Ta höjd för **ISO 27001, 27002, 27005 samt 27799**

- Etablera **en process för riskhantering inom informationssäkerhetsområdet**.
  - Resultatet från en riskanalys måste vara **kopplat till en handlingsplan** med utpekade ansvariga. Denna handlingsplan måste regelbundet följas upp.
  - Utifrån denna process kommer **rapporter till landstingsledningen**
  - Ta höjd för **ISO 27001, 27002, 27005 samt 27799**

- Implementera ISO/IEC 27799:2016 Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO 27002

- VLLs **Råd för säkerhet och beredskap bör förändras**. Rådet ska vara beredande i alla frågor om informationssäkerhet och ha mandat att fatta beslut i vissa. För att markera detta bör benämningen förslagsvis ändras till **Rådet för informationssäkerhet**.
  Ordförandeskapet i rådet bör innehas av den som driver informationssäkerhetsfrågan. I rådet bör områden som IT, IT-säkerhet, fysisk säkerhet, patientsäkerhet, beredskap, juridik och informationssäkerhet finnas representerade.

- **Etablera en styrmodell för informationssäkerhetsarbetet**, styrmodellen bör integreras i den allmänna verksamhetsstyrningsmodellen.

- **Tillsätt en informationssäkerhetsstrateg** med ansvar att driva VLLs informationssäkerhetsarbete. Informationssäkerhetsarbetet bör drivas från en stabsfunktion. Detta är en process som redan nu bör förberedas, och kan löpa parallellt med de övriga aktiviteter som rekommenderas i denna förstudie.
  - Se till att det finns **en sammanställning** som beskriver vad informationssäkerhetsstrategens roll och ansvar innebär.

- **Utse en IT-säkerhetsansvarig** med mandat att ta formella operativa IT-säkerhetsbeslut. Detta är en process som redan nu bör förberedas, och kan löpa parallellt med de övriga aktiviteter som rekommenderas i denna förstudie.

- Analysera inom vilken del av organisationen som ett sk dataskyddsombud, **data protection officer, DPO**, ska tillsättas med anledning av dataskyddsreformen. Förordningen, som kommer att träda i kraft i maj 2018, anger att denna behöver ha kunskaper om lagstiftningen och praxis kring dataskydd. DPO behöver kunna rapportera direkt till ledningen för VLL.
  Min rekommendation är för VLL att utse någon som utreder denna fråga och ger förslag på hur VLL organisatoriskt kommer att lösa kravet på ett dataskyddsombud.
- I god tid före dataskyddsförordningen träder i kraft (maj 2018) bör VLL **informera hela organisationen om vad dataskyddsförordningen innebär**, och vilka rutiner och processer VLL har för att ta hand om VLLs ansvar i frågan och de registrerades rättigheter enligt förordningen. Informera också organisationen **vem som är utsedd** till data protection officer och **kontaktuppgifter till denna**.

- Ur informationssäkerhetsperspektivet och regionbildningsfrågan är min bedömning att informationssäkerhetsområdet kommer att få allt mer betydelse, då en samverkan kring funktioner och tjänster kommer att realiseras. Information kommer att få en vidare spridning. Det kommer sannolikt vara mycket som kan samordnas inom regionen, såsom modeller, processer, metoder. EN informationssäkerhetsstrateg som leder hela regionen. Det är dock rimligt att tro att varje
  del av regionen, nuvarande län, **kommer att behöva en lokal informationssäkerhetsstrateg för att hålla samman informationssäkerhetsarbetet lokalt**.

Innehåll

Bakgrund, syfte och metod

Den starka utvecklingen på IT-området skapar nya möjligheter för sjukvården och för medborgarna, till exempel vad gäller patienters delaktighet och tillgång till sina journaluppgifter. Samtidigt högaktualiseras frågor kring informationssäkerhet och integritet.

Inom Västerbottens läns landsting, VLL, används mängder med information som måste skyddas på olika sätt. Informationsflödet stödjer många verksamhetskritiska funktioner inom sjuk- och hälsovård, men även andra viktiga funktioner inom landstingets ansvarsområde. Ett strategiskt och systematiskt informationssäkerhetsarbete är en förutsättning för att uppnå exempelvis säkerhet och integritet för patienter och medarbetare, samt för landstingets förmåga att leverera service till medborgarna och informationsutbyte mellan verksamhetsområdena.

Information är en viktig tillgång för alla verksamheter i VLL och den måste kommuniceras, förstås, skyddas på ett säkert sätt. Flödet av information har under senare tid ökat både i omfattning och i komplexitet. Ett ökat informationsflöde innebär ökade möjligheter till effektiviseringar men också ökade risker. I detta perspektiv är hantering av information en ledningsfråga.

Behovet av att reda ut frågan om informationssäkerhet har påtalats från olika håll inom VLL, där många verksamhetsstrategiska frågor är beroende av styrning av informationssäkerhet.
Det har därför beställts en förstudie för att hitta en väg framåt i arbetet med informationssäkerhet inom VLL.

SYFTE

Förstudien visar vilka delmoment verksamheten behöver planera för och investera i för att nå sin målbild i informationssäkerhet, utifrån det nuläge som landstinget befinner sig i.

Förstudien har fokuserat på följande delområden:

- Organisation och ansvar för informationssäkerhet
- Ramverk för informationssäkerhet
- Riskanalys
- Informationsklassificering
- Styrning av åtgärder

Vid uppstart av förstudien framkom även önskemål att ta i beaktande den kommande dataskyddsförordningen (2018) samt den nya regionbildningen (2019) i perspektivet informationssäkerhet.

METOD

Atea har under förstudien genomfört inläsning av ramverk i verksamhetssystem såsom LINDA och LiTA. Kunden, VLL, har under förstudien tillhandahållit personella resurser som Ateas konsult har haft samtal med.

Under förstudien har det genomförts intervjuer med följande resurser inom VLL:

- Anders Sylvan, Landstingsdirektör

- Katarina Holmgren, Ekonomidirektör
- Margit Håkansson, Stabschef Staben för verksamhetsutveckling
- Ulf Olofsson, Verksamhetsområdeschef Service, tf chef för Informatikenheten
- Christina Igasto, Chef för enheten för E-hälsa
- Anna Sundén, Verksamhetschef Enheten för medicinsk teknik och strålningsfysik
- Karin Nygren, Verksamhetschef Laboratoriemedicin, systemägare flertal labbsystem
- Göte Lindahl, IT-strateg
- Göran Lindmark, leveransansvarig Informatikenheten
- Ingrid Hugosson Wallén, kvalitets- och patientsäkerhetssamordnare
- Andrea Kickinger, beredskapssamordnare
- Josefin Leijon, landstingsjurist och personuppgiftsombud

Kontaktperson för arbetet har varit Josefin Leijon, landstingsjurist och personuppgiftsombud. Beställare är staben för verksamhetsutveckling, och dess verksamhetsområdeschef Margit Håkansson.

Området Fysisk säkerhet och Säkerhetsskyddsarbetet inom VLL har inte analyserats och tagits med i denna förstudie.

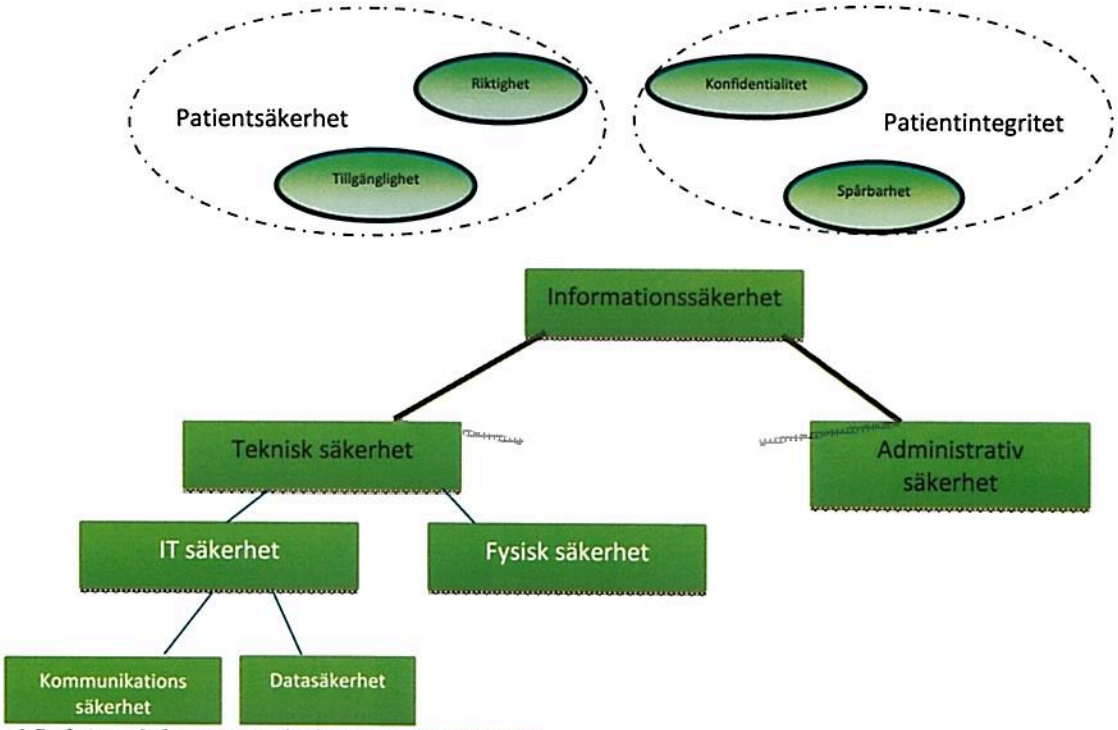
Inledning - Informationssäkerhetsbegreppet

För det första - Informationssäkerhet ska skydda viktig information **oavsett i vilken form** den förekommer; på ett papper, i talad form eller i ett system. Skyddet ska vara avvägt mellan skyddsvärdet och mellan risker och hot samt man måste se till hela kedjan i informationens livscykel.

För det andra – Informationen kan vara viktig ur olika perspektiv. Vi talar om olika aspekter på informationen; **Tillgänglighet, Riktighet, Konfidentialitet och Spårbarhet**. Hur viktigt är det att informationen finns där när du behöver den? Är det viktigt att den är helt oförvanskad? Vem ska få ta del av informationen? Och hur viktigt är det att vi kan följa vad som har skett med informationen? Vad ställs det för krav enligt lagar, förordningar och föreskrifter? Enligt våra avtal med intressenter? Och hur värderar verksamheten (informationsägaren) värdet av informationen? Man utgår därför ifrån **informationsklassificeringen.**

För det tredje - Informationssäkerhet handlar om **samverkan mellan teknisk och administrativ** säkerhet.
Teknisk säkerhet består av fysisk säkerhet och IT-säkerhet och omfattar krav på tekniska skyddsåtgärder för information och omfattar bland annat brandskydd, redundans i datahallar och databaser, virusskydd, krypteringsfunktion och övervakning av kommunikation.

Administrativ säkerhet omfattar bland annat analyser, strategier, regelverk, rutiner, omfattning av övervakning och kontroll samt revision och uppföljning. Se fig.1



Figur 1 Definition Informationssäkerhet, med vårdperspektiv

Organisation och ansvar för informationssäkerhet

DISKUSSION

Ytterst är landstingsledningen ansvarig för informationssäkerheten inom VLL.

Enligt Socialstyrelsens föreskrift **§3 SOSFS 2008:14** ska det av landstingsledningen utses en eller flera personer som ansvarar för informationssäkerhetsarbetet. Denne ska genomföra granskningar och förbereda beslut om skyddsåtgärder i linje med informationssäkerhetspolicyn.

Som i andra frågor följer informationssäkerhetsansvaret med verksamhetsansvaret. Enligt VLLs strategi för kvalitet och patientsäkerhet sägs att ansvaret för informationssäkerheten följer det **ordinarie verksamhetsansvaret.**
Det vill säga att verksamheternas ledning även ansvarar för arbetet med informationssäkerhet, inom sin verksamhet. Men för att faktiskt kunna ta emot ansvaret måste hen ha kompetens och verktyg.
Därför behövs stöd av en utpekad medarbetare som leder arbetet och samordnar de olika verksamhetscheferna, jag vill kalla det en utpekad informationssäkerhetsstrateg.

VLLs **organisation vad gäller informationssäkerhet är idag bristande**. Det är tydligt att informationssäkerhetsområdet **saknar en ledare**.
Ingen inom VLL har formellt tilldelats uppgiften att samordna och driva informationssäkerhetsfrågan efter det att förra informationssäkerhetsansvarige slutade sin anställning.
Man har istället försökt driva informationssäkerhetsarbetet med befintliga personalresurser. Det har med facit i hand inte blivit bra. Informationssäkerhetsfrågor "ramlar mellan stolarna".

Det råder dessutom en viss förekommande falsk föreställning om att personuppgiftsombud också är informationssäkerhetsansvarig.

Det nämns i strategi för kvalitet och säkerhet att **en informationssäkerhetsansvarig** svarar för att utforma de övergripande bestämmelserna för informationssäkerheten samt **vara personuppgiftsombud** för landstinget vilket innebär att självständigt se till att personuppgifter behandlas på ett korrekt och lagligt sätt.

Mina intervjuer visar att **en landstingsjurist** är **utsedd till personuppgiftsombud**. Men vid ersättningsrekrytering av landstingsjurist (tillika personuppgiftsombud) **ingick aldrig frågan om informationssäkerhet**. Det tydligaste beviset för detta är personuppgiftsombudets egen berättelse samt att det saknas en arbetsbeskrivning för informationssäkerhetsansvarig.
Dessutom har detta personuppgiftsombud enligt egen uppgift varken tid, kunskap eller erfarenhet av området informationssäkerhet. Personuppgiftsombudet, understryker dock att denne har kunskap och erfarenhet inom delarna som rör de legala aspekterna av informationssäkerhet, det vill säga personuppgiftslagen, patientdatalagen, offentlighets- och sekretesslagen samt föreskrifter och rättsfall som hör därtill.
Kompetens och erfarenhet är två absoluta nyckelingredienser i informationssäkerhetsrollen. Att driva informationssäkerhetsfrågan inom ett landsting av liknande storlek och komplexitet som VLL, är dessutom vanligtvis ett heltidsarbete som kräver full uppmärksamhet från den utsedde.

Det finns alltså ingen som har fått ett formellt uttalat och överlämnat ansvar och roll som informationssäkerhetsansvarig.

Arbetet med informationssäkerhet inom VLL har under en längre tid varit vilande. Detta har skapat **förvirring i säkerhetsfrågan** för verksamheten. Lyckligtvis, tack vare erfarna och engagerade medarbetare som har samverkat under olika samarbetsformer, löser man dock de allra vanligaste

informationssäkerhetsaktiviteterna. Men på olika håll känner man nu att **frågan måste få en ledare** och **en strategisk inriktning** så att alla involverade arbetar åt samma håll med samma målsättning. Men framförallt **för att bl.a. verksamhetsansvariga och systemägare får stöd och vägledning** i att värdera informationen, prioritera informationssäkerhetsaktiviteter med analyser, metoder och verktyg så att de kan uppfylla det informationssäkerhetsansvar som följer med verksamhetsansvaret och informationsägaransvaret. Det är också viktigt att landstingsledningen kan försäkra sig om att informationssäkerhetsrelaterade frågor som har betydande påverkan på VLLs teknik- och organisationsutveckling utreds och beslutas på rätt nivå. Tex frågan om molntjänster i vården och vilken information som kan läggas i sådana tjänster. Det saknas enligt uppgift idag en molntjänststrategi.

Enheten för E-hälsas medarbetare har däremot ett uttalat arbetsområde som innebär strategisk IT och medicinsk teknik, invånartjänster, framtidens vårdinformationsstöd, vård på distans, **strategisk IT-säkerhet**, arkitektur, processer och projekt.
Den **operativa IT-säkerheten** hanteras av **enheten för Informatik**, men det **saknas en formellt utpekad IT-säkerhetschef.**

I **Socialstyrelsens föreskrift 2008:14** är **informationssäkerhet en fråga om kvalitetsledning**. Det handlar om att skydda information av betydelse för verksamhetskritiska processer. Kvalitets- och säkerhetsfrågor måste i det här perspektivet möta varandra, till exempel genom vårdgivarens samordnade ledning av kvalitets- och säkerhetsinsatser i informationshantering. Det omfattar kvalitetskrav på informationssäkerhetsarbetet till exempel att genomföra regelbundna och systematiska riskanalyser, dvs. att utveckla och tillämpa kvalitets- och säkerhetskrav på verksamhetskritisk information, att specificera och precisera normer, krav och kriterier avseende informationens *konfidentialitet, riktighet, tillgänglighet och spårbarhet*. Detta arbete avser alla typer av verksamhetskritisk information, inte bara system.

Historiskt sett så har informationssäkerhet inte tagits med i den **patientsäkerhetsberättelse** som årligen lämnas till landstingsledningen. Under 2015 beslutade VLL att en **informationssäkerhetsberättelse** ska ingå i den ordinarie patientsäkerhetsberättelsen. I underlaget inför patientsäkerhetsberättelsen finns nu informationssäkerhet med i perspektivet **loggkontroll och driftavbrott** i IT miljön. Detta är endast en **liten del av informationssäkerhet**. VLL har även en plan att utgå ifrån de riskanalyser/avvikelser som Informatikenheten utreder samtidigt som man ställer vissa specifika frågor till verksamheterna.
Det finns säkerligen fler händelser ur ett informationssäkerhetsperspektiv som skulle kunna tas med i en patientsäkerhetsberättelse. **Underlaget bör VLL arbeta vidare med och utveckla.**

Sedan 2012 finns ett **råd för säkerhet och beredskap**, som ska verka för en helhetssyn på säkerhetsfrågor och kontinuerligt utveckla området. Rådet ska samordna och bereda strategiska säkerhetsfrågor och lämna förslag till förbättringar till landstingets ledningsgrupp. Det ska också utarbeta förslag till styrande dokument inom området och överlämna dessa till beslut. Gruppen ska också vara projektgrupp i arbetet med risk- och sårbarhetsanalyser inför extraordinära händelser samt löpande gå igenom de risker som verksamheten har lyft till säkerhetsrådet. I säkerhetsrådet ska de 13 olika säkerhetsområdena i "säkerhetscirkeln" (VLL begrepp) representeras.
Rådet har **historiskt sett dock varit helt fokuserat på kris- och katastrofberedskap**, av naturliga orsaker då ordförandeskapet enligt styrande dokument ligger hos beredskapssamordnaren. En ny beredskapssamordnare tillträdde i maj 2016, och ha identifierat **behovet att se över funktionen av detta råd för säkerhet och beredskap.**

REKOMMENDATION

VLL bör påbörja processen att **tillsätta en informationssäkerhetsstrateg.** Hen bör ha ansvar för att verkställa samordningen av informationssäkerhetsarbetet inom landstinget, att förvalta landstingets informationssäkerhetspolicy, riktlinjer, landstingets tillämpningsanvisningar samt den övergripande handlingsplanen för informationssäkerhet. Hen bör arbeta med informationssäkerhetsfrågor på en **övergripande och strategisk nivå**. I ansvaret bör ingå omvärldsbevakning, samordning, att vara sammankallande i landstingets informationssäkerhetsråd samt att inhämta information om och rapportera informationssäkerhetsläget i landstinget som ett led i uppföljningen av informationssäkerheten. Hen bör även vara landstingets representant i kontakt med externa organisationer, myndigheter och medborgare i frågor som rör informationssäkerhet.

För att åstadkomma en god säkerhet **krävs en helhetssyn på styrning av åtgärder, kravställning vid upphandlingar, kontroll och uppföljning och kontinuerlig förbättring**. Detta ska drivas av denna informationssäkerhetsstrateg.

Kontaktuppgifter till denna informationssäkerhetsstrateg bör kommuniceras inom hela VLL.

Det etablerade rådet för säkerhet och beredskap är en bra grund för VLL att bygga vidare på. En möjlighet för VLL är att benämna rådet för **Informationssäkerhetsrådet**.
Rådet bör bemannas av informationssäkerhetsstrateg (ordförande för rådet), IT-säkerhetschef, säkerhetschef, personuppgiftsombud, landstingsjurist, kvalitets- och patientsäkerhetssamordnare, IT-strateg (e-hälsa), kvalitetsansvarig (KVA) Informatikenheten, säkerhetsskyddschef och beredskapssamordnare. Andra berörda adjungeras vid behov

Syftet med rådet ska vara att **verka för en helhetssyn på informationssäkerhetsfrågor** och **kontinuerligt utveckla området**.

Rådets uppdrag bör vara att samordna och bereda strategiska frågor för informationssäkerhet, lämna förslag till förbättringar till landstingsledningen, ta fram styrande och stödjande dokument inom informationssäkerhetsområdet och lämna dessa till beslut. Rådet ska löpande gå igenom och behandla de risker som är lyfta till informationssäkerhetsrådet. Rådet ska årligen lämna och föredra en rapport till landstingsledningen över informationssäkerhetsläget inom VLL.

Ramverk för informationssäkerhet

DISKUSSION

Enligt **2 kap §1 SOSFS 2008**:14 **ska det** i en vårdgivares ledningssystem för kvalitet och patientsäkerhet **finnas en informationssäkerhetspolicy**.

I VLLs policy för kvalitet och säkerhet (2016) finns följande:
" Vi hanterar information på ett säkert sätt och som värnar den personliga integriteten och sekretessen"

I landstingets strategi för säkerhet och beredskap (2011) sägs:
"Landstinget eftersträvar ett balanserat skydd efter analys av hot och risker. Syftet med informationssäkerhetsarbetet är att:
- Skapa förutsättningar för god tillgänglighet till riktig och spårbar information
- Skydda information mot obehörig åtkomst
- Uppnå en säker hantering och bearbetning av all information
Västerbottens läns landstings informationssäkerhetsarbete ska präglas av att:
"Rätt användare arbetar med rätt information på rätt plats med stöd av rätt utrustning".

Att **införa ett standardiserat arbetssätt** i verksamheten kan vara en bra arbetsmetod för att säkerställa informationssäkerhetskraven, internationellt inom informationssäkerhet pekar man på standarderna **ISO 27001 och ISO 27002**. En specifik standard för informationssäkerhet inom hälsa- och sjukvården har tagits fram baserad på ISO 27002; den heter **ISO/IEC 27799:2016 Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO 27002.**

Enligt internationella vedertagna standarder såsom de ovan nämnda sägs att högsta ledningen ska upprätta en informationssäkerhetspolicy som:
a) är anpassad till organisationens syfte;
b) ger ett ramverk för att sätta informationssäkerhetsmål;
c) innefattar ett åtagande att uppfylla tillämpliga krav relaterade till informationssäkerhet; och
d) innefattar ett åtagande att ständigt förbättra ledningssystemet för informationssäkerhet.

Informationssäkerhetspolicyn ska:
e) finnas tillgänglig i dokumenterad form;
f) kommuniceras inom organisationen; och
g) i tillämplig utsträckning vara tillgänglig för intressenter.

Med det kan slutsatsen tas att **en informationssäkerhetspolicy i den bemärkelsen saknas för VLL**.

REKOMMENDATION

Det som strategin för säkerhet och beredskap säger om informationssäkerhet bör utvidgas i **en separat informationssäkerhetspolicy.**
Policydokumentet måste beskriva informationssäkerhetsområdet, mål med arbetet och hur ansvarsfördelningen ser ut.

Informationssäkerhetspolicyn **ska sedan kompletteras med riktlinjer och anvisningar** till stöd för verksamhetsansvariga, till systemägare, till medarbetare och andra viktiga funktioner.

VLL bör ha ISO/IEC 27799:2016 Hälso- och sjukvårdsinformatik – Ledningssystem för informationssäkerhet i hälso- och sjukvården baserat på ISO 27002 som guidning i arbetet med informationssäkerhet och ramverket för detta.

Ramverket för informationssäkerhet bör kommuniceras och **ingå i befintliga ledningssystem** inom VLL.

Informationssäkerhetsarbetet inom VLL bör **utgå ifrån interna och externa krav**

- VLLs vision – "världens bästa hälsa år 2020"
- VLLs värdegrund – "ständigt bättre – patienten alltid först"
- VLLs mission
- VLLs övergripande mål satta av ledningen
- VLLs informationssäkerhetspolicy
- Samhällets krav på hanteringen av offentlig information och personuppgifter och tillvaratagandet av den personliga integriteten, med tillhörande lagar, förordningar och föreskrifter
- Samhällsutvecklingen och de av landstingets antagna strategierna som knyter an till en informationssäkerhetsaspekt
- Internationella standarder för informationssäkerhet

Informationssäkerheten ska bidra till att **upprätthålla varumärket VLL**.

Riskanalys

DISKUSSION

Det är genom riskprioriteringar och skyddskrav på information som kontroller, risk- och incidentrapportering, kan införlivas i det dagliga vårdarbetet. Utan riskprioriteringar och skyddskrav förblir informationssäkerhet en fråga om efterlevnad av externa krav, varför åtgärder blir ineffektiva, om inte rent av riskfyllda. I säkerhetsarbetet måste skyddskostnaden stå i proportion till riskkostnaden.

Anpassad informationssäkerhet i en organisation innefattar att möjliga risker identifieras, värderas och åtgärdas. Det är viktigt att inte bara fokusera på risken då sekretessbelagd eller annan känslig information kan röjas för obehöriga, utan även på risker som kan innebära att informationen blir otillgänglig eller förvanskad. Risker som identifierats av flera olika delar av landstinget där systematiska fel verkar ligga bakom lyfts sedan som landstingsgemensamma risker och hanteras därefter.

Idag genomförs riskanalyser av olika slag inom VLL, ur patientsäkerhetsperspektivet, ur beredskapsperspektivet, ur IT-säkerhetsperspektivet; men **någon riskhantering inom informationssäkerhetsområdet förekommer inte.**

Landstingsdirektören har under förstudien uttalat att han i sin roll **önskar ha återkoppling** om hur **risker** inom informationssäkerhetsområdet har hanterats samt om ny riskbild föreligger. Det är en del av ett ledningssystem. Idag saknar landstingsdirektören sådan återkoppling.

REKOMMENDATION

VLL bör etablera en rutin för riskanalys, förslagsvis bör rutinen utgå ifrån **ISO 27005:2011 – Riskhantering för informationssäkerhet – samt ISO/IEC 27799:2016**.

ISO 27005 standarden innehåller **riktlinjer för hanteringen av informationssäkerhetsrisker** i en organisation, och ger särskilt stöd inom detta område för ett ledningssystem för informationssäkerhet (LIS) i enlighet med SS-ISO/IEC 27001.
ISO 27005 tillhandahåller inte någon specifik metod för hanteringen av informationssäkerhetsrisker. Det åligger varje organisation att definiera sitt förhållningssätt till riskhantering beroende på till exempel LIS omfattning, riskhanteringens kontext eller bransch. Ett antal befintliga metoder kan användas. VLL bör hitta sin metod utifrån denna standard.

Återkommande riskanalyser ger en bra grund för att säkerställa rätt nivå av skydd. Riskanalyser bör med fördel utföras med stöd av information från omvärldsbevakning, resultat av tidigare riskanalyser, incidentrapportering samt affärsmässiga- och juridiska krav. Alla identifierade hot och sårbarheter bör klassificeras och riskbestämmas. Risker som bedöms som oacceptabla lindras med fördel genom införandet av säkerhetsåtgärder.

Hanteringen av informationssäkerhetsrisker bör ge följande resultat:

- att risker identifieras,
- att risker bedöms efter vilka konsekvenser de har för verksamheten och sannolikheten för att de uppträder,
- att sannolikheten och konsekvenserna för dessa risker kommuniceras och förstås,
- att en prioritetsordning för riskbehandling fastställs,
- att prioriterade åtgärder för hantering av risker fastställs,
- att intressenter involveras när beslut om hantering av risker fattas och hålls informerade om status för riskhanteringen,

- övervakning av riskbehandlingens verkan,
- att risker och riskhanteringsprocessen övervakas och granskas regelbundet,
- att information samlas in för att förbättra metoden för riskhantering,
- att chefer och personal utbildas om riskerna och de åtgärder som vidtas för att hantera dem.

Ett införande av rutin för riskanalys är i ett inledande skede resurskrävande. Det är också av vikt att **resultatet** från riskanalyserna **leder till förbättring**.

VLL bör **ta expertishjälp** i frågan.

Informationsklassificering

DISKUSSION

För att veta **hur man ska skydda VLLs informationstillgångar** krävs att det genomförs **informationsklassificering**. Det är informationen som är skyddsobjektet, d v s det som ska skyddas.
Genom att placera information i särskilda informationsklasser vet VLL vilka tillgångar som kräver mer skydd än andra.
Varje informationstillgång måste tilldelas en informationssäkerhetsklass som **motsvarar dess betydelse** för den aktuella verksamheten. Även system och andra resurser bör klassificeras om de t.ex är starkt knutna till viss information. Informationens klass styr ju systemets klassificering.

När man bedömer informationens klass sker det både **utifrån den egna verksamhetens behov och utifrån externa krav**. Avsikten är ju att varje informationstillgång ska omges med **rätt skydd**.
Informationsklassningen styr vilken skyddsnivå som ska tillämpas för att skydda informationen. I detta ingår även skyddsnivåer för information på olika sorters media t.ex. digitalt, i pappersform eller i andra former.

Skyddsåtgärderna som därefter införs ska vara kopplade till en riskbedömning och ska spegla informationens värde.

Det finns idag ingen informationsklassificeringsmetod eller -modell inom VLL.
Det innebär att **det finns risk för att VLL dels inte lever upp till legala eller intressenters krav**, men även att information inom VLL kan komma obehöriga till del, kan bli förvanskad och inte kommas åt när den behövs för att utföra en arbetsuppgift.
Klassificeringen ligger ju till grund för vilka skyddsåtgärder som ska utformas och vilka rutiner som ska gälla, dvs hur informationen får hanteras, lagras, distribueras och avvecklas.

REKOMMENDATION

Informationsklassning är ett område inom VLL som bör förtydligas och omges med riktlinjer, hanteringsregler och skyddsnivåer. Erfarenheter från andra landsting är att detta fungerar dåligt i praktiken så det är viktigt att det blir rätt.

Informationsklassificeringen är väldigt central i informationssäkerhetsarbetet.
För att VLL ska etablera en för er anpassad informationssäkerhetsnivå måste ni inleda ett arbete med att **ta fram en metod och modell för informationsklassificering**.
I modellen klassificeras information utifrån de konsekvenser som oönskad påverkan på informationens kvalitet bedöms leda till. Konsekvenserna värderas i termer av oönskad påverkan på verksamheten eller annan part till följd av otillräcklig konfidentialitet, riktighet eller tillgänglighet. Om exempelvis organisationen lider allvarlig skada av att viktig information för verksamheten blir tillgänglig för obehöriga, ska informationen placeras i en klass med hög konsekvensnivå avseende konfidentialitet.
Alla relevanta aspekter, inte bara konfidentialitet, ska vägas in i informationsklassificeringen.

Det är informationsägaren som är ansvarig för att informationsklassningen sker, eftersom det är en del av informationssäkerheten, men idag finns varken metod eller modell för informationsklassificering framtagna inom VLL så informationsklassificeringen blir därför inte genomförd.
Den som har rollen att driva och leda informationssäkerhetsarbetet i VLL är ansvarig för att **förse verksamheten med rätt verktyg och metoder i informationssäkerhetsarbetet.**

Informationsklassificering kan vara resurskrävande och ett komplicerat moment i informationssäkerhetsarbetet, VLL bör därför överväga att **ta expertishjälp i frågan**.

Styrning av åtgärder

DISKUSSION

Landstingsrevisorernas rapport från 2014 beskriver att **landstingsstyrelsen och hälso- och sjukvårdsnämnden saknar rutiner** som säkerställer att **de får rapporter om informationssäkerhetsarbetet i VLL**. Varken landstingsstyrelsen eller nämnden har fått rapporter om vilka granskningar, riskanalyser, skyddsåtgärder mm av större betydelse som är gjorda inom området för vårdgivarens informationssäkerhet.
Avsaknad av uppföljning och väsentliga funktioner för arbete med informationssäkerhet medför **risk att landstingsstyrelsen och hälso- och sjukvårdsnämnden inte uppfyller sitt vårdgivaransvar inom informationssäkerhetsområdet**.

Ur Patientsäkerhetsberättelsen 2015, ver 1:
"Västerbottens läns landsting har ett flertal riktlinjer för att upprätthålla informationssäkerheten, det finns bland annat riktlinjer för personal och riktlinjer för åtkomst till elektronisk information. Varje verksamhetschef ansvarar för att det finns ett systematiskt arbete med att göra loggkontroller och att avvikelser som uppmärksammas hanteras enligt gällande rutin. Sedan hösten 2015 krävs SITHS kort och ett medarbetaruppdrag för att arbeta ibland annat patientjournalen vilket ökat säkerheten.
Att dokumentationen i journalen sker enligt gällande författningar kontrolleras och diskuteras i samband med patientsäkerhetsdialogen."
Noteras bör att vid tidpunkten för patientsäkerhetsberättelse 2015 hade inga frågor om informationssäkerhet ställts till verksamheten eller informatik tillfrågats om underlag. Detta arbete håller på att förändras inom VLL.

Verksamhetschefen skall årligen genom patientsäkerhetsberättelsen rapportera de risker, analyser och genomförda åtgärder som vidtagits i verksamheten utifrån dess informationssäkerhetsansvar.

Som ett försök till att uppnå ovanstående har personuppgiftsombud tillsammans med patientsäkerhetssamordnaren infört vissa frågor om informationssäkerhet i det underlag som ligger till grund för patientsäkerhetsberättelsen.

REKOMMENDATION

Det årliga arbetet med **informationssäkerhetsberättelsen** bör ledas av informationssäkerhetsstrategen.

I informationssäkerhetsberättelsen bör landstingsstyrelsen och nämnden få rapporter om **vilka granskningar, riskanalyser, skyddsåtgärder mm av större betydelse som är gjorda inom området för vårdgivarens informationssäkerhet.**

Informationssäkerhetsberättelsen bör också redovisa vilka betydande åtgärder på sammanhållen nivå som har vidtagits under året för att förbättra informationssäkerheten i patientrelaterad verksamhet inom VLL.
Dessa delar av informationssäkerhetsberättelsen **kan förslagsvis läggas med i patientsäkerhets-berättelsen.**

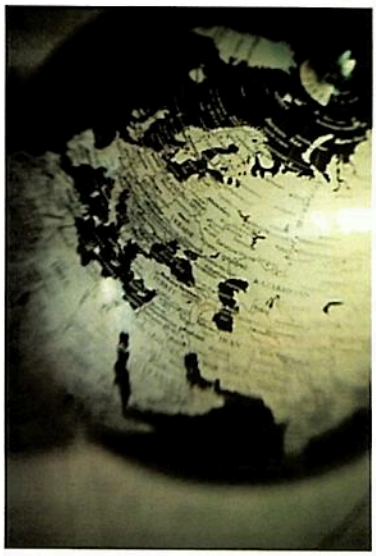
Att kunna **ta med informationssäkerhetsperspektivet** i VLLs styrmodell skulle kunna vara en möjlig väg att gå. Där verksamheten inför sitt **verksamhetsplaneringsarbete** belyser informationssäkerheten som ett perspektiv att ta med i verksamhetsplanen. Möjligheten för detta bör VLL analysera redan nu, eftersom VLL nu ser över sin styrmodell.

Informationssäkerhet & den nya dataskyddsförordningen (2018)

DISKUSSION

(Källa Sveriges Kommuner och landsting, SKL)
Dataskyddsförordningen (EU) 2016/679 blir svensk lag och **ska börja tillämpas i maj 2018**. Förordningen kommer att ersätta personuppgiftslagen (PuL) men kommer också att påverka patientdatalagen (PDL).

Principerna för behandling personuppgifter är i stort sett densamma som i direktivet från 1995, dock finns ett **ökat fokus på öppenhet och på att säkerställa att lämpliga säkerhetsåtgärder vidtas.**



Att förstå EU: s nya dataskyddsförordning (förordningen) är viktigt för varje organisation t.ex. vårdgivare som hanterar personuppgifter. Förordningen stärker dataskyddet genom att sätta mer fokus på ansvar och säkerhet. De som behandlar personuppgifter kommer nu att tvingas inte bara att följa den nya lagstiftningen utan också **visa att de har uppfyllt kraven**.

Den nya förordningen har i princip samma mål som EU: s direktiv om dataskydd från 1995 och syftar till att göra skyddet mer lämpat för dagens tekniska miljö och att säkerställa samma skyddsnivå för dataskydd inom EU.
Genom den nya förordningen ges mindre tolkningsutrymme på nationell nivå. **Inom området hälso- och sjukvård kommer det dock fortfarande att finnas vissa möjligheter att ha kompletterande lagstiftning, vägledningar och regler, eftersom det är ett område där EU tillåter en nationell lagstiftning**.

Genom förordningen införs också nya definitioner (artikel 4) för personuppgifter som rör hälsa, genetiska data och biometriska uppgifter:

- uppgifter om hälsa: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,
- genetiska uppgifter: alla personuppgifter som rör nedärvda eller förvärvade genetiska kännetecken för en fysisk person, vilka ger unik information om denna fysiska persons fysiologi eller hälsa och vilka framför allt härrör från en analys av ett biologiskt prov från den fysiska personen i fråga

Den rättsliga grunden för laglig behandling av personuppgifter är i stort sett den samma som i direktivet från 1995. **En viktig förändring är dock att som laglig behandling räknas inte längre den intresseavvägning som myndigheter tidigare kunde åberopa som grund för sin behandling** när de utför sina uppgifter. Enligt förordningen måste myndigheter (inklusive offentliga sjukhus och övriga vårdgivare) numera **kunna ange en laglig grund för sin behandling**.

I Sverige finns den lagliga grunden för behandling av personuppgifter inom hälso- och sjukvården huvudsakligen i patientdatalagen. Medlemsländerna kan välja att ha en nationell lagstiftning för behandling av personuppgifter i hälso- och sjukvården.

Regeringen har dels tillsatt utredningen (Dir 2016:15) om dataskyddsförordningen som ska föreslå hur den centrala svenska lagstiftningen på området bäst anpassas till den nya förordningen och dels utredningen (Dir 2016:52) om anpassningar av författningar inom Socialdepartementets verksamhetsområde. Dessa utredningar kommer att presenteras under våren respektive hösten 2017.

SKL arbetar för att ge råd och stöd för kommuner, landsting och regioners arbete med att anpassa sin verksamhet till Dataskyddsförordningen.

REKOMMENDATION

Kommuners, landstings och regioners verksamheter inom hälso- och sjukvården **behöver redan nu förbereda sig** då dataskyddsförordningen innehåller **flera nyheter och viktiga förändringar** jämfört med nuvarande regelverk.

De registeransvariga förväntas nu inte bara följa principerna, men **ska också kunna visa att regelverket efterlevs på ett ansvarsfullt sätt**. Det är en viktig och betydande förändring från passiv till aktiv efterlevnad som VLL bör uppmärksamma. Ett sätt att visa att personuppgifts behandling är i överensstämmelse med lagstiftningen kan vara att anta uppförandekoder, interna riktlinjer och förfaranden.

VLL kan **redan nu inleda ett arbete att analysera vilken påverkan** dataskyddsförordningen kan få på den egna verksamheten.
Landstingets jurister har redan börjat titta på frågan och bevakar området.

Analysera inom vilken eller vilka delar av organisationen som ett sk **dataprotection officer, DPO**, ska tillsättas med anledning av dataskyddsreformen. Förordningen, som kommer att träda i kraft i maj 2018, anger att hen behöver ha yrkesmässiga kvalifikationer, såsom kunskap om lagstiftning och praxis om dataskydd. DPO behöver kunna rapportera direkt till högsta ledningen för den personuppgiftsansvarige.

I god tid före dataskyddsförordningen träder i kraft (maj 2018) bör VLL **informera hela organisationen om vad dataskyddsförordningen innebär**, och vilka rutiner och processer VLL har för att ta hand om VLLs ansvar i frågan och de registrerades rättigheter enligt förordningen. Informera också organisationen **vem som är utsedd** till data protection officer och **kontaktuppgifter till denna.**

Informationssäkerhet & den nya regionbildningen (2019)

DISKUSSION

På förslag är att Västernorrlands, Jämtlands, Västerbottens och Norrbottens län kommer att läggas samman till en region, detta under 2019.
Nivån på informationssäkerheten inom respektive landsting i dessa län **är troligtvis väldigt varierande**. Och man har styrkor och svagheter inom olika delområden vad gäller informationssäkerhet. Det kommer att bli ett givande och tagande i fråga om vilka modeller, processer, rutiner mm som ska gälla för regionen.

Förmodligen blir det ett län som har kommit längst i sitt informationssäkerhetsarbete som blir tongivande i informationssäkerhetsarbetet för hela regionen.

REKOMMENDATION

Ur informationssäkerhetsperspektivet och regionbildningsfrågan är min bedömning att informationssäkerhetsområdet kommer att få allt mer betydelse, då en samverkan kring funktioner och tjänster kommer att realiseras. Information kommer att få en vidare spridning.

Det kommer sannolikt vara mycket som kan samordnas inom regionen, såsom modeller, processer, metoder. EN informationssäkerhetsstrateg som leder hela regionen. Det är dock rimligt att tro att varje del av regionen, nuvarande län, kommer att behöva en lokal informationssäkerhetssamordnare för att hålla samman informationssäkerhetsarbetet lokalt.

Min rekommendation i fråga om informationssäkerhet och regionbildningen är att **uppmana till samverkan mellan länen** redan idag, att **utse någon att vara VLLs representant** i detta samverkansarbete för att vara i samma fas som övriga i samverkansgruppen i det fall en regionbildning sker.