Ålands hälso- och sjukvård

IT-granskning med fokus på informationssäkerhet (patientinformation)

11.1.2016
Sidantal 23
4423828_2.docx

Innehåll

1 Inledning

1.1 Sammanfattning

Under granskningen har KPMG ur olika perspektiv granskat informationshanteringen och informationssäkerheten i ÅHS.

Positiva observationer under granskningen är bl.a. att:

- Man är på ÅHS öppen för diskussion inom ämnet och man har en klar vilja att ställa informationssäkerheten i ordning så fort som möjligt
- I viss mån har arbetet med att beta av den tekniska IT-skulden påbörjats
- I viss mån har arbetet med att förhöja informationssäkerheten och förbättra kontinuiteten påbörjats

För att kunna utveckla sin informationssäkerhet bör ÅHS dock ta fasta på alla perspektiv vad beträffar informationssäkerhet. Det är frågan om ett strategiskt val och gediget samarbete både inom ÅHS men också mellan ÅHS och ÅDA samt ÅHS och övriga leverantörer. Som en sammanfattning kan sägas att följande utvecklingsområden är speciellt kritiska för att ÅHS skall kunna utveckla och bibehålla en sådan nivå på informationssäkerheten att riskerna kan hanteras:

- Höjandet av informationssäkerheten bör vara ett strategiskt mål inom ÅHS och man bör från styrelse och ledning neråt i organisationen organisera sig och reservera resurser och kompetens både inom ÅHS och hos ÅDA för att både höja informationssäkerhetsnivån och hållas på denna nivå (ref. observation 3, 5, 10)
- IT-Riskhantering och riskanalys (informationssäkerhet) bör vara en naturlig del av allt arbete inom IT-verksamheten[1] och speciellt inom kontinuitetsplaneringen. Man bör evaluera kontinuitetsplaner, befintliga risker och nya risker kontinuerligt under verksamhetsåret (ref. observation 1, 6, 14)
- Man bör målmedvetet införa och anpassa metodologier, ramverk och standarder[2] för att beskriva verksamheten och specifikt IT-verksamheten. Beskrivningarna är till för att få en helhetsbild av verksamheten och IT-verksamheten för att lättare kunna styra IT-verksamheten mot utställda mål. Bland dessa mål bör på organisationsnivå finnas att försäkra sig om att informationssäkerheten tas i beaktande jämlikt inom organisationen och ur väsentliga perspektiv (administrativ, arkitektur, teknisk) (ref. observation 2, 8, 9, 11)
- Man bör utan dröjsmål inleda arbetet att
    - uppdatera systemkarta,
    - klassificera all information och alla system (risk, kontinuitet och information),
    - utförligt beskriva informationsarkitekturen (patientinformation) och
    - utförligt beskriva integrationsarkitekturen (mellan system)

[1] Med IT-verksamhet menas en helhet som omfattar både ÅHS och ÅDA vad beträffar personer, processer och teknologi inom IT
[2] Se länkar till referensmaterial i bilaga A

för att kunna beskriva i första hand de kritiska systemens samverkan (ref. observation 7, 2)

- Man bör utan dröjsmål skydda sitt nätverk genom att
    - utföra en extern och intern teknisk sårbarhetstestning på nätverket
    - på basen av testresultaten planera och utveckla nätverksarkitekturen från ett riskbaserat perspektiv. I planeringen bör beaktas segregation mellan olika nätverksanvändning, brandväggar, intrångsskydd (IPS/IDS) och kontinuitet (t.ex. UPS för WLAN-routers) (ref. observation 12)
- Man bör utan dröjsmål samla observationer från övriga granskningar och starta arbetet med utvecklingsförslagen i respektive granskning

I följande stycke följer sammandrag ur olika perspektiv: Informationssäkerhet som sådan (stycke 2.1), IT-verksamhet och systemutveckling (stycke 2.2) och IT-drift och teknologiarkitektur (stycke 2.3). I slutet av sammanfattningen finns de mest kritiska observationerna listade.

I den konfidentiella delen av rapporten hittas mera ingående information om observationerna, dess prioritet och utvecklingsförslag.

1.2 Bakgrund för IT-granskningen

I samband med revisionen 2015 av Ålands Hälso- och Sjukvård (ÅHS) har en granskning av IT-verksamheten inom sjukhuset genomförts. Fokus har varit på informationssäkerhet och –integritet (eng. Privacy) med hänseende till att ÅHS äger och hanterar sensitiv information, såsom patientinformation. Granskningen har utförts ur olika perspektiv, såsom arkitektur, riskbedömning och granskning av väsentliga informationssäkerhetskontroller.

Eftersom ÅHS den 1 januari 2015 överfört sin IT-verksamhet till Åda Ab (ÅDA), är det av yttersta vikt att också känna till ÅDA:s verksamhet i förhållande till ÅHS behov av informationssäkerhet. I granskningen har därför tagits i beaktande de respektive roller och ansvarsområden ÅHS och ÅDA sinsemellan har vad beträffar IT-verksamheten (närmast IT-drift, IT-utveckling samt IT-förvaltning).

Inför denna IT-granskning har till KPMG:s kännedom tilldelats tre olika rapporter, där utomstående parter vid olika tidpunkter och i olika sammanhang gjort en bedömning av IT-verksamheten inom ÅHS. Dessa rapporter är följande:

- Informationssäkerhetsgranskning av Ålands hälso- och sjukvård (ÅHS), version 1, 2014-10-03, C2Solutions
- Utvecklingsprocessen samt teknisk plattform för Medix, Februari 2013, PwC
- Revisionsrapport - Granskning av IT-verksamheten 2011, Mars 2012, PwC

Slutresultaten i dessa rapporter har konsekvent varit sådana, att man kan tolka att informationshanteringen och informationssäkerheten är på en låg nivå. Med hänseende till tidigare resultat, sågs det nödvändigt att i revisionen 2015 fokusera på IT-granskning och därigenom analysera de underliggande orsakerna till dylika slutresultat sedan 2011 inom ÅHS.

1.3 Syftet med granskningen

Syftet med granskningen var att:

- bedöma hur informationssäkerheten tas i beaktande i sjukhusets verksamhet
- kartlägga och bedöma IT-risker som kan påverka informationssäkerheten både i befintliga system samt vid utveckling och upphandling
- bedöma hurudana förutsättningar det för tillfället finns för att utveckla eller förnya komplexa system såsom journalsystemet
- kartlägga och bedöma helhetsarkitekturarbetet och hur det understöder verksamheten
- bedöma hurudan styrning och kontroll IT-verksamheten drivs av

1.4 Målet med granskningen

Målet med granskningen var att få en insyn i:

- underliggande orsaker till varför informationssäkerheten är på en låg nivå
- om det finns tillräcklig kompetens inom ÅHS och ÅDA att sköta IT-verksamheten så att
  - man kan hantera IT-driften och samtidigt utveckla den
  - man kan uppnå efterlevnad av t.ex. informationssäkerhetsramverk
  - man kan förnya teknologiarkitekturen och ta igen på systemskulden
- om det finns tillräckliga resurser och kompetens inom ÅHS och ÅDA att
  - krav ställa systemutveckling och/eller upphandling
  - förverkliga systemutveckling

1.5 Granskningens omfattning

Granskningen har utförts av Kristian Backman och Alex Fagerström (KPMG Oy Ab) under oktober och november 2015. Granskningen har genomförts genom intervjuer av nyckelpersoner, genomgång av befintlig och relevant dokumentation samt genom utförandet av tre olika bedömningsfaser baserat på KPMG:s globalt utvecklade metodologier. Följande faser har genomförts:

Fas	*Innehåll*	*Metodologi*	*Resultat*
Strategisk verksamhetsanalys	Analys av verksamheten och organisationen	Intervjuer och granskning av dokumentation	1. Kännedom om affärs- och IT-landskap
	Maturitetsanalys av helhetsarkitekturen	KPMG EA Maturity Assessment Methodology	2. Maturitetsmatris på helhetsarkitektur
IT-riskbedömning	Identifikation av IT-risker	KPMG Business Continuity Management Methodology – Risk Assessment	3. IT-risk register
	Analys och prioritering av identifierade risker		4. IT-risk prioritering
Datasäkerhetsanalys	Intervju, IT-risk genomgång, analys och rekommendationer	Anpassad ISO 27001	5. Lista på observationer, dess risker samt rekommendationer

1.6 Avgränsning

Granskningen avser att bedöma IT-verksamheten. Informationssäkerheten granskas generellt ur ett administrativt perspektiv utan fokus på något speciellt system. Ingen teknisk testning utförs.

2 Sammanfattning ur olika perspektiv

2.1 Informationssäkerhet

Informationssäkerheten är på en låg nivå, såsom framkommit i tidigare granskningar och även i denna granskning. Det finns en stor risk att patientinformationen oavsiktligt eller avsiktligt kan komma i fel händer, eftersom man inte har tillräckliga informationssäkerhetskontroller eller beskrivningar över systemens samverkan.

De underliggande orsakerna är mångfasetterade, men en stor bidragande orsak ligger i att ingen tidigare har haft helhetsansvar över informationssäkerheten i ÅHS. Man strävar i första hand till att försäkra patientsäkerheten men missar onekligen däri, att patientinformationen är en del av patientsäkerheten. En informationssäker miljö skyddar förutom patientinformationen också i vården använda system både för diagnoser, behandling och rapportering – vilket har en direkt koppling till patientsäkerheten.

IT-riskerna kartläggs inte kontinuerligt vilket skulle vara en förutsättning för att man årligen vet var man står och såtillvida har en möjlighet att planera åtgärder framöver för att hantera riskerna. Situationen idag är sådan, att då man inte identifierat IT-riskerna styr man heller inga utvecklingsresurser på t.ex. informationssäkerhet vilket gör att allt utvecklingsarbete mot en informationssäker miljö blir ogjort.

Man utgår inte ifrån något som helst ramverk för informationssäkerhet, vilket gör att man på organisationsnivå inte har någon enhetlig linje och inget gemensamt mål att nå vad beträffar informationssäkerhet. Då man inte har något fastställt ramverk att arbeta mot, är det snarast omöjligt att prioritera utvecklingsarbetet vilket gör att allt utvecklingsarbete mot en informationssäker miljö blir ogjort.

Informationssäkerheten bör ha en större roll inom ÅHS och den bör som en del av patientsäkerheten vara på styrelsen agenda och därigenom vara en del av ledningen strategiska mål. På detta sätt får informationssäkerheten den vikt den inom hälso- och sjukvård bör ha, och genom att aktiviteterna har strategiska mål mäts dessa också kontinuerligt. För att förverkliga de strategiska målen bör IT-strategikommitén och vårdsystemgruppen återaktiveras samt en IT-säkerhetsgrupp skapas. Dessas roll är att ta fasta vid utvecklandet av informationssäkerheten och informationssäkerhetskulturen inom ÅHS.

Se länkar till referensmaterial i bilaga A.

2.2 IT-verksamhet och systemutveckling

IT-verksamheten i sin helhet och speciellt systemutveckling har under flera år lidit av resursbrist. Resursbristen har lett till att man egentligen enbart kunnat koncentrera sig på att underhålla befintliga IT-arkitektur vilket lett till att utvecklingsprojekt vad beträffar förnyanden av föråldrade system och föråldrad teknologi lagts mer eller mindre på is. Detta har lett till att ÅHS har en enorm teknologiskuld vad beträffar både system, systemplatformer och övrig infrastruktur och detta påverkar även nivån på informationssäkerhet genom sårbarheter i äldre teknologi och systemvara.

IT-verksamheten på ÅHS har inte alltid drivits med långsiktiga målsättningar utan det har varit frågan om att överleva med den IT man har ett budgetår i taget. Detta har lett till att man inte

planerat och förvekligat sin IT baserat på långsiktiga mål som baserat sig på verksamhetsstrategin, IT-strategin och systemens och teknologins livscykel vilket i sin tur förorsakat en IT-skuld.

Såsom framgår i maturitetsanalysen (konfidentiell, stycke 4.1) är IT-verksamheten på ÅHS på en låg nivå med tanke på styrning och kontroll. Funktioner som IT-strategikommité och vårdsystemgrupp är inte idag aktiva och IT-säkerhetsgrupp fattas. Det är inte befogat att inte ha eller vara del av IT-verksamheten på ÅHS av den orsaken att IT-driften flyttat till ÅDA. ÅDA:s roll gentemot ÅHS är att förverkliga teknologiska lösningar och infrastruktur på basen av det som ÅHS beställer och lägger krav på och till det måste det på ÅHS finnas en IT-verksamhet med insikt om nuvarande IT-omgivning, arkitektur och substanskännedom.

För att ÅHS skall ha en sund möjlighet att genomföra de stora utvecklingsprojekt som är på kommande och samtidigt utveckla informationssäkerheten och däri patientsäkerheten, bör man lägga stort fokus på utvecklandet av styrandet av IT-verksamheten inom ÅHS och mot ÅDA. Nyckeln är klara gränsdragningar med ansvar och skyldigheter både inom ÅHS och speciellt mellan ÅHS och ÅDA. IT kommer i fortsättningen att ha en allt större roll i hälso- och sjukvården även inom ÅHS. Digitalisering av både system för patienter och klienter (t.ex eRecept, KanTa) och medicinteknik gör att IT blir mera centralt och får en ännu mera kritisk roll. Kravspecifikationen för att utveckla detta kommer från ÅHS och det bör finnas den kompetens inom ÅHS att de kan se till att utvecklingen är i linje med verksamhetsstrategin, yttre och inre krav, lagar och stadgar.

Se länkar till referensmaterial i bilaga A.

2.3 IT-drift och teknologiarkitektur

IT-driften är sedan januari 2015 utlokaliserat till ÅDA. Samtidigt har ÅHS driftspersonal, en systemplanerare och en IT-chefstjänst flyttat över till ÅDA. I praktiken ansvarar ÅDA i fortsättningen över förverkligandet av hela IT-infrastrukturen och teknologiarkitekturen. Genom att utlokalisera IT-driften till ÅDA, förväntar man sig kostnadsinbesparingar vad beträffar IT med hänseende till gemensamma teknologier, upphandlingar osv med de övriga ägarkunderna till ÅDA. I övergångsfasen och speciellt under utvecklandet och uppbyggnaden av ÅDA, kommer det dock att krävas investeringar vilket gör att under de första åren kommer IT-kostnaderna för ÅHS att öka, vilket är helt typiskt för dylik utveckling. För ÅHS gäller det att försäkra sig om att man har den kompetens som krävs för att ställa krav på ÅDA och den vägen se till att kostnadsinbesparingarna verkligen realiseras inom rimlig tid. För tillfället finns inte denna kompetens på ÅHS.

Vad beträffar kompetensen på ÅDA, har man ont om personal med kompetens på nya teknologier. För att ÅDA skall kunna svara på kommande krav från ÅHS och övriga kunder, verkar det vara nödvändigt att omskola, rekrytera eller köpa in rätt kompetens till ÅDA. Närmast, men inte endast, gäller detta förnyandet av teknologiplatformerna till färskare teknologi.

I dagens läge driftas medicinteknik helt på samma sätt som övrig IT inom ÅHS. Detta är vare sig ändamålsenligt eller kostnadseffektivt eftersom det inte går att anpassa livscykeln på medicintekniska system till motsvarande administrativa system. Detta leder till ett antal risker som är både relaterade till informationssäkerhet och kontinuitet. Det är helt generellt också viktigt att inom IT-driften starta med att segmentera nätverken så att man klart kan särskilja olika nivåer på funktionella behov, åtkomst och informationssäkerhet.

För ÅDA är det synnerligen viktigt att få noggrann och uppdaterad dokumentation på ÅHS systemomgivning inklusive systemens samverkan, integrationer och information systemen hanterar. För ÅDA är det vidare synnerligen viktigt att varje system är klassificerat med hänseende till t.ex. krav på kontinuitet. Det är på ÅHS ansvar som systemägare att denna information finns ÅDA tillhanda. På basen av denna information utarbetas antingen systemvisa SLA eller SLA beroende på nätverkssegment systemet befinner sig i (t.ex. skyddat segment, publikt segment, medicintekniskt segment, hög risk segment osv).

Se länkar till referensmaterial i bilaga A.

2.4 Sammanfattning av observationer

Ref.	Observation	Prioritet
1.	Otillräcklig insikt i IT-risker och otillräcklig riskanalys	Hög
12.	Osegmenterat och otillräckligt skyddat nätverk	Hög
10.	Informationssäkerhetskultur fattas	Hög
4.	Otillräckligt med resurser som har relevant IT-kompetens	Hög
5.	IT-strategikommitén och vårdsystemgruppen är inte aktiv och IT-säkerhetsgrupp fattas	Hög
6.	Observationer i granskningar blir obehandlade och åtgärdas inte	Hög
7.	Beskrivning över systemens samverkan fattas (informations- och integrationsarkitektur)	Hög
2.	Beskrivning över verksamheten fattas (verksamhetsarkitektur som IT-strategin anpassas till)	Medium
3.	Ingen tydlig IT-strategi finns definierad (IT-strategi som är anpassad till verksamhetsarkitekturen)	Medium
11.	Inga fastställda ramverk	Medium
14.	Kontinuitetsplanering fattas	Medium
8.	Beskrivning över systemens arkitektur fattas (systemarkitektur)	Låg
9.	Beskrivning över teknologi fattas (teknologiarkitektur)	Låg
13.	Medicinteknikens behov för drift och underhåll oklara	Låg

Helsingfors, 11.1.2016

KPMG Oy Ab

Leif-Erik Forsberg
Audit Director, CGR, OFR
KPMG Audit

Kristian Backman
Senior Manager, Certifierad säkerhetsarkitekt
KPMG Cyber Security

A Referensinformation

Ärendeområde	Användningsområde	Publicerat av	Länk
Föreskrift för plan på egenkontroll, informationssäkerhet THL	Egenkontroll av informationssäkerhet	THL/KanTa	http://www.thl.fi/attachments/oper/THL_foreskrift2_2015.pdf
IT-arkitektur och arkitektroller	Definition av olika arkitektroller	IASA Sverige	http://www.iasa.se/wp-content/uploads/2012/05/IASA-Arkitektroller-2012.pdf
Informationssäkerhet VAHTI	Modell för klassificering av system	VAHTI	https://www.vahtiohje.fi/c/document_library/get_file?uuid=ae185ae6-3e67-4a1d-ab23-6ec91049111b&groupId=10128
Informationssäkerhet VAHTI	Beskrivning av systemens samverkan	VAHTI	https://www.vahtiohje.fi/c/document_library/get_file?uuid=22de5fb1-65f8-41f8-bad7-fd07f2ddf3f8&groupId=10128
Business Model Canvas	Beskrivning av verksamheten	Wikipedia	https://en.wikipedia.org/wiki/Business_Model_Canvas
Business Capability Mapping	Beskrivning av verksamheten kopplad till underliggande system	Ulrich Kalex/The Open Group	http://www.opengroup.org/johannesburg2011/Ulrich%20Kalex%20-%20Business%20Capability%20Management.pdf
Informationssäkerhet HITRUST	HITRUST CSF Ramverk för informationssäkerhet	HITRUST Alliance	https://hitrustalliance.net/csf-assurance/
Helhetsarkitektur TOGAF	Ramverk för helhetsarkitektur, beskrivning av verksamheten, av systemarkitektur osv	The Open Group	http://www.opengroup.org/subjectareas/enterprise/togaf
Informationssäkerhet TOGAF	Ramverk för informationssäkerhet	The Open Group	http://www.opengroup.org/subjectareas/security
HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities	Referensinformation om informationssäkerhet inom hälso- och sjukvård	KPMG	https://advisory.kpmg.us/content/dam/kpmg-advisory/PDFs/ManagementConsulting/2015/KPMG-2015-Cyber-Healthcare-Survey.pdf