Myndigheten för samhällsskydd och beredskap

Uppföljning av informationssäkerhet i vården

Vårdgivarnas rapportering av kontroller, risker och incidenter

MSB:s kontaktperson:
Tom Andersson, 010-240 42 10

Publikationsnummer: MSB820 – mars 2015
ISBN 978-91-7383-544-2

Innehållsförteckning

1. Sammanfattning 5
2. Bakgrund 10
2.1 Kartläggningens syfte 10
2.2 Regelverk 15
3. Undersöknings- och analysmetoder 18
3.1 Dokumentation 18
3.1.1 Nyhetsmedier, forskning och utredningar 18
3.1.2 Verksamhetsrapporter och klagomål 20
3.2 Enkätundersökning 25
3.2.1 Deltagare och design 26
3.2.2 Former för resultatredovisning 28
3.3 Metodkritik 28
4. Resultat 30
4.1 Externa perspektiv 30
4.1.1 Nyhetsbilder 30
4.1.2 Nationella granskningar 32
4.1.3 Forskningsstudier 34
4.2 Vårdgivarnas uppföljning 38
4.2.1 Landstingens riktlinjer och årsrapporter 38
4.2.2 Andra verksamhetsrapporter från landsting 40
4.2.3 Kommunernas riktlinjer och rapporter 42
4.2.4 Revisioner 45
4.2.5 Avvikelser i vårdverksamhet 46
4.2.6 Orsaks- och händelseanalyser 49
4.2.7 It-incidenter 51
4.2.8 Klagomål från patienter 52
4.3 Enkätresultat 54
4.3.1 Bakgrundsprofil 54
4.3.2 Riktighet 55
4.3.3 Konfidentialitet 55
4.3.4 Tillgänglighet 56
4.3.5 Analys 56
5. Diskussion 59

Bilaga 1 Enkätfrågor och svar (LSF) 62

Bilaga 2 Enkätfrågor och svar (SCB) 69

Bilaga 3 Forskningspublikationer om vårdrelaterad informationssäkerhet 76

Bilaga 4 Avhandlingar av svenska forskare om informationssäkerhet (LIBRIS) 79

Bilaga 5 Årsrapport – Jämtlands läns landsting 85

Bilaga 6 Årsrapport – Landstinget i Uppsala län 89

Bilaga 7 Egenkontroll 2014 – Landstinget i Uppsala län 95

Bilaga 8 Checklista egenkontroll – Landstinget i Uppsala län ... 99

Bilaga 9 Fokusområden 2014 – Landstinget i Uppsala län 101

Bilaga 10 Utdrag ur Västra Götalandsregionens säkerhetsredovisning 2013..... 103

Bilaga 11 Enkätfrågor i Västra Götalandsregionens säkerhetsredovisning 106

Bilaga 12 Internkontroll – Skellefteå kommun 109

Bilaga 13 Urval av revisioner 113

Bilaga 14 Lathund för informationssäkerhet – Landstinget i Jönköpings län..... 114

1. Sammanfattning

11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet […] I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer.

Förordning (2008:1002) med instruktion för
Myndigheten för samhällsskydd och beredskap (MSB)

Denna rapport sammanfattar en kartläggning av vårdgivarnas uppföljande arbete på informationssäkerhetsområdet. Den omfattar framför allt arbetet i landsting och kommuner, men även privata vårdgivare. Kartläggningen utgår från Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14). I föreskriften formuleras informationssäkerhet som en komponent i kvalitetsledningssystemet. Fokus i denna kartläggning ligger på rapportering av verksamhetskontroller, risker och incidenter (avvikelser) avseende informationssäkerhet i vårdsystem och dokumentation.

I SOSFS 2008:14 ställs krav på uppföljning och rapportering. Dessa är viktiga utgångspunkter för kartläggningen. Än viktigare är att *regelbunden uppföljning och systematisk rapportering är nödvändiga komponenter för effektiv styrning*. Det gäller oavsett lagar och föreskrifter. Kartläggningen tar därför också formen av en utvärdering av ledning och styrning på området, överensstämmelsen mellan regelverk och riktlinjer, rutiner och praxis samt mål och resultat. Följande information utgör underlag för arbetet:

- Granskningar, revisioner och rapporter på området som finns på hemsidor hos myndigheter, landsting och kommuner.
- Nyhetsartiklar och forskningspublikationer på området som finns i internationella och svenska databaser.
- Förfrågan till alla landsting och kommuner om följande handlingar:
    - senaste årsrapport avseende informationssäkerhet enligt SOSFS 2008:14
    - informationssäkerhetspolicy/riktlinjer
    - diarieförda granskningar, revisioner och rapporter om it- och informationssäkerhet för perioden 2011–2013
    - patientsäkerhetsberättelse 2013.
- Förfrågan till alla landsting om följande handlingar:
    - regional årsredovisning 2013
    - patientnämndens årsberättelse 2013
    - dokumentation om system för hantering av avvikelser respektive it-incidenter
    - statistikrapport om avvikelser respektive it-incidenter 2013.
- Förfrågan till ett urval av kommunala social- och omsorgsnämnder om verksamhetsplanering och uppföljning av informationssäkerhet.

- Enkät ”Säker vårddokumentation” till medlemmar i Läkarsekreterares och Sjukvårdsadministratörers Förbund (LSF).
- Enkät ”Säker vårddokumentation” till ett urval sjuksköterskor i SCB:s yrkesregister.

Många och stora satsningar på e-hälsa, it och digital teknik i vården har gjorts det senaste decenniet. De har inte åtföljts av lika många granskningar av effekter och resultat på vården och patientsäkerheten.[1] Det görs utvärderingar av enskilda kvalitets- och säkerhetsfrågor, brister i tillgänglighet och funktionalitet samt it- och systemstöd i användarperspektiv.[2,3] Informationshantering på läkemedelsområdet är till exempel ett prioriterat område i både forskning och hos vårdgivare.[4,5,6] Ett annat viktigt exempel är det nationella kontrollarbete som bedrivs av Inera AB genom årliga revisioner av vårdgivarnas användning av nationella e-tjänster, HSA och SITHS-kort.[7] Dessa kontrollåtgärder förblir dock avgränsade och begränsade. Övergripande frågor om styrning, kvalitetsledning och säkerhetsarbete avseende vårdinformation förblir mer eller mindre obesvarade, trots att just svag styrning går som en röd tråd genom nationella granskningar.[8,9,10]

---

[1] Black AD, Car J, Pagliari C, Anandan C, Cresswell K, Bokun T, McKinstry B, Procter R, Majeed A, Sheikh A. The impact of eHealth on the quality and safety of health care: a systematic overview. PLoS Med. 2011 Jan 18;8(1).
[2] Störande eller stödjande? Om eHälsosystemens användbarhet 2013. Slutrapport från projektet eHälsosystemens användbarhet. Vårdförbundet.
[3] Hedström, Karin, Jäger, Kerstin, Krasnizi, Hanife, Linderoth, Henrik, Nohlberg, Marcus, Persson, Anne & Åhlfeldt, Rose-Mharie, Vårdens framtida informationssystem – Vision i form av en demonstrator. Slutrapport. Skövde 2010.
[4] Ekedahl A, Tärning E, Rutberg H, et al. Mycket vanligt med fel i läkemedels- och receptlistorna. Patientuppgifter om ordinationer jämförda med journaler och receptdatabas. Läkartidningen. 2012;109:1024-7. http://www.lakartidningen.se/Functions/OldArticleView.aspx?articleId=18237
[5] Kontinuitetshantering i praktiken. MSB. Rapport 657. 2014: https://www.msb.se/RibData/Filer/pdf/27346.pdf
[6] Hammar T. (2014) eMedication – improving medication management using information technology. Institutionen för medicin och optometri, Linnéuniversitetet, Kalmar. Linnaeus University Doctoral Dissertations No. 76/2014. ISBN: 978-91-87925-15-3
[7] Information och rapporter avseende revisioner av HSA och SITHS-kort finns på Ineras hemsida: http://www.inera.se/TJANSTER--PROJEKT/HSA/HSA-regelverk-och-riktlinjer/Revisioner-av-SITHS-och-HSA/.
[8] Socialstyrelsens verksamhetstillsyn av vårdgivarens informationssäkerhet 2011: http://www.socialstyrelsen.se/pressrum/nyhetsarkiv/it-problemskaparriskerforpatienter
[9] Datainspektionens granskning av behörighets- och åtkomstkontroll i kommunal hälso- och sjukvård: http://www.datainspektionen.se/press/nyheter/2014/granskning-klar-av-kommunal-halso-och-sjukvard/
[10] Ineras årliga revisioner av SITHS och HSA: http://www.inera.se/TJANSTER--PROJEKT/SITHS/SITHS-regelverk-och-riktlinjer/Revisioner-av-SITHS-och-HSA/

Även nyhetsrapportering och forskning är begränsade till mängd och perspektiv. Trenden i svenska nyhetsmedier kan sammanfattas som ett svagt växande intresse för integritetsrisker och dataintrång i journalsystem och nätverk. Trenden i internationell forskning är ett växande intresse för it-stöd i vården, men utan att informationssäkerhetsfrågor följer med. Den forskning som bedrivs om informationssäkerhet lägger tonvikten på frågor om tekniska skydd mot obehörig åtkomst till vårdsystem och dataintrång snarare än informationshantering i ett verksamhetsperspektiv. En handfull forskare inriktar sig på informationssäkerhet i vården. Dessa är i högre grad verksamhetsanknutna, men inriktade på integritetsfrågor samt it- och systemstöd snarare än verksamhetsstyrning.

Den offentliga bilden av informationssäkerhet är snäv och otydlig, ett växande hot om dataintrång. Det präglar även vårdgivarnas verksamhetsrapportering. I deras riktlinjer är det vanligt att ställa krav på anställda att snabbt rapportera it-incidenter till chefer. I regel ställs inga krav på sammanställning och rapportering av informationssäkerhetsfrågor från chefer till ledning. Det finns dock undantag, till exempel kravet på rapportering enligt SOSFS 2008:14. Sex landsting (6 av 21 svar) hänvisar explicit eller implicit till kravet i egna riktlinjer på området. Av de policyer eller riktlinjer som landets kommuner har delgett, 107 stycken, nämns inte kravet någon gång. Däremot finns det fall där kommunens socialnämnd eller omsorgsförvaltning har egna riktlinjer för dokument- eller informationshantering där kravet nämns.

Enligt SOSFS 2008:14 ska vårdgivare upprätta en årsrapport om förebyggande informationssäkerhetsinsatser. Efter begäran har ett av tre landsting delgett en årsrapport med en disposition i enlighet med föreskriften. Ytterligare fyra landsting har åberopat eller delgett årsrapporter som kraftigt avviker från föreskriften. Inga kommuner har så gjort. Enligt rekommendation i Handbok till SOSFS 2008:14 bör allvarliga informationssäkerhetsincidenter redovisas i samma årsrapport. Två landsting har så gjort, Jämtlands läns landsting och Landstinget i Uppsala län. Dessa årsrapporter återfinns i bilagor (5–9). Årsrapporten från Landstinget i Uppsala län är omfångsrik, men tjänar som ett viktigt exempel på behovet av att knyta samman central rapportering och lokal egenkontroll. Ansatsen till helhetsperspektiv är lovvärd. Generellt råder det annars brist på årlig rapportering. Flera kommuner har på telefon eller i brev uppgett att de inte kände till kravet på rapportering. I policyer nämns vikten av regelbunden uppföljning, men i praktiken uteblir det. Vissa kontrollpunkter finns i vårdgivarnas internkontroll, men de är sällsynta och sporadiska. I sin helhet kan resultatet bara tolkas som ett tecken på att informationssäkerhet är en lågprioriterad fråga för vårdgivarna.

Sexton landsting och en av sex kommuner (47) har delgett granskningar av it- och informationssäkerhet under perioden 2011–2014 samt översyner och revisioner. Flertalet är inriktade på it- och systemsäkerhet. I liten utsträckning berörs frågor om verksamhetsstyrning och kvalitetsledning av informationshantering och vårddokumentation, till exempel genom

informationsklassning samt risk-, kontinuitets- och incidenthantering. Frågor om säkerhetskultur berörs inte i något fall.

Enligt SOSFS 2008:14 ska informationssäkerhet vara en del av vårdgivarens kvalitetsledningssystem. Det omfattar bland annat kvalitetsgranskningar av vårddokumentation och logguppföljning. Patientsäkerhetsberättelser är den enda tvingande kvalitetsredovisningen för vårdgivare. Det är inget krav på att inkludera informationssäkerhetsfrågor, men det är ett rimligt val om SOSFS 2008:14 är utgångspunkten för informationssäkerhetsarbetet.

I patientberättelserna år 2013 nämner närmare ett av fyra landsting (5 av 21) samt en av fem kommuner (45 av 224) resultat av kvalitetsgranskning i någon form, i flertalet fall begränsade granskningar, till exempel riktighet i läkemedelslistor. Inget landsting tar upp några resultat av logguppföljning, även om ett par nämner att det görs som rutin. Två av femton kommuner (30 av 224) tar upp logguppföljning. Resultatredovisningen är mycket sparsam. Inte någon vårdgivare har delgett en utvärdering av logguppföljning.

En splittrad styrning framträder som tydligast i uppföljningen av avvikelser, fel och klagomål på informationssäkerhetsområdet. Rapportering av problem görs i olika system och delsystem för hantering av avvikelser (vårdverksamhet), incidenter (it och medicinteknik) och klagomål (patienter och anhöriga). Roller och ansvar saknas generellt för samordning. Informationssäkerhetsfrågor och problem tolkas inte sällan i tekniska termer, *dataintrång och driftstörningar i journalsystem*, varmed frekvenser av avvikelser och klagomål (andelar) kan ses som låga (någon procent). När informationssäkerhet uppfattas som en fråga om informationshantering generellt kan incidentfrekvenser växa till 20 % och mer. Variationen i rutiner och praxis hos vårdgivare är stor.

Bristande helhetssyn på kvalitets- och säkerhetsfrågor i informationshantering, vårdsystem och dokumentation bekräftas i en enkät till vårdpersonal, dels till medlemmar i Läkarsekreterares och Sjukvårdsadministratörers Förbund (LSF), dels till sjuksköterskor i ett urval från Statistiska centralbyråns (SCB) yrkesregister. MSB administrerade den första versionen i samarbete med LSF. Den resulterade i 753 svar från 1 450 medlemmar (52 %). SCB administrerade den andra versionen med drygt 2 700 svar (57 %).

- Fler än 1 av 3 sjuksköterskor samt närmare 1 av 5 LSF-medlemmar uppger att felaktig vårddokumentation har varit en patientsäkerhetsrisk på arbetsplatsen. Cirka 1 av 3 har erfarit kvalitetsgranskning av journalföring.
- Fler än 1 av 4 sjuksköterskor och närmare 1 av 10 LSF-medlemmar uppger att otillgänglig vårddokumentation har varit en patientsäkerhetsrisk. Färre än 1 av 10 har övat reservrutiner för journalföring.
- Cirka 1 av 10 uppger att obehöriga har tagit del av vårdinformation. Cirka 1 av 3 sjuksköterskor och cirka 2 av 3 LSF-medlemmar har erfarit åtkomstkontroll av patientjournaler på arbetsplatsen.

- Erfarenhet av kontrollinsatser och avvikelser i informationshantering beror mer på ledningsansvar och utbildning i informationssäkerhet än på kategori av arbetsplats och arbetsgivare.
- LSF-medlemmar med ledningsansvar uppger förekomst av kontroller och avvikelser i högre grad än sjuksköterskor med ledningsansvar.

LSF-medlemmar har vårddokumentation som huvudsaklig arbetsuppgift. De kan därför potentiellt utveckla tydligare ansvar och engagemang för kvalitets- och säkerhetskontroller av vårddokumentation. De som har svarat på enkäten har dessutom lång arbetslivserfarenhet. Den grupp som har arbetat i minst 10 år i vården utgör 86,5 % av de svarande, jämfört med 74 % för sjuksköterskor.

Sammanfattningsvis bekräftar enkäten den generella bilden i kartläggningen. *Regelbunden uppföljning och systematisk rapportering av kontroller, risker och incidenter saknas i stor utsträckning*. Det gör det i princip omöjligt att skapa gemensamma nationella lägesbilder av kvalitet och säkerhet avseende vårdsystem och dokumentation. Till viss del har Socialstyrelsen, numera Inspektionen för vård och omsorg (IVO), uppmärksammat problemet i en egeninitierad tillsyn 2011. Fokus låg dock på systemsäkerhet, inte på kvalitets- och säkerhetskontroller eller risker och incidenter i informationshantering.

En förklaring till dagens situation är ansvars- och rollfördelningar som sprider ut kvalitets- och säkerhetsfrågor utan tydliga mandat för samordning. En annan förklaring är dagens fokus på it- och systemutveckling som överskuggar frågor om kvalitet och säkerhet i vårdsystem och dokumentation. Det saknas en förståelse för risk- och kontinuitetshantering av verksamhetsinformation med utgångspunkt i mål, analyser och informationsklassning.

2. Bakgrund

2.1 Kartläggningens syfte

11 a § Myndigheten ska stödja och samordna arbetet med samhällets informationssäkerhet samt analysera och bedöma omvärldsutvecklingen inom området. I detta ingår att lämna råd och stöd i fråga om förebyggande arbete till andra statliga myndigheter, kommuner och landsting samt företag och organisationer.

Förordning (2008:1002) med instruktion för
Myndigheten för samhällsskydd och beredskap (MSB)

Vårdgivaren ansvarar för att ledningssystemet för kvalitet och patientsäkerhet innehåller en dokumenterad informationssäkerhetspolicy. Vårdgivaren ska också säkerställa att ledningssystemet omfattar de rutiner som behövs för att uppfylla kraven på informationssäkerhet.

Handbok till Socialstyrelsens föreskrifter (SOSFS 2008:14) om
informationshantering och journalföring i hälso- och sjukvården[11]

I syfte att skapa en lägesbild av informationssäkerhetsarbetet i vården har MSB genomfört en kartläggning av kontrollarbetet. Med kontrollarbete avses här ”systematiska och regelbundna kvalitets- och säkerhetskontroller samt rapportering av kontrollresultat”. Sådan uppföljning och rapportering speglar kanske mer än något annat organisationens säkerhetskultur och ledningens delaktighet i säkerhetsarbetet. En förståelse av hur kontrollarbetet fungerar i praktiken är en förutsättning för att utvärdera informationssäkerhetsrisker, åtgärder och incidenter på området.

Definitioner[12]

Informationssäkerhet: *Tillstånd som innebär skydd med avseende på konfidentialitet, riktighet, tillgänglighet och spårbarhet hos information.*

---

[11] Citat från pdf-version 2015-01-04 av handbok till Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården (2009:12):
http://www.socialstyrelsen.se/regelverk/handbocker/handbokominformationshanteringochjournalforing

[12] Definitionen av informationssäkerhet återfinns i Vägledning – informationssäkerhet i upphandling, Myndigheten för samhällsskydd och beredskap (MSB) 2013:39.
https://www.msb.se/RibData/Filer/pdf/26589.pdf
Övriga definitioner: Kommunens informationssäkerhet – en vägledning. Myndigheten för samhällsskydd och beredskap (MSB) 2012:508.
https://www.msb.se/RibData/Filer/pdf/26420.pdf

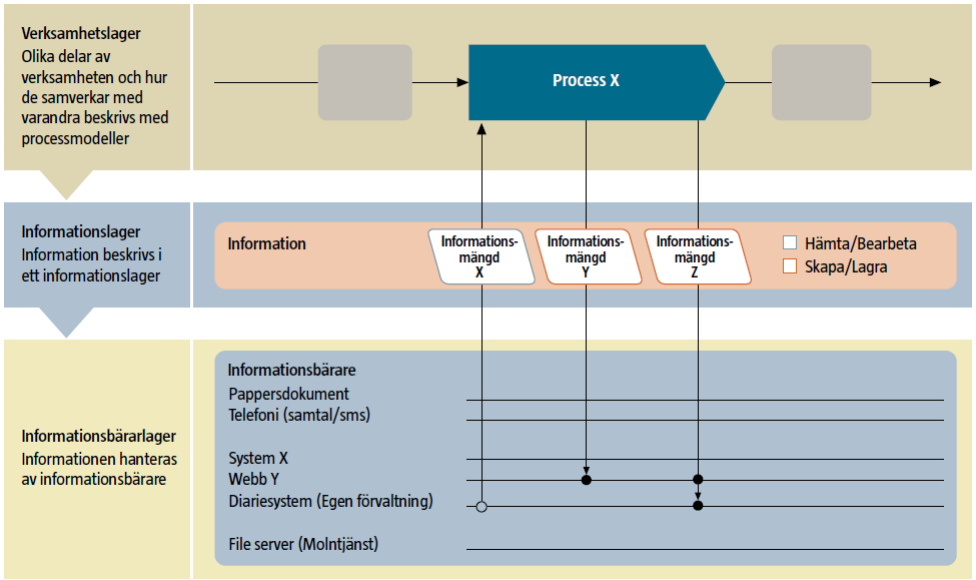
Tillgänglighet: Att information är tillgänglig i förväntad utsträckning och inom önskad tid.

Konfidentialitet: Att den inte i strid med lagkrav eller lokala överenskommelser/riktlinjer tillgängliggörs eller delges obehörig.

Riktighet: Att den skyddas mot oönskad och obehörig förändring eller förstörelse.

Spårbarhet: Att i efterhand entydigt kunna härleda specifika aktiviteter eller händelser till ett identifierat objekt eller användare (vem, vad, när).

Informationssäkerhet handlar om att uppfylla en uppsättning normer, krav och mål avseende *tillgänglighet, konfidentialitet, riktighet och spårbarhet* i informationshantering, system och infrastruktur. Dessa följer av externa och interna krav, lagar, standarder, egna säkerhets- och kvalitetskrav med mera. I praktiken måste organisationer utveckla och specificera normer för sin verksamhet. En viktig del i det arbetet är att genomföra så kallad informationskartläggning och klassning, dvs. att identifiera och värdera information i verksamhetsprocesser (figur 1) samt därefter specificera de externa och interna skyddskrav som gäller.



Figur 1. Illustration av processorienterad informationskartläggning
I ett processperspektiv är information – uppgifter och dokument i analoga medier eller digitala system – komponenter i verksamhetsprocesser. Informationssäkerhet handlar om att styra informationshantering med avseende på externa och interna säkerhets- och kvalitetskrav, *konfidentialitet, riktighet, tillgänglighet och spårbarhet*. I praktiken innebär det både förebyggande åtgärder, risk- och kontinuitetshantering, och insatser i skarpt läge, incidenthantering.[13]

[13] Källa: Vägledning för processorienterad informationskartläggning, Myndigheten för samhällsskydd och beredskap (MSB) och Riksarkivet, 2012:493; pdf-version: https://www.msb.se/RibData/Filer/pdf/26410.pdf.

I it-beroende verksamheter går det lätt och snabbt att identifiera elektroniska informationssystem och nätverk som kritiska resurser. Det kan förefalla som om all viktig och känslig information ligger i digitala system och nätverk, varför informationssäkerhet kan uppfattas som detsamma som system- eller it-säkerhet. Å ena sidan innebär det att samma kvalitets- och skyddskrav ställs på all information i ett och samma system eller nätverk. Å andra sidan innebär det att inga eller andra krav ställs på informationshantering utanför system och nätverk, trots att det kan vara samma information som cirkulerar. Det innebär oklar verksamhetsstyrning av informationshantering.

Utgångspunkten för denna kartläggning är att informationssäkerhet börjar och slutar med verksamhetsstyrning av information (informationsstyrning), genom kravställning på och uppföljning av verksamhetskritisk information. Styrning omfattar i princip manuell och automatisk informationshantering, processer, system och teknik, försörjning och förädling, bearbetning, lagring och spridning av information, inom och mellan verksamheter.

Det traditionella säkerhetsperspektivet handlar om att skydda information från obehörig åtkomst och påverkan samt säkra tillgång för behöriga personer. Det är centrala frågor på informationssäkerhetsområdet. Samtidigt kan frågorna inte vara utgångspunkten för informationsstyrning och därmed inte heller för styrningen av informationssäkerhet. Utgångspunkten är verksamhetskrav och behovet av extern och intern samordning av informationskrav. De fyra säkerhetskraven på *konfidentialitet*, *riktighet*, *tillgänglighet* och *spårbarhet* gränsar till exempel till kvalitetskrav, *korrekthet*, *aktualitet* och *fullständighet*.[14,15] Överlappande krav kan och bör inte specificeras oberoende av varandra. Viken av samordnad styrning är ett av skälen till varför informationssäkerhetskrav, *konfidentialitet*, *riktighet*, *tillgänglighet* och *spårbarhet*, i denna kartläggning betraktas som en fråga om både kvalitet och säkerhet. Ett annat skäl är att riskerna på området inte erkänner några absoluta gränser mellan olika typer av risker, till exempel mellan kvalitets- och säkerhetsrisker.

Riskhantering är en viktig del av förebyggande kvalitets- och säkerhetsarbete, utöver ledning, ansvars- och rollfördelningar samt informationsklassning. I det ligger att genomföra riskanalyser, dvs. värdering av nya risker, omvärdering av kända risker och åtgärdsprioriteringar. I ett avgränsat sammanhang, inom en bransch eller profession, kan det te sig enkelt att urskilja och särskilja en typ av risk från en annan. I praktiken är risker sammansatta och överlappande.

---

[14] Wang, R. Y., & Strong, D. M. (1996). Beyond accuracy: What data quality means to data consumers. Journal of management information systems, 5-33.
[15] Lee, Y. W., Strong, D. M., Kahn, B. K., & Wang, R. Y. (2002). AIMQ: a methodology for information quality assessment. Information & management, 40(2), 133-146.

En kvinna opererade en tå. Vid utskrivningssamtalet gavs ingen information om stygnen. Efter några veckor kontaktade kvinnan specialistmottagningen med frågor gällande detta. Sjuksköterskan blev osäker eftersom hon inte hittade operationsberättelsen. Hon gav rådet att klippa i ena änden och dra, då ortopederna brukar sy med resorberbar tråd. När kvinnan gjorde så gick tråden av. Två veckor senare kontaktade hon mottagningen igen, fortfarande fanns ingen operationsberättelse. När såret blev infekterat gick kvinnan till husläkaren som öppnade såret och ordinerade antibiotika. Det visade sig att såret sytts med icke resorberbar tråd. Mottagningen uppgav att de trodde att kvinnan önskade information om hur hon själv skulle ta bort stygnen. Hon fick inte klart besked om hur det hade sytts. Alla patienter informeras att stygnen ska tas hos distriktssköterska.[16]

Berättelsen är hämtad från patientnämndens årsrapport 2013 i Stockholms läns landsting. Är detta en informationssäkerhetsfråga? För MSB är svaret ja, men det är inte otvetydigt varför så är fallet. En operationsberättelse saknas. Var är den? En eller flera informationsrutiner har inte följts. Vilka? Felaktiga uppgifter cirkulerar. Var, när och hur uppstod de? Frågorna får illustrera att riskhantering av information är förenat med osäkerhet. Till sin natur ligger informationssäkerhetsrisker nära andra verksamhetsrisker, generella informations- och kommunikationsrisker. Inte sällan är det svårt att skilja en typ av risk från en annan, men det är en del av verksamhetens säkerhets- och kvalitetsarbete att göra det, att reda ut potentiella förluster och faktiska skador, orsaker och åtgärder.

Patienten har inkommit med synpunkter på att obehöriga har varit inne i tidigare spärrad journal. Spärren har av okänd anledning försvunnit. Patienten har själv diskuterat problemet med berörd personal som arbetar med journalsystemet, utredning pågår. Patienten mår mycket dåligt av det som inträffat och vill söka ersättning från Patientförsäkringen. Yttrande har inkommit från enhetschef som förklarar att ingen begäran om spärr av journal finns.[17]

Patienten genomgick utredning som ledde fram till diagnosen Borderline och remiss skickades för DBT-behandling (dialektisk beteendeterapi). När patienten inte fick någon återkoppling på den skickade remissen kontaktades öppenvården som informerade om att den avslagits, eftersom underlag saknades vid remittering. När man kontrollerade patientens journal fanns ingen utredning dokumenterad och hon fick besked om att en ny utredning måste göras. Allt detta försenade möjligheten för behandling.[18]

Berättelserna är hämtade från patientnämndernas verksamhetsberättelser 2013 i Landstinget i Uppsala län respektive Örebro läns landsting. Även dessa väcker frågor om informationssäkerhet, inte minst om *spårbarhet*. När viktig

[16] Patientnämnden Stockholms län landsting. Årsrapport 2013.
[17] Patientnämnden Landstinget i Uppsala län. Verksamhetsberättelse 2013.
[18] Patientnämnden Örebro läns landsting. Verksamhetsberättelse 2013.

eller känslig information plötsligt försvinner är det centralt att kunna rekonstruera händelser och information. Berättelserna väcker även frågor om kontinuitetshantering och incidenthantering, reservrutiner och system. Hur kan vårdens informationshantering göras mindre sårbar och mer robust? Hur länge fungerar vården i händelse av större och mer långvariga störningar i verksamhetens informationshantering?

Informationssäkerhet börjar med det dagliga kvalitets- och säkerhetsarbetet. Det handlar inte bara, eller ens först och främst, om åtgärder och insatser för nödsituationer och katastrofer. Det handlar om att skydda all slags information som kan orsaka verksamhetsförluster. Det innebär generell riskhantering, ett dagligt förebyggande arbete för att möta alla slags hot och faror. I det avseendet kan informationssäkerhet jämföras med vårdens smittskyddsarbete. Det dagliga arbetet inriktas på riskhantering, hygien, identifiering, isolering och hantering av enskilda fall. Det är grunden för hantering av akuta, allvarliga och större utbrott av infektionssjukdomar. Det senare drar till sig offentliga nyhetsmediers uppmärksamhet, men representerar inte det generella arbetet med smittskydd. Så är det även med informationssäkerhet. Det förebyggande arbetet handlar inte bara om att förbereda sig för säkerhetskriser, utan att hantera informationsbrister på bred front.

I denna rapport ligger fokus på vårdgivarnas uppföljning och rapportering av kvalitets- och säkerhetskontroller, risker och incidenter. Det går givetvis inte att ge något uttömmande svar på hur uppföljning och rapportering ser ut eller går till. Det är ett arbete som tar många former och uttryck, mer eller mindre formella. För regelbunden uppföljning och systematisk rapportering är det dock viktigt med en viss grad av formalisering. Följande frågor har därför fått vägleda kartläggningen:

Vilken officiell rapportering finns av vårdens informationssäkerhet?

Vad säger rapporteringen om kontrollmetoder och resultat?

Vad säger rapporteringen om risker och incidenter?

Varierande informationskällor och perspektiv är ett nödvändigt, om inte tillräckligt, villkor för en rättvisande lägesbild. I princip kan kartläggningen därför omfatta allt offentligt underlag som belyser hur vårdens uppföljning av informationssäkerhetskrav går till i praktiken. I praktiken är valet av källor en fråga om tid och resurser.

Denna kartläggning vilar på tre typer av underlag: (1) externa rapporter (oberoende granskningar, forskning och nyhetsrapportering), (2) verksamhetsrapporter från vårdgivare samt (3) enkätundersökningar bland vårdpersonal. Dessa tre underlag kan ses som tre nivåer på uppföljning och rapportering i vården, dvs. samhälle, ledning och medarbetare. En närmare beskrivning följer i ett senare avsnitt. Först följer en sammanfattning av regelverket av relevans för vårdgivarnas uppföljning.

2.2 Regelverk

Syftet med denna kartläggning är att skapa en lägesbild av vårdens uppföljning och rapportering av kvalitets- och säkerhetskontroller, risker och incidenter på informationssäkerhetsområdet. För ändamålet är det centralt att klargöra om och hur dagens regelverk ställer krav på uppföljning och rapportering. Motivet är inte att utvärdera efterlevnad av lagar. Däremot är *krav på uppföljning och efterlevnad av dessa krav* en del av lägesbilden.

Uppföljning och rapportering i hälso- och sjukvård regleras genom riktlinjer på alla organisationsnivåer – nationella, regionala och lokala – med såväl generella som specifika riktlinjer – generella riktlinjer för hälso- och sjukvård samt specifika riktlinjer för informationshanteringen på området. På nationell nivå finns Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14) som ställer krav på uppföljning och rapportering inom ramen för vårdgivarens ledningssystem för kvalitet och patientsäkerhet. Patientdatalagen (2008:335) ställer krav på skydd av personuppgifter, men säger inget om styrning och uppföljning, annat än att vissa generella ansvar följer med behandlingen av personuppgifter, samt att åtkomst till patientuppgifter ska dokumenteras och kontrolleras.

Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården (SOSFS 2008:14)

2 kap. Ansvar för informationssäkerhet

1 § Vårdgivaren ska ge direktiv och säkerställa att det i verksamhetens ledningssystem för kvalitet och patientsäkerhet finns en dokumenterad informationssäkerhetspolicy.

3 § Vårdgivaren ska 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

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

19 § Verksamhetschefen ska inom ramen för vårdgivarens ledningssystem för kvalitet och patientsäkerhet ansvara för

- *uppföljning av patientuppgifternas kvalitet och ändamålsenlighet [...] och*
- *uppföljning av informationssystemens användning genom regelbunden kontroll av loggarna.*

Kravet på en årlig rapport från informationssäkerhetsansvariga till vårdgivaren gäller uppföljning av enskilda granskningar, analyser och åtgärder. Det är inte ett krav på systematisk och regelbunden uppföljning. Om inga granskningar, analyser eller åtgärder görs föreligger det inte heller några krav på uppföljning.

I ett riskperspektiv är frånvaro av kontrollarbete en lika viktig fråga som att åtgärder faktiskt vidtas. Det är en svaghet i uppföljning som förstärks av att föreskrifterna inte heller ställer krav på rapportering av incidenter, även om Socialstyrelsens handledning på området rekommenderar det.[19]

Utöver årlig rapportering ställer föreskrifterna krav på uppföljning av kvalitet hos patientuppgifter och logguppföljning, användning av informationssystem. I SOSFS 2008:14 formuleras inga regelrätta krav på rapportering. Samtidigt är det tydligt att informationssäkerhetsarbetet är en del av kvalitetsarbetet och att verksamhetschefen har ansvar för dess ledning och uppföljning. Det innebär att regelverket för kvalitetsledning är tillämpligt på informationssäkerhetsarbetet. Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete (SOSFS 2011:9) är därmed av direkt relevans för frågor om rapportering på området.

5 kap. Systematiskt förbättringsarbete

6 § Inkomna rapporter, klagomål och synpunkter ska sammanställas och analyseras för att vårdgivaren eller den som bedriver socialtjänst eller verksamhet enligt LSS ska kunna se mönster eller trender som indikerar brister i verksamhetens kvalitet.

7 kap. Dokumentationsskyldighet

1 § Arbetet med att systematiskt och fortlöpande utveckla och säkra verksamhetens kvalitet ska dokumenteras.

Allmänna råd

Vårdgivare som omfattas av 1 kap. 1 § 1 och 2 eller den som bedriver socialtjänst eller verksamhet enligt LSS bör med dokumentationen som utgångspunkt varje år upprätta en sammanhållen kvalitetsberättelse av vilken det bör framgå

- *hur arbetet med att systematiskt och fortlöpande utveckla och säkra verksamhetens kvalitet har bedrivits under föregående kalenderår,*
- *vilka åtgärder som har vidtagits för att säkra verksamhetens kvalitet, och*
- *vilka resultat som har uppnåtts.*

Berättelsen bör ha en sådan detaljeringsgrad att det går att bedöma hur arbetet med att systematiskt och fortlöpande utveckla och säkra kvaliteten har bedrivits i verksamhetens olika delar, och att informationsbehovet hos externa intressenter tillgodoses.

Berättelsen bör hållas tillgänglig för den som önskar ta del av den.

---

[19] Handbok till SOSFS 2008:14 (sida 24): ”Det är lämpligt att den ansvarige samlar in och rapporterar de IT-incidenter som har inträffat under året. Formen för rapporteringen får anpassas till verksamhetens utformning och storlek”.

2 § Enligt 3 kap. 10 § patientsäkerhetslagen (2010:659) ska vårdgivaren senast den 1 mars varje år upprätta en patientsäkerhetsberättelse.

3 § Patientsäkerhetsberättelsen ska ha en sådan detaljeringsgrad

- *att det går att bedöma hur det systematiska patientsäkerhetsarbetet har bedrivits i verksamhetens olika delar, och*
- *att informationsbehovet hos externa intressenter tillgodoses.*

Inom ramen för kvalitetsledningssystem och patientsäkerhetsarbetet finns krav på uppföljning och åtgärder avseende verksamhetsrisker, avvikelser och klagomål. Dessa ska dokumenteras enligt vårdgivarens riktlinjer och rutiner för kvalitetsarbetet. Föreskrifterna kan därmed sägas ge stöd för en sammanhållen uppföljning och rapportering av informationssäkerhetsfrågor inom ramen för kvalitetsarbetet. Kraven på kvalitetsuppföljning är dock rubricerade som ”allmänna råd”, till skillnad från patientsäkerhetsarbetet där kravet på en årlig berättelse är explicit. De allmänna råden manar till helhetssyn, systematik och regelbundenhet, men i princip är vårdgivaren helt fri att utforma riktlinjer för uppföljning och rapportering av kvalitetsarbetet.

Socialstyrelsens föreskrifter utgår från en rad lagar och förordningar som inte diskuteras närmare här. Nämnda föreskrifter är tillräckliga för att belysa att regelverket ger utrymme för tolkning och variation i vårdens styrning och uppföljning av informationssäkerhetsarbetet. De kan inte sägas motivera till systematik och regelbundenhet i planering och rapportering. Ansvaret för att leda och samordna säkerhets- och kvalitetskrav på området, för hantering av risker, avvikelser och incidenter, lämnas obesvarat. Det är några exempel på oklarheter som kan bidra till oklar styrning och uppföljning på området.

3. Undersöknings- och analysmetoder

Rapporten bygger på två slags fakta- och informationsunderlag, dels offentliga rapporter om informationssäkerhetsarbetet i vården, dels en enkätundersökning bland vårdpersonal. Offentliga rapporter representerar samhällets, forskarsamhällets och vårdgivarnas perspektiv. De sistnämnda omfattar framför allt sjukvårdshuvudmän, landsting och kommuner, även om visst material även kommer från lokala, enskilda vårdgivare. För att urskilja mönster i verksamhetsrapporter används innehållsanalys, dvs. analyser av ämnesstrukturer och ordfrekvenser. Enkäterna representerar medarbetarnas perspektiv, även hos privata vårdgivare. Beskrivande statistik sammanfattar resultat. Vissa enklare statistiska analyser fördjupar beskrivande delar.

3.1 Dokumentation

3.1.1 Nyhetsmedier, forskning och utredningar

Informationssäkerhet i vården styrs inte bara av externa regelverk och interna riktlinjer. Omvärldens värderingar och förväntningar påverkar också. Den offentliga bilden i nyhetsmedier kan till exempel påverka relationer mellan vårdpersonal och patienter och därmed säkerhetsarbetet. Förtroendefrågor är en faktor i all informationsdelning, inte minst i vården. Nyhetsmediernas rapportering samspelar vidare med forskarsamhällets bilder. Tillsammans återverkar de på samhällspolitiska debatter, regelverk och riktlinjer samt rutiner och praxis. Omvärldsbilder i medier och forskning ger med andra ord en bakgrund och ett sammanhang till en lägesbild av informationssäkerhets-arbetet i vården, varför kartläggningen även har omfattat en genomgång av svenska nyhetsmedier och forskningspublikationer.

Retriever Mediearkivet är Sveriges största digitala nyhetsarkiv och en lämplig källa för att utvärdera nyhetsbilden av informationssäkerhetsfrågor i vården.[20] Databassökningar gjordes för perioden 2001–2014. För varje år noterades andel artiklar som berörde (1) dataintrång och (2) it-störningar, dels generellt för hela nyhetsflödet, dels avgränsat till vårdrelaterade nyhetsartiklar. Antal årliga artikelträffar på sökordet ”och” användes för att beräkna andelar, dvs. för normalisering av frekvenser. Vidare gjordes en sökning på nyhetsartiklar om patientsäkerhet. Alla sökningar var avgränsade till rubriker och ingresser i svensk dagspress.

Söksträngarna var som följer:

[20] Dataunderlaget från Mediearkivet fastställdes 2014-12-16. Länk till Mediearkivet: http://www.retriever-info.com/sv/category/news-archive/.

- patientsäkerhet*
- dataintrång*
- it-fel* OR datorfel* OR datafel* OR it-haveri* OR datorhaveri* OR datahaveri*
- (patient* OR *sjuk* OR *vård* OR *journal*) NOT journalist* NOT kriminal* (*söksträng för avgränsning till vårdrelaterat material*).

PubMed är en fritt tillgänglig söktjänst på nätet anpassad till MEDLINE, en databas för medicinska artiklar. United States National Library of Medicine (NLM) driver söktjänsten och databasen.[21] Söktjänsten listar över 24 miljoner artiklar och sökningar kan göras med fria söksträngar eller MeSH-termer (Medical Subject Headings), medicinska ämnesrubriker. NLM kontrollerar och kvalitetssäkrar MeSH. Karolinska institutet gör detsamma för översättningar till svenska.

Forskning om informationssäkerhet är begränsad,[22] varför det är möjligt att söka litteratur med enkla söksträngar, vilket normalt sett resulterar i stora mängder material. Sökning på ”information security” gjordes för en inledande bedömning av omfånget på publikationer (drygt 300 publikationer). Därefter avgränsades sökningarna till ”audit”, granskningar och revisioner.

För att sammanställa statistik om utvecklingen av forskningspublikationer om informationssäkerhet i vården användes MeSH-termer: ”health care category”, ”medical informatics”, ”privacy” och ”computer security”. Termen ”health care category” är en ämneskategori på den högsta kategorinivån som omfattar drygt 8 miljoner artiklar. Årliga antal artikelträffar för denna term användes för att normalisera artikelfrekvenser för övriga MeSH-termer.

I Sverige tillhandahåller Kungliga biblioteket (KB) två söktjänster av relevans för forskningspublikationer, LIBRIS och SwePub. LIBRIS tillåter sökning efter avhandlingar av svenska forskare. SwePub omfattar alla typer av vetenskapliga publikationer. LIBRIS ger dock långt fler träffar på avhandlingar inom området informationssäkerhet. Därför har båda tjänsterna använts.

Termer och klassificeringar i LIBRIS och SwePub är inte lika kvalitetssäkrade som i PubMed. Termerna ”it-säkerhet” och ”dataskydd” finns listade i Svenska ämnesord[23], en databas med svenska ämnesord för klassificering av artiklar. I databasen hänvisar termerna till varandra samt till MeSH-termen ”Computer

[21] Länk till söktjänsten: http://www.ncbi.nlm.nih.gov/pubmed
[22] Silic, Mario, and Andrea Back. "Information security: Critical review and future directions for research." Information Management & Computer Security 22.3 (2014): 279-308.
Karlsson, Fredrik, Åström, Joachim, and Karlsson, Martin. "Information security culture: State-of-the-art review between 2000 and 2013." To be published in Information Management and Computer Security.
[23] http://www.kb.se/katalogisering/Svenska-amnesord/om/

Security”[24]. I svenska MeSH översätts ”Computer Security” till ”datasäkerhet” och ”privacy” till ”integritet.[25] Termen ”informationssäkerhet” utgör ingen egen databaspost, men en hänvisning finns till ”it-säkerhet” i Svenska ämnesord. Med tanke på bristerna i kvalitetssäkring användes bara enkla söksträngar för sökningar i LIBRIS och SwePub:

- Söksträng på LIBRIS: (informationssäkerhet* OR it-säkerhet* OR datasäkerhet* OR dataskydd*) mat:(avhandling)
- Söksträng på SwePub: (informationssäkerhet* OR "information security" OR it-security OR it-säkerhet* OR "cyber security" OR cybersäkerhet*)
- Kompletterande söksträng på SwePub för att avgränsa litteratursökningar till vårdrelaterat material: (healthcare OR care OR sjuk* OR vård* OR health).

Nyhetsartiklar och forskningspublikationer är två källor till externa perspektiv på informationssäkerhet i vården. En tredje källa är offentliga utredningar och oberoende granskningar, till exempel tillsynsrapporter av Socialstyrelsen (innan 1 juni 2013) och IVO (efter 1 juni 2013). Granskningar och revisioner av enskilda säkerhetskontroller, till exempel Datainspektionens granskningar av vårdgivarnas åtkomstkontroller (logguppföljning) och Inera AB:s revisioner av SITHS-kort och HSA, berörs inte närmare i denna kartläggning. Hänvisning görs dock till generella slutsatser i dessa granskningar.

För att upprätta statistik på ämnesval i nyhetsartiklar, forskningspublikationer och granskningar har ordfrekvenser beräknats för rubriker, sammanfattningar och/eller hela texter. En frekvensanalys inleds med en automatisk sökning efter ordstammar och frekvensräkning av dessa. För ändamålet har programmet R använts, kompletterat med manuell granskning. Efter automatisk sökning sker en manuell genomgång och redigering.

3.1.2 Verksamhetsrapporter och klagomål

> *Alla landsting har en informationssäkerhetspolicy vilket är ett lagkrav och 62 % har en informationssäkerhetsplan.*[26]
>
> *En central del av patientdatalagen är logguppföljning. I alla landsting sker loggranskning med stickprov på lokal nivå, men hälften av landstingen har också en central granskning.*[27]

Citaten är hämtade från SLIT-rapporten, en årlig redovisning av landstingens it-utveckling och förvaltning. Förutom dessa citat finns det några meningar om

---

[24] Engelska översättningar enligt hänvisning från Kungliga biblioteket till Library of Congress Subject Headings.
[25] Länk till Karoliska institutets webbsida för MeSH på svenska: http://mesh.kib.ki.se/swemesh/swebrowse.cfm
[26] eHälsa i landstingen. Rapport 2014. SLIT (Landstingens IT-strateger/IT-chefer): http://www.inera.se/Documents/OM_OSS/Styrdokument_o_rapporter/SLITrapport_2014.pdf
[27] Ibid.

SITHS-kort och behörighetskontroller. Fokus ligger på inventering av system och nätverk. Utrymmet för vårdgivarnas kvalitets- och säkerhetskontroller är minimalt.

För att kartlägga vårdgivarnas uppföljning av kontroller, risker och incidenter sändes en begäran om offentlig dokumentation till landsting och kommuner. Begäran och påminnelser har gått ut i flera steg. Sökningar efter dokumentation på vårdgivarnas hemsidor har genomförts parallellt för att både kontrollera och komplettera vårdgivarens svar.

Steg 1 (maj–juli 2014)

- Begäran till central registrator (e-postadresser på SKL:s hemsidor) om diarieförda granskningar och verksamhetsrapporter om informations- och it-säkerhet för perioden 2011–juni 2014, med specifik hänvisning till föreskrift SOSFS 2008:14, men där begäran som sådan avser alla diarieförda granskningar och rapporter på området (brevtext nedan)
- Sökningar på vårdgivarnas hemsidor efter årsredovisningar, revisioner och verksamhetsrapporter.

Steg 2 (augusti–oktober 2014)

- Påminnelse och precisering av förfrågan:
  - Vårdgivarens senaste årsrapport enligt SOSFS 2008:14
  - Landstingens och kommunernas revisioner av it- och informationssäkerhet 2011–2013
- Begäran om patientsäkerhetsberättelse och kvalitetsredovisning 2013 för vård och omsorg från kommuner där sökningar på hemsidan inte gav något resultat
- Begäran till landsting om beskrivning och årsstatistik av system för avvikelsehantering och it-incidenthantering.

Steg 3 (november 2014–januari 2015)

- Begäran till central registrator om informationssäkerhetspolicy och riktlinjer från landsting och kommuner
- Begäran om statistik avseende informationsrelaterade klagomål till landstingens patientnämnder under 2014
- Begäran om verksamhetsplaner avseende informationssäkerhet från 30 omsorgsnämnder i kommuner med explicita krav på uppföljning och rapportering i riktlinjerna för informationssäkerhet.

Inledande e-brev med begäran om verksamhetsrapportering

”I syfte att analysera kunskapsläget om it- och informationssäkerhet i svensk vård och omsorg önskar jag ta del av diarieförda rapporter avseende kommunens it-säkerhet och informationssäkerhet under de senaste tre åren, drygt, från januari 2011, fram till och med juni 2014.

Utgångspunkten för denna förfrågan är den årliga rapporteringen av informationssäkerhetsinsatser enligt SOSFS 2008:14, dvs. Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården, dvs. ansvariges rapportering till vårdgivare.

Utöver denna specifika rapportering önskar jag ta del av kompletterande information i den utsträckning som den existerar: uppföljningar och revisioner. I fall delar av materialet är klassat med sekretess önskar jag bara ta del av datum och rubrik på handlingen i diariet.

Om det inte finns något att tillgå för perioden 2011–2014 önskar jag den senast diarieförda rapporten.

Om det är möjligt tar jag tacksamt emot pdf-filer."

Vid tidpunkten för förfrågan om verksamhetsrapporter (juni 2014) fanns det inga planer på att efterfråga vårdgivarens riktlinjer för informationssäkerhet. Med tiden blev det dock klart att vårdgivarnas kännedom om rapporteringskrav enligt SOSFS 2008:14 inte var självklar, varmed frågor om vårdgivarnas egna krav på uppföljning och rapportering aktualiserades. Begäran om policyer och riktlinjer på området sändes därför ut i ett senare steg av kartläggningen istället för att det fick inleda arbetet, vilket hade varit en mer naturlig ordning.

Ansvaret för uppföljning och rapportering av informationssäkerhet ligger på både centrala och lokala verksamhetsledningar. Denna kartläggning omfattar primärt regionala och kommunövergripande centrala verksamhetsrapporter. Lokal dokumentation från enskilda förvaltningar har samlats in när centrala styrdokument eller svar på förfrågningar har motiverat det, till exempel om riktlinjer för informationssäkerhet anger att uppföljning och rapportering ska ske i lokala årsredovisningar.

Alla verksamhetsrapporter och revisioner kontrollerades, ämnesstruktur och nyckelord, och kodades med avseende på förekomst av resultat från kvalitets- och säkerhetskontroller i informationshantering i enlighet med SOSFS 2008:14:

- Övergripande granskningar av informationssäkerhet
- Risk- och incidentrapporter på området
- Verksamhetsutveckling inom informationssäkerhet
- Kvalitetsgranskningar av vårddokumentation
- Loggguppföljning av vårdsystem.

I princip är det enkelt att definiera informationssäkerhetsrisker och incidenter i vården, dvs. *potentiella eller faktiska händelser där krav på konfidentialitet, riktighet, tillgänglighet eller spårbarhet i vårdinformation, dokumentation eller system inte tillgodoses*. I praktiken är det oklart vad det omfattar och hur det tolkas av vårdgivare. Kvalitets- och säkerhetsfrågor angränsar till varandra. It-incidenter, till exempel dataintrång och driftstörningar, är delmängder av

alla tänkbara störningar som gör att kvalitets- och säkerhetskrav inte uppfylls. Om remisser och provsvar är felaktiga, försenade eller har gått förlorade, är det ett kvalitetsproblem eller ett säkerhetsproblem? Vem avgör det? Vem kontrollerar? Vem sammanställer resultat?

I princip kan risker och incidenter på området omfatta alla typer av oönskade händelser i informationsförsörjning och hantering, endemiska och akuta, i alla processteg, från mottagande och lagring av information till bearbetning och förmedling. Händelserna kan föranleda avvikelsehantering i vårdverksamhet och incidenthantering inom it-förvaltning. Det väcker frågan om och hur vårdgivare hanterar risker och incidenter på området.

> *I Socialstyrelsens föreskrifter och allmänna råd om ledningssystem för systematiskt kvalitetsarbete (SOSFS 2011:9) framgår att vårdgivaren ska ha ett ledningssystem för att planera, leda, kontrollera, följa upp, utvärdera och förbättra verksamhetens kvalitet. En del av ledningssystemets grundläggande uppbyggnad är risk- och avvikelsehantering.*[28]
>
> *Avvikelser delas in i händelser som dels ledde till att en patient skadats (negativ händelse), dels händelser som kunde ha lett till att en patient skadats (tillbud). Även avvikelser (klagomål och synpunkter) rapporterade av patient och närstående ska tas tillvara och följas upp. Avvikelser kan också vara en icke förväntad händelse i verksamheten som medfört eller skulle kunna medföra skada på närstående, medarbetare, utrustning eller organisation.*[29]

Vårdhandboken listar en rad exempel på avvikelser som bör rapporteras. Dessa omnämner inte informationssäkerhetsrisker och incidenter explicit. Däremot finns det exempel som kan vara eller uppfattas vara säkerhetsrelaterade (listan nedan).[30] Vidare ska vårdens händelse- och riskanalyser av avvikelser innehålla orsaksanalyser och åtgärdsbeslut,[31] vilka kan beröra informationssäkerhet. Det är öppen fråga om det finns någon samlad uppföljning på området.

> *Exempel på avvikelser i Vårdhandboken som kan beröra informationssäkerhet:*
>
> - *Förväxlingar (läkemedel, dokumentation, identitet och så vidare)*
> - *Brister i informationsöverföring mellan landsting och kommun*
> - *Felaktig, otillräcklig, avsaknad av eller vilseledande instruktion, information eller dokumentation*

---

[28] Vårdhandboken, Stockholms läns landsting (elektronisk version 2015-01-04): http://www.vardhandboken.se/Texter/Avvikelse--och-riskhantering /Oversikt/
[29] Ibid.
[30] Ibid.
[31] Riskanalys och händelseanalys – handbok för patientsäkerhetsarbete. Socialstyrelsen 2009: http://www.socialstyrelsen.se/publikationer2009/2009-126-120/Documents/RiskanalysochHandelseanalys_original.pdf

- *Felaktig användning eller felaktigt underhåll av medicintekniska produkter eller annan utrustning som tekniska försörjningssystem, nödkraftaggregat och informationssystem*
- *Bristande eller otillräckliga resurser (till exempel kompetens, bemanning, lokaler, utrustning)*
- *Klagomål från patient/närstående.*

För att klargöra om och hur risk- och incidentrapporteringen fungerar omfattar insamling och analys av dokumentation även landstingens system för hantering av avvikelser i vårdinformation respektive it-incidenter. Av tids- och resursskäl omfattas kommunerna inte av denna del av kartläggningen. Följande uppgifter och dokumentation begärdes in från landstingen:

- Beskrivning av klassificeringssystem – hur avvikelser respektive it-incidenter klassificeras i olika system
- Handledning eller vägledning för användare avseende system för hantering av incidenter respektive avvikelser
- Statistikrapporter för typer eller kategorier av avvikelser och incidenter av relevans för informationssäkerhet, utöver patientsäkerhetsberättelser.

Materialet granskades med avseende på hur informationssäkerhetsrisker och incidenter potentiellt kan klassificeras, explicita och implicita kategorier. I de fall ett system tillåter explicit klassificering av avvikelser eller incidenter som ett informationssäkerhetsproblem skickades en förfrågan om kompletterande statistikuppgifter för denna kategori.

Rapportering av avvikelser och incidenter i informationssäkerhet görs inte bara av vårdpersonal. Det görs även av patienter och anhöriga i form av klagomål. Klagomål kan riktas dels till vårdgivaren och bli föremål för avvikelsehantering, dels till patientnämnderna i landstingen. De senare ska fungera som oberoende stöd till missnöjda patienter. Stödet handlar först och främst om information om rättigheter och kommunikation med vårdgivaren.

För sitt arbete använder patientnämnderna riktlinjer för ärendehantering som tillåter en nationell klassificering av klagomål.[32] Det finns ingen motsvarande standardisering av avvikelsehantering, med undantag för händelseanalyser med NITHA.[33] Det gör patientnämndernas arbete intressant för en lägesbild av informationssäkerhet i vården, även med tanke på att patientnämnderna i Sverige generellt registrerar fler klagomål än vårdgivare.[34] Mot denna

[32] Handbok för Patientnämndernas kanslier i Sverige 2014. Pdf-dokument från Patientnämnden i Jönköpings läns landsting.
[33] NITHA, Nationellt IT-stöd för händelseanalys.
[34] Skillnader i antal ärenden till patientnämnder och avvikelser framgår i en del av landstingens patientsäkerhetsberättelser 2013.

bakgrund skickades en begäran till landstingens patientnämnder om statistik för följande klagomål under 2014.

Typer av patientklagomål i patientnämndernas ärendehantering av relevans för informationshantering och säkerhet:

Vård och behandling

- *Remiss/vårdbegäran*
- *Intyg*
- *Medicinskteknisk utrustning*

Kommunikation

- *Information till patient/närstående*

Patientjournal och sekretess

- *Bruten sekretess/tystnadsplikt*
- *Patientjournal/loggar*
- *Dataintrång*

Vårdansvar

- *Informationsöverföring inom vårdgivare*
- *Informationsöverföring mellan vårdgivare*

Administrativ hantering

- *Brister i hantering av remisser mm*
- *Övrig administrativ hantering.*

3.2 Enkätundersökning

Offentliga rapporter ger sällan en bild av kontrollarbetet i praktiken, vare sig det rör sig om externa eller interna rapporter, gransknings-, forsknings- eller verksamhetsrapporter. Det är vanligtvis enskilda förekomster av kontroller som tas upp, inte deras kvalitet, till exempel kontrollfrekvens och spridning i en organisation och dess olika verksamheter. För en lägesbild av uppföljning och rapportering i praktiken är det därför nödvändigt att återge vårdpersonalens kännedom och erfarenhet av kontrollarbete och avvikelser. Professionell kännedom och erfarenhet på området kan också ses som mål för och effektmått på styrning och uppföljning av informationssäkerhet. För att kartlägga denna del genomfördes en enkätundersökning bland två grupper hos vårdpersonal, dels medlemmar i Läkarsekreterares och Sjukvårdsadministratörers Förbund (LSF-medlemmar), dels ett slumpmässigt nationellt urval av sjuksköterskor.

3.2.1 Deltagare och design

Läkarsekreterare och sjukvårdsadministratörer har vårddokumentation som huvudsaklig arbetsuppgift. De utgör specialister, en expertgrupp, men är inte listade som yrkeskategori i SCB:s yrkesregister. Det gör det omöjligt med en representativ enkätundersökning. Genom LSF är det dock möjligt att nå dessa specialister. Legitimerade sjuksköterskor är däremot listade i registret, vilket möjliggör ett slumpmässigt urval. Nämnda skillnader mellan yrkesgrupperna är det främsta skälet till en enkätundersökning i två delar, dels en webbenkät till LSF-medlemmar, dels en enkät till sjuksköterskor. MSB administrerade den första delen, SCB den andra.

Fördelen med enkätuppdelningen var att LSF:s ledning kunde engageras som granskare och rådgivare i enkätdesign och valet av frågor. LSF är ett mindre yrkesförbund. Det resulterade i kvalificerade, effektiva samråd. Utöver LSF granskades enkäten av SCB:s och MSB:s experter samt fyra oberoende forskare på Karolinska institutet, Sahlgrenska akademin och Högskolan i Skövde.

Yrkesenkäten till LSF-medlemmar var en webbenkät. LSF sände ut information om enkätens syfte och upplägg. En webblänk till enkäten bifogades. Premissen var en anonym enkät, varför inga personnycklar användes. Inga organisations-, person- eller adressuppgifter samlades in, varken analoga eller digitala.

Flera faktorer bidrog till beslutet om endast en målgrupp för SCB:s yrkesenkät, dels begränsade resurser, dels enkätdesign. Enkätfrågorna berörde rutiner och avvikelser vars relevans varierar med yrkesroll, även inom vården. Med en stor variation i svarsmönster krävs fler respondenter för att säkerställa slutsatser, vilket ställer krav på större urval och mer resurser. För att undvika alltför stor variation begränsades SCB:s yrkesenkät till sjuksköterskor. De har en central roll i samordning av vårdinformation och kommunikation.

Ett slumpmässigt urval på 5 000 legitimerade sjuksköterskor gjordes från SCB:s yrkesregister hösten 2014. Efter justering för icke yrkesaktiva personer uppgick nettourvalet till 4 757 personer. Eftersom uppgifterna i registret är 2 år gamla är urvalet begränsat till personer med minst två års yrkeserfarenhet.

Följande mål och kvalitetskriterier vägledde designarbetet:

- Enkäten är ett verktyg för att samla in och sammanställa målgruppernas kännedom och erfarenhet av kontrollarbete och avvikelser (incidenter) avseende informationshantering och -säkerhet.
- Enkäten ska beröra kontrollrutiner, uppföljning och avvikelser av relevans för informationens *konfidentialitet, riktighet och tillgänglighet*. *Spårbarhet* är en mer sammansatt och svårare fråga som kräver en utförligare och kanske separat enkät.
- Enkäten ska vända sig till yrkesaktiva personer. Definitionen av ”aktiv” är att tiden för ett aktuellt avbrott i vårdyrket uppgår till maximalt 3 månader.
- Enkäten ska vara kort och enkel för att kompensera ett potentiellt bortfall på grund av sällan prioriterade frågor.

- För effektiv svarshantering användes bara frågor med slutna svarsalternativ, med ett undantag. I enkäten till LSF-medlemmar ingick en avslutande öppen fråga om reflektioner och synpunkter på enkäten och kontrollarbetet i vården.

Med dessa riktlinjer utformades en enkät, Säker vårddokumentation, med 35 frågor, plus en öppen avslutande fråga i enkäten till LSF-medlemmar. Frågorna med svarstabeller finns i bilagorna 1 och 2, med undantag för den öppna frågan till LSF-medlemmar som redovisas i en separat rapport till LSF. Definitioner och förklaringar av centrala begrepp återges också i bilagorna. I den faktiska enkäten upprepades definitioner och förklaringar vid sidbrytningar, om det var relevant och aktuellt. I bilagorna återges de bara en gång.

Informationen till grupperna var i princip densamma, men det fanns givetvis stilistiska skillnader beroende på målgrupp och undersökningsdesign. Följande brevtext följde med LSF:s medlemsutskick (närmare metodbeskrivningar av SCB-enkäten finns i en teknisk rapport[35]):

Informationsbrev till LSF-medlemmar

Till dig som arbetar som läkarsekreterare eller sjukvårdsadministratör

Är dagens säkerhet för vårddokumentation tillräcklig för att garantera patientsäkerheten?

Vårddokumentation är en central del av det dagliga arbetet i hälso- och sjukvården. Rätt och korrekt dokumentation kan vara avgörande för patienters liv och hälsa. Det innebär att informationssäkerheten är viktig, dvs. att vårddokumentationen skyddas och hanteras på ett säkert sätt.

Idag saknar samhället en helhetsbild av informationssäkerheten i hälso- och sjukvården. För att få fram en lägesbild genomför Myndigheten för samhällsskydd och beredskap (MSB) en undersökning i samverkan med Läkarsekreterares och Sjukvårdsadministratörers Förbund (LSF).

I dialog med förbundets styrelse har MSB utformat en enkät. Syftet är en lägesbild av medlemmarnas kännedom om och erfarenhet av kontrollarbete med vårddokumentation. I egenskap av läkarsekreterare eller sjukvårdsadministratör är dina svar centrala, värdefulla och viktiga.

Vi vänder oss till dig som yrkesperson. Frågorna handlar om din kännedom om och erfarenhet av kontrollarbetet på din arbetsplats. Du svarar anonymt. Vi samlar inte in några person- eller organisationsuppgifter. Vi hoppas på dina svar, inte uppgifter från någon annan källa. Följande länk tar dig till en webbversion av enkäten.

[WEBBLÄNK]

[35] SCB. Teknisk Rapport – En beskrivning av genomförande och metoder. Avtalsrelationer 2014. Rapport. Myndigheten för samhällsskydd och beredskap.

I fall du föredrar en pappersenkät, kontakta undertecknad. Det gäller även om du har andra frågor, till exempel frågor om sekretess.

Vi kommer att delge resultatet på flera sätt: en sammanfattning i LSF Magazinet, en fullständig rapport på MSB:s hemsida i början av februari 2015 (www.msb.se) samt en analys på LSF:s kongress 7–8 maj 2015.

3.2.2 Former för resultatredovisning

Enkätresultatet delges i flera former, dels tabeller för alla frågor i bilagorna 1 och 2, dels frekvenstal i löpande text. Felmarginaler, 95 %-konfidensintervall, återges bara för resultat från SCB-enkäten. Felmarginaler representerar den osäkerhet som ligger i att generalisera enkätresultatet till sjuksköterskor som population. LSF-enkäten är däremot en enkät till medlemmar som inte utan vidare kan antas representera yrkeskåren i sin helhet. Det är också osäkert om respondenterna till LSF-enkäten utgör ett rättvisande urval av medlemmar. Att utvärdera representativitet kräver personuppgifter av något slag. Med hänsyn till etik och praktiska frågor var det inte aktuellt att samla in personuppgifter av något slag. Enkäten till LSF-medlemmar är att betrakta som en expertenkät till specialister på vårddokumentation, inte en representativ enkät. Därför återges inga felmarginaler för resultat från LSF-enkäten.

För att undvika olika format på statistik redovisas inga felmarginaler i löpande text, även om hänvisningar kan göras till signifikanta skillnader. Felmarginaler presenteras bara i bilaga 2 med resultat från SCB-enkäten. Det är vidare viktigt att notera olika betydelser av procent i LSF- och SCB-enkäterna. I LSF-enkäten representerar ett procenttal *andel respondenter som väljer ett svarsalternativ framför andra svarsalternativ*. I SCB-enkäten är procenttalet *en skattning av andel svar för hela populationen av legitimerade sjuksköterskor*.

I texten förekommer olika andelstal och sammansatta frekvenstal. Procent är en form av andelstal, *antal per 100*. Basen 100 är dock godtycklig. Andelstal kan uttryckas i andra baser för att göra resultatredovisningen lättare att följa, till exempel antal per 10 eller 1 000 (promille). För samma syfte kan det vara värdefullt att använda sammansatta frekvenstal när frågor och svar beror på andra frågor och svar. Till exempel, om 50 % svarar ja på en följdfråga som bara 50 % av respondenterna kan svara på är den totala andelen ja inte 50 % utan 25 % (50 % x 50 %). Sammansatta frekvenstal tillåter effektivare och mer överskådliga resultatpresentationer.

3.3 Metodkritik

Kunskaps- och faktaunderlaget i kartläggningen är omfattande, men långt ifrån heltäckande. Det som framför allt saknas är en systematisk genomgång av lokal intern kontroll och egenkontroll, dvs. verksamhetskontroller i och av enskilda förvaltningar. Denna typ av kontroll är sällan förenad med offentliga rapporter, annat än generella revisioner av riktlinjer för kontrollarbetet. Kontrollen tjänar verksamhetsledningens interna styrning och omfattar ett urval kontrollpunkter som bedöms viktiga och relevanta med utgångspunkt i tidigare kontrollresultat,

revisioner och riskanalyser. Formerna för planering och uppföljning varierar från förvaltning till förvaltning inom en och samma vårdgivare. En systematisk kartläggning av denna kontroll, om och hur den berör informationssäkerhet, är ett omfattande arbete i sig. I den aktuella kartläggningen har resultatrapporter från intern kontroll delgivits eller begärts in sporadiskt.

En relaterad fråga är det nationella kontrollarbetet av vårdgivarnas användning av nationella e-tjänster, HSA och SITHS-kort. Arbetet bedrivs av Inera AB som utvecklar och förvaltar infrastruktur och nationella e-tjänster för vården. I den aktuella kartläggningen berörs Ineras kontrollarbete inte närmare, eftersom det handlar om två specifika e-tjänster. Information och revisionsrapporter finns tillgängliga på Ineras hemsida.[36]

Ett annat problem är att resultatet av en begäran om diarieförd dokumentation beror på vem som får och vem som svarar på frågan. En sådan begäran innebär sökningar i diarier och arkiv, vars resultat beror på vårdgivarnas varierande processer och system för ärendehantering. I kartläggningen riktades en första begäran till sjukvårdshuvudmännens centrala e-postadresser som finns listade på SKL:s webbsida.[37] Svaren på denna begäran kom från både central och lokal administration, olika förvaltningar. Verksamhetsrapporter på området var inte sällan en tolkningsfråga, även om förslag till söktermer bifogades. Med hänsyn till det och diskussionen om intern kontroll är det varken säkert eller troligt att kartläggningen är fullständig eller heltäckande. Det säger dock något om läget på området, nämligen att riktlinjerna för uppföljning är oklara.

Ett tredje metodproblem i kartläggningen är bredden av material. Syftet är att återge en generell, nationell lägesbild. Det innebär begränsade möjligheter att gå in på detaljer i enskilda frågor, något som ökar risken för onyanserade och orättvisa beskrivningar. Frågan om *underrapportering* är ett exempel. I vård och omsorg är verksamhetsledningar vana vid externa frågor om uppföljning och rapportering. Externa regelverk kräver uppföljning av vårdverksamheter. I fråga om it och teknik är regelverket svagare. Uppföljning av it-incidenter är sällan offentlig, till skillnad från vårdens krav på anmälan av vårdskador. Dessa kulturskillnader gör att det är jämförelsevis lätt att få tag i material om vårdens uppföljning, men långt svårare att få tag i material från it-förvaltningar. Det innebär en risk för en offentlig problembild med fokus på vården snarare än en problembild med fokus på informationsstyrning och ledning.

---

[36] Länk till Ineras webbsida för revisioner av HSA och SITHS-kort: http://www.inera.se/TJANSTER--PROJEKT/HSA/HSA-regelverk-och-riktlinjer/Revisioner-av-SITHS-och-HSA/

[37] Länk till webbsida hos Sveriges kommuner och landsting (SKL): http://skl.se/tjanster/kommunerlandsting.431.html

4. Resultat

4.1 Externa perspektiv

4.1.1 Nyhetsbilder

Sedan 2001 har andelen nyhetsartiklar om patientsäkerhetsfrågor ökat (diagram 1). It- och informationssäkerhetsrisker är ingen drivkraft i utvecklingen. Bland alla artiklar om patientsäkerhet under perioden kan ett journalrelaterat innehåll observeras i drygt 6 % av fallen. Andelen är stabil över tid. Sex artiklar handlar om it-störningar. Endast två artiklar handlar om dataintrång.

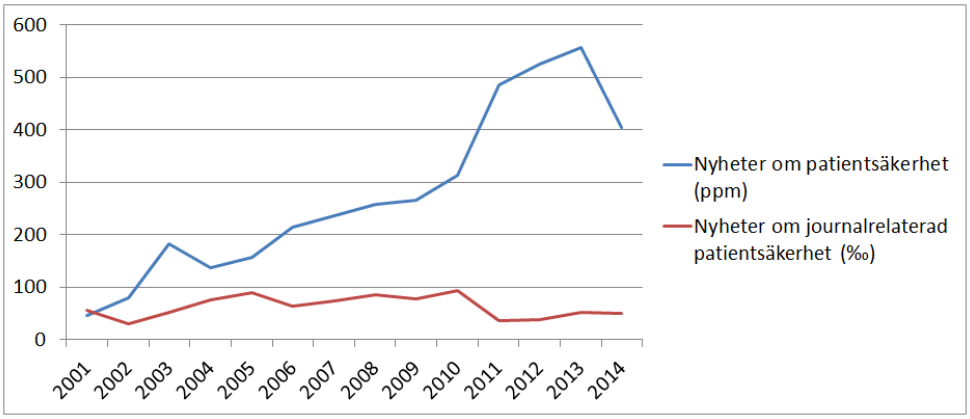


Diagram 1. Andel nyhetsartiklar om patientsäkerhet
Blå linje representerar andel artiklar om patientsäkerhet av samtliga nyhetsartiklar (ppm = ”parts per million”, antal per miljon). Orange linje representerar andel journalrelaterade artiklar av samtliga artiklar om patientsäkerhet (‰ = promille, antal per tusen).

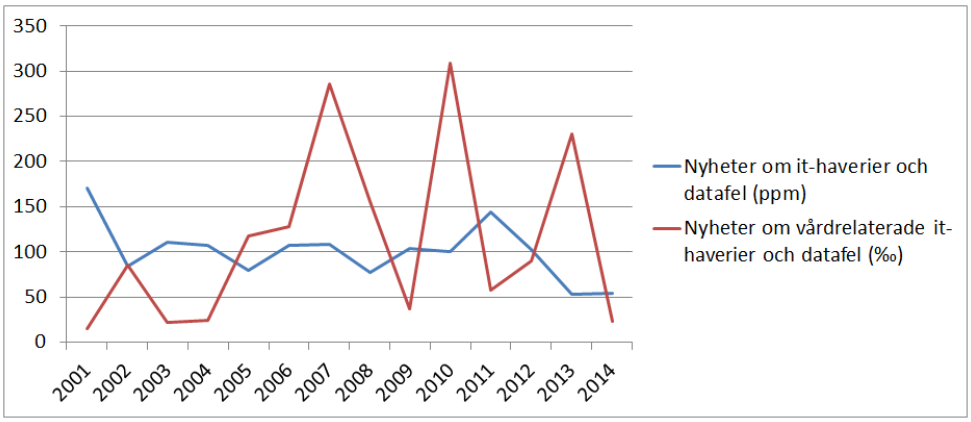


Diagram 2. Andel nyhetsartiklar om it-störningar i vården
Blå linje representerar andel artiklar om it-störningar av samtliga nyhetsartiklar (ppm = ”parts per million”, antal per miljon). Orange linje representerar andel vårdrelaterade artiklar av samtliga artiklar om it-störningar (‰ = promille, antal per tusen). Toppnoteringen 2006 relaterar till Folkpartiets intrång i Socialdemokraternas it-system.

Andelen artiklar om it-störningar i nyhetsmedierna har varit stabil sedan 2001, cirka 0,1 ‰ (diagram 2). I snitt är drygt 10 % av dessa artiklar vårdrelaterade. Siffran varierar kraftigt. Under 2010 var över 30 % av nyhetsartiklar om it-störningar vårdrelaterade.

Andelen artiklar om dataintrång i nyhetsmedierna är i snitt 3 gånger högre än andelen artiklar om it-störningar (diagram 3). En växande trend kan urskiljas för de senaste åren samt en stabil och hög nivå för andelen vårdrelaterade artiklar, cirka 20 %. För hela perioden är andelen vårdrelaterade artiklar 17 %.

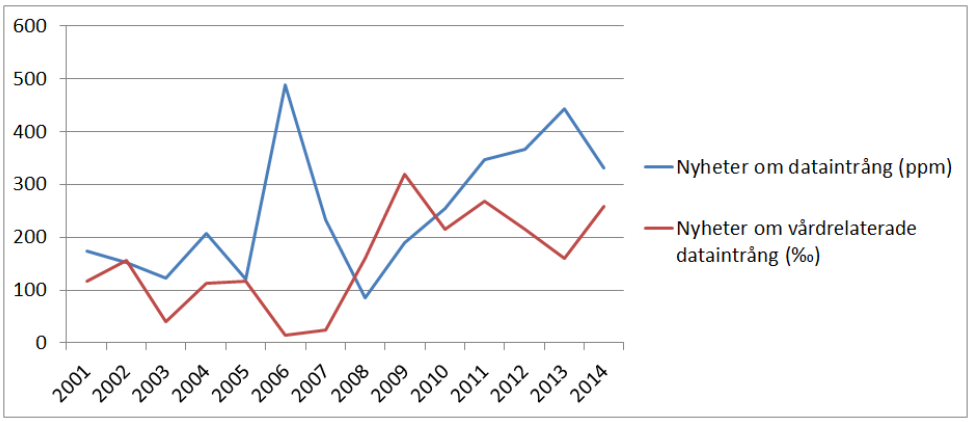


Diagram 3. Andel nyhetsartiklar om dataintrång i vården

Blå linje representerar andel artiklar om dataintrång av samtliga nyhetsartiklar (ppm = ”parts per million”, antal per miljon). Orange linje representerar andel vårdrelaterade artiklar av samtliga artiklar om dataintrång (‰ = promille, antal per tusen).

Sammantaget har patientsäkerhetsfrågorna fått en allt större plats i mediernas nyhetsrapportering. I fråga om it-störningar är intresset mer eller mindre oförändrat. Andelen artiklar om vårdrelaterade informationsstörningar speglar vårdens arbetsmarknadsandel, drygt 16 % av de förvärvsarbetande år 2013.[38] Ett växande intresse kan dock noteras för dataintrång, där andelen vårdrelaterade artiklar också växer. Ökningen sammanfaller med patientdatalagens tillkomst, ett växande antal anmälningar av vårdpersonal för dataintrång samt debatter om patientdatalagens tillämpning.[39]

[38] SCB Registerbaserad arbetsmarknadsstatistik (RAMS), antal förvärvsarbetande (dagbefolkning) efter näringsgren och NUTS2 (EU-standard) för år 2013.
[39] Patientdatalagen ger ansvariga tjänstemän huvudbry. Läkartidningen 2013(15).

4.1.2 Nationella granskningar

Socialstyrelsen har granskat informationssäkerheten på sex universitetssjukhus i landet. Vid samtliga sjukhus finns brister som kan leda till att patienter kommer till skada.[40]

Under 2011 genomförde Socialstyrelsen egeninitierad verksamhetstillsyn av informationssäkerhet på sex universitetssjukhus i Sverige. Tillsynen omfattade vårdgivarens ledning och styrning av informationssäkerhetsarbetet samt informationssäkerhetskrav på journalsystem. Inspektioner skedde enligt Socialstyrelsens föreskrifter (SOSFS 2005:12) om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården, patientdatalagen (2008:355) och Socialstyrelsens föreskrifter (SOSFS 2008:14) om informationshantering och journalföring i hälso- och sjukvården. Inspektioner på plats skedde under två dagar och berörde systemfunktioner, riktlinjer och rutiner (områden nedan). Vårdgivaren meddelades om inspektion ett par månader innan och ombads samtidigt att delge informationssäkerhetspolicy och systembeskrivningar.

Inspektionsområden avseende informationssäkerhet[41]

- Journalsystem
- Styrning av informationssäkerheten (policy med mera)
- Drift, incident & support
- Ändringshantering (hantering av systemförändringar)
- Fysiskt skydd
- Behörigheter
- Loggning
- Öppna nät
- Kontinuitet och personalens utbildning.

Socialstyrelsens oberoende tillsyn av vårdens informationssäkerhet är hittills den enda i sitt slag.[42] Den resulterade i kritik mot samtliga vårdgivare med krav på åtgärder inom flertalet inspektionsområden. Kritik riktades mot oklara riktlinjer och bristande uppföljning. Styrningen av och kravställningen på journalsystemen ansågs svag. Ansvaret låg på it-förvaltningarna, vilket resulterade i ett bristande verksamhetsperspektiv på systemutveckling och

---

[40] Länk till Socialstyrelsens webbsida med tillsynsbeslut och pressinformation 2011-06-20: http://www.socialstyrelsen.se/pressrum/nyhetsarkiv/it-problemskaparriskerforpatienter

[41] Utöver publicerade beslut på Socialstyrelsens webbsida (ibid.) har MSB begärt och tagit del av inspektionsplaner och rapporter från IVO. Inspektionsområden återges i inspektionsplaner och korrespondens med sjukhusledningarna.

[42] Datainspektionen har tillsynsansvar för regelverket om hantering av person- och patientuppgifter, men inte för informationssäkerhet som ett verksamhetsansvar. Riksrevisionen genomför också granskningar, men dessa avser statliga myndigheter, inte landsting och kommuner. En granskningsrapport av statliga myndigheters arbete publicerades i slutet av 2014: *Informationssäkerheten i den civila statsförvaltningen*. Rapport. Riksrevisionen. RiR 2014:23.

förvaltning. Tillsynsbesluten ställde också krav på åtgärder som Socialstyrelsen senare godkände. Åtgärderna förändrar dock inte den generella lägesbilden, en svag verksamhetsstyrning. Sjukhusens åtgärder var punktinsatser avseende systemfunktioner, rutiner och rapportering. I brist på uppföljning är det svårt att veta dess effekter på det dagliga arbetet. Det är än svårare att bedöma om det förändrade verksamhetsstyrningen på området.

Trots en bred ambitionsförklaring var Socialstyrelsens tillsyn begränsad. Fokus var systemsäkerhet och efterlevnad av regler för behörigheter i och åtkomst till journalsystem. Tabell 1 återger de vanligaste nyckelorden i Socialstyrelsens sex beslut. Frågor om systemdrift och behörighetskontroll dominerar. Det speglar ett traditionellt it-perspektiv. För verksamhetsanknytning hade det varit värdefullt att genomlysa hur processtyrningen av vårddokumentation fungerar samt om och hur säkerhets- och kvalitetskrav på information utarbetas, omsätts och följs upp, till exempel i informationsklassningar och riskanalyser. Riskanalyser nämns i anslutning till systemutveckling och förvaltning, men inte som ett generellt verktyg för verksamhetsstyrning. Tillsynen går inte heller närmare in på säkerhet och kvalitet i informationshantering, till exempel databasdesign och kvalitetsgranskningar.

Tabell 1. Tio-i-topp nyckelord i Socialstyrelsens beslut om informationssäkerhet 2011[43]

Nyckelord av relevans för tillsynsområdet	Antal
Patientuppgift	57
Verksamhet	54
Behörighet	41
System	41
Rutin	39
Journal	36
Drift	28
Ansvar	25
Fax	25
Information	24

Betoningen på behörighets- och systemfrågor är inte unik för Socialstyrelsens tillsynsarbete. Det präglar även offentliga diskussioner och utredningar som

[43] Listan bygger på ordfrekvenser i Socialstyrelsens publicerade beslut efter tillsyn av informationssäkerheten på sex universitetssjukhus 2011: http://www.socialstyrelsen.se/pressrum/nyhetsarkiv/it-problemskaparriskerforpatienter. Från en komplett lista på ordfrekvenser har de tio vanligaste nyckelorden av relevans för tillsynsområdet identifierats. Antalet utgör summan av frekvenser för nyckelordet i dess olika grammatiska former, böjningar och avledningar, men med bibehållen grundbetydelse. Nyckelordet ”system” inkluderar till exempel system på tekniska plattformar, journalsystem, men exkluderar abstrakta system, till exempel ledningssystem.

berör informationshantering i vård och omsorg. Däremot är problembilden ofta den motsatta. Tonvikten ligger på behovet av tillgänglig och användbar vårdinformation för behörig vårdpersonal och patienter. Det präglar inte minst utredningen ”Rätt information på rätt plats i rätt tid” (SOU 2014:23). Den centrala frågeställningen är hur samhället ska tillgodose behovet av direktåtkomst till patientuppgifter mellan vårdgivare för att främja patientsäkerheten. Förslag till åtgärder handlar om att lätta på regelverk som begränsar digitala lösningar för åtkomst till vårdsystem mellan vårdgivare. Andra kvalitets- och säkerhetskrav diskuteras inte närmare. Det är sparsamt med orsaks- och konsekvensanalyser. Ändå är det fullt möjligt att dagens vårdsystem lider av bristfällig kravställning på kvalitet och säkerhet, snarare än begränsningar i regelverk. Det förblir dock oklart vad som är det huvudsakliga problemet.

Sammanfattningsvis, utvärderingar på området tenderar att betona enskilda kvalitets- och säkerhetskrav. Bristfällig interoperabilitet och systemintegration, bristfällig tillgänglighet, är det vanligaste problemet. Andra kvalitets- och särkerhetskrav kan hamna i skymundan. Inte sällan ses *bättre systemdesign för bättre tillgänglighet* som en universallösning på informationsproblem. Samtidigt går det att urskilja en gemensam nämnare i offentliga granskningar som går bortom enskilda kvalitets- och säkerhetskrav, nämligen bristfällig styrning och efterfrågan på en lokalt förankrad, långsiktig och samordnad verksamhets- och systemutveckling. Det är något som även framkommer i Ineras revisioner av de nationella e-tjänsterna HSA och SITHS. Det mest förekommande problemet är att internrevision uteblir.[44] Det svala intresset för styrning och uppföljning präglar även forskningsrapporter på området.[45,46]

4.1.3 Forskningsstudier

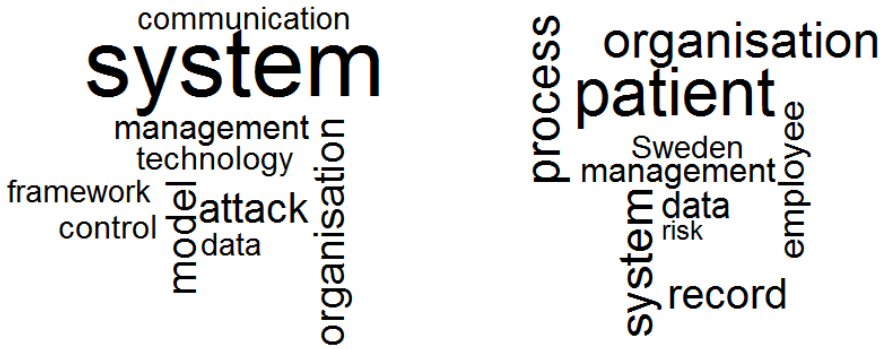
Sökningar med SwePub och granskningar av sökresultat gav 292 publikationer av svenska forskare i ”it- och informationssäkerhet”, varav 33 vårdrelaterade (bilaga 3). I figur 2 nedan illustreras frekvenser av de tio vanligaste nyckelorden i artikelrubriker och sammandrag (abstract) för två kategorier av publikationer: *icke vårdrelaterade* (vänster figur) respektive *vårdrelaterade* (höger figur), exklusive söktermerna it- och informationssäkerhet samt hälso- och sjukvård. Ju större typsnitt, desto mer frekvent nyckelord. Inga exakta siffror återges eftersom giltigheten av statistiken kan ifrågasättas. Antal

---

[44] Revisionsrapport SITHS och HSA 2014, Version 1.0 2014-09-29, Inera AB. http://www.inera.se/Documents/TJANSTER_PROJEKT/Gemensamt_infrastruktur/Revision_hsa_siths/revisionrapport_siths_hsa_2014_avidentifierad.pdf
[45] *Störande eller stödjande? Om eHälsosystemens användbarhet* 2013. Slutrapport från projektet eHälsosystemens användbarhet. Vårdförbundet.
[46] Hedström, Karin, Jäger, Kerstin, Krasnizi, Hanife, Linderoth, Henrik, Nohlberg, Marcus, Persson, Anne & Åhlfeldt, Rose-Mharie, Vårdens framtida informationssystem – Vision i form av en demonstrator. Slutrapport. Skövde 2010.

vårdrelaterade artiklar är litet. De domineras av en enskild forskare (bilaga 3, 13 av 33 publikationer). Ändå är mönstret talande för perspektivskillnader.

Skillnader i nyckelord speglar tydliga perspektivskillnader, skydd av tekniska system mot yttre hot, cyberattacker, kontra skydd av patientuppgifter mot inre hot, anställdas felaktiga hantering av patientuppgifter. Det externa perspektivet dominerar forskning om it- och informationssäkerhet. I forskningsöversikter ligger tonvikten på systemlösningar mot obehörig tillgång till och användning av system och nätverk.[47] Det bekräftas av en Libris-sökning på avhandlingar på området (bilaga 4, 97 publikationer). Återkommande ämnen är systemutveckling för detektion av skadlig kod, effektiv autentisering och åtkomstkontroll. Styrning och uppföljning av informationssäkerhetsarbetet, till exempel informationsklassning, är perifera frågor. Inriktningen är dock inte självklar. Ansvaret för informationssäkerhet ligger på verksamhetsledningen. I vården ingår det i kvalitetsledningsarbetet och den övergripande informationsstyrningen. Svensk forskning på området är dock begränsad och fragmenterad. Verksamhetsnära systemutveckling är utan tvivel en viktigare fråga för vårdrelaterad forskning på området, men det är svårt att urskilja forskning om vårdens informationsstyrning som sådan, dvs. processer för utarbetande och uppföljning av verksamhetens säkerhets- och kvalitetskrav på informationshantering, system och teknik.



Figur 2. Nyckelord i forskningspublikationer om it- och informationssäkerhet
Vänster figur representerar frekvenser av nyckelord (tio-i-topp) i 259 rubriker och 225 sammandrag (abstract) i icke vårdrelaterade publikationer om informationssäkerhet av svenska forskare. Höger figur representerar frekvenser av nyckelord (tio-i-topp) i 33 rubriker och 30 sammandrag i vårdrelaterade publikationer av svenska forskare på området. Nyckelordet ”technology” inkluderar även ordfrekvenser för ”machine” och ”computer”; ”employee” inkluderar även ”staff” och ”personnel”.

[47] Löfvenberg, Jacob. 2010. En översikt över IT-säkerhetsforskning i Sverige. Rapport. Totalförsvarets forskningsinstitut. FOI-R--3069--SE. Jämför med MSB:s sammanställning av informationssäkerhetsforskning: https://www.informationssakerhet.se/Global/Kompetensutveckling/Informationssakerhetsforskning.pdf

PubMed är den främsta sökmotorn för internationella forskningspublikationer på hälso- och sjukvårdsområdet. Flera söktermer är relevanta för en lägesbild av forskning om informationssäkerhet i vården. MeSH-termerna ”Health Care Category” och ”Information Science Category” rymmer drygt 8,4 respektive 3,2 miljoner artiklar.[48] MeSH-termen ”Medical Informatics”, avseende datoriserad hantering av medicinska data, omfattar drygt 327 000 artiklar. MeSH-termerna ”Computer Security” och ”Privacy” (personlig integritet) ger 5 295 respektive 11 314 artikelträffar. Söksträngarna ”information security” och ”cyber security” resulterar i 312 respektive 27 träffar. Forskningsintresset kan inte sägas vara något annat än svalt. Det bekräftas av en jämförelse av artikelträffar med PubMed och i Mediearkivet. Förhållandet mellan antalet artikelträffar för ”information security” och ”healthcare” är 1:3 000 i PubMed. I Mediearkivet är förhållandet mellan ”informationssäkerhet” och ”sjukvård” 1:200. Med andra ord, nyhetsintresset för informationssäkerhet i vården kan sägas vara högre än forskningsintresset.

Utvecklingen av forskningen på området är också svag över tid. Sökningar med PubMed visar att cirka 3,9 % av alla artiklar i ”Health Care Category” klassas även som ”Medical Informatics”, cirka 0,1 % som ”Computer Security” och cirka 0,2 % som ”Privacy”. I diagram 4 skildras utvecklingen över tid. Informatikrelaterade publikationer ökar, men forskningsfrågor om säkerhet och personlig integritet är marginella och stabila över tid.

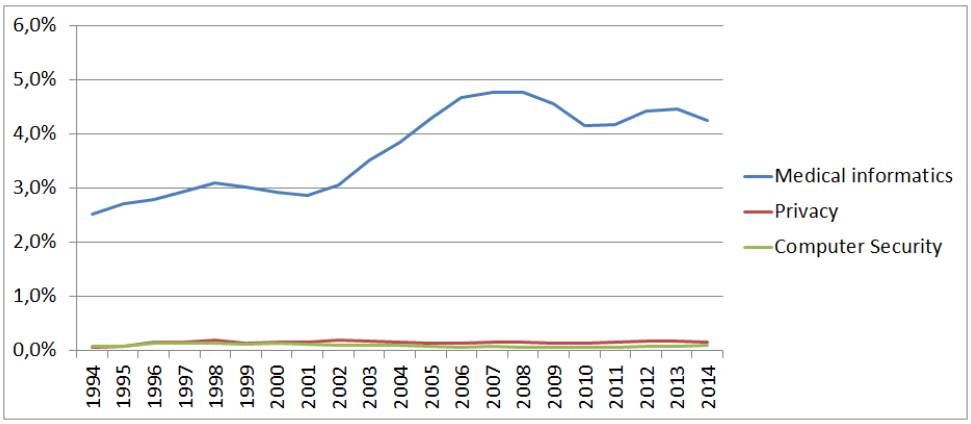


Diagram 4. Forskningsartiklar om hälso- och sjukvård
Diagrammet visar andel artikelträffar i PubMed av alla träffar för MeSH-kategorin ”Health Care Category” som även är klassade med MeSH-termerna ”Medical Informatics”, ”Privacy” och ”Computer Security”. Under 2000-talet har andelen artiklar om datoriserad medicinsk informationshantering ökat, samtidigt som andelen artiklar om it-säkerhet (MeSH ”Computer Security”) respektive personlig integritet (MeSH ”Privacy”) har varit oförändrad.

[48] Antalet avser resultat av sökning 2014-12-18.

Forskning om informationssäkerhet i vården är generellt begränsad. Specifika frågor om uppföljning är än mer sällsynta. En sökning på ”information security” och ”audit” resulterade i tolv träffar, varav endast en berörde faktisk uppföljning av informationssäkerhet i vården.[49]. Uppföljning och utvärdering av it-system i vården är dock generellt eftersatt.[50] Effekter av att införa nya informationssystem och e-hälsa utvärderas sällan systematiskt. Riskerna med bristande och felaktig vårddokumentation är inte heller klarlagda.[51,52,53] Det som ändå görs på området verkar inte heller kunna tas tillvara.

ECRI, ett oberoende forskningsinstitut, publicerar årligen rankningslistor av patientsäkerhetsrisker och medicintekniska risker. Risker med bristande eller felaktig vårdinformation hamnar i topp.[54] I Socialstyrelsens senaste lägesrapport inom patientsäkerhetsområdet tas inte dessa risker upp explicit, även om de framkommer indirekt, till exempel bristfällig vårddokumentation i form av underrapportering av vårdskador.[55] Det stora gapet mellan ECRI:s riskanalyser och svenska prioriteringar väcker frågor om riskernas natur. Är det fråga om nationella skillnader i verkliga vårdrisker? Eller är det fråga om skillnader i styrning och uppföljning av informationssäkerhetsfrågor?

> *[…] there is a dearth of empirical literature that considers the relationship between the configuration of security practices and compliance.*[56]

I en studie av informationssäkerhetsarbetet på 204 sjukhus i USA framkom en rad samband mellan kontrollarbetet i praktiken, regelefterlevnaden och nivån på säkerhetsincidenter.[57] Sjukhusen kunde grupperas i tre mognadsklasser: hög (A), mellan (B) och låg (C). Dessa var jämförbara i fråga om teknisk it-säkerhet, men skilde sig med avseende på administrativa kontroller, dvs. styrdokument, rutiner, uppföljning och kravställningar. Ju större engagemang i

---

[49] Kwon, J., & Johnson, M. E. (2012). Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association, amiajnl-2012.
[50] Black AD, Car J, Pagliari C, Anandan C, Cresswell K, Bokun T, McKinstry B, Procter R, Majeed A, Sheikh A. The impact of eHealth on the quality and safety of health care: a systematic overview. PLoS Med. 2011 Jan 18;8(1).
[51] Bowman S. Impact of electronic health record systems on information integrity: quality and safety implications. Perspect Health Inf Manag. 2013 Oct 1;10:1c.
[52] Sharp L, Klinga C och Hansson J. Elektronisk patientjournal riskerar patientsäkerheten. Läkartidningen. 2014;111:CRDD.
[53] Koch, S. Säkra den elektroniska journalen! Läkartidningen. 2014;111:2.
[54] Information om ECRI:s riskrankningar, inklusive bedömningar av risker med "Data Integrity: Incorrect or Missing Data in EHRs and Other Health IT Systems", finns på institutets hemsida *https://www.ecri.org/* samt i följande publikationer: Top 10 Patient Safety Concerns for Healthcare Organizations. 2014 ECRI Institute. Top 10 Health Technology Hazards for 2015. 2014 ECRI Institute.
[55] http://www.socialstyrelsen.se/publikationer2014/2014-4-7
[56] Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. J Am Med Inform Assoc. 2013 Jan 1;20(1):44-51.
[57] Ibid.

administrativa kontroller, desto högre var regelefterlevnaden och desto färre säkerhetsincidenter.

> *[…] security breaches are not directly related to perceived regulatory compliance, but related to hospitals' security practice patterns.*[58]

4.2 Vårdgivarnas uppföljning

I det här avsnittet presenteras resultatet av begäran om riktlinjer och rapporter från landsting och kommuner. Det omfattar redovisning av svarsfrekvenser och innehållsanalys av dokumentation. I tabell 2 återges generella svarsmönster. Av skäl som har nämnts i metodkapitlet ska inte resultatet ses som fullständigt eller uttömmande för sjukvårdshuvudmännens dokumentation. Resultatet bör dessutom tolkas i ljuset av osäkerheten som gäller för diarieföring.

Tabell 2. Resultat av förfrågan om dokumentation av relevans för vårdgivarnas uppföljning och rapportering av informationssäkerhet

Typ av dokumentation	Antal	
	Landsting	Kommuner
Skriftligt svar om diarieförda rapporter	21	244
Informationssäkerhetspolicy eller riktlinjer	20	107
Årsrapporter enligt SOSFS 2008:14	7	0
Patientsäkerhetsberättelse 2013	21	224
Revisioner it- och informationssäkerhet	16	47
Årsredovisning 2013	21	Ej aktuellt
Dokumentation om avvikelsehantering	14	Ej aktuellt
Dokumentation om incidenthantering	7	Ej aktuellt

4.2.1 Landstingens riktlinjer och årsrapporter

Av 21 regioner och landsting delgav 20 riktlinjer för informationssäkerhet.[59] I två fall finns det en explicit hänvisning till rapporteringskravet i SOSFS 2008:14. I fyra andra fall görs en implicit hänvisning, dvs. samma krav men utan explicit referens till föreskriften. Sju landsting saknar mål eller krav på uppföljning och rapportering av förebyggande insatser; nio landsting saknar det för incidenthantering.[60] I övriga fall finns det mer eller mindre explicita krav på uppföljning och rapportering. Här följer några exempel:

> *Revision och granskning av informationssäkerheten ska genomföras kontinuerligt, dock minst en gång om året, och rapporteras till ansvarig nämnd, styrelse eller bolagsstyrelse (Västra Götalandsregionen).*

---

[58] Ibid.
[59] Örebro läns landsting hänvisar till att beslut om policy tas under februari 2015.
[60] Vaga hänvisningar till "årlig uppföljning" utan mål eller krav på rapportering i ledningen räknas inte som ett rapporteringskrav. Inte heller räknas vaga hänvisningar till allas ansvar för incidentrapportering utan ledningsmål eller krav på uppföljning.

Uppföljning av informationssäkerhetsarbetet ska genomföras årligen, dels genom egenkontroller i respektive verksamhet, dels med hjälp av säkerhetsdialogen, riktade undersökningar och mätningar. Denna uppföljning ska sammanställas av informationssäkerhetsansvarig och rapporteras till landstingets ledning (Landstinget Sörmland).

RH-Check är verksamhetens egenkontrollverktyg för arbetet med risk och säkerhet. RH-checklistorna ska användas minst en gång per år. Informationssäkerhetsansvarig och IT-säkerhetsansvarig tar årligen fram en rapport som visar statistik och trender ur avvikelsesystemet Synergi som rör informationssäkerhet (Landstinget i Östergötland).

Sju landsting har delgett en årsrapport av informationssäkerhetsarbetet, varav fem innehåller en explicit hänvisning till SOSFS 2008:14. Tre av sju rapporter har en disposition i enlighet med föreskriften. Ett exempel återfinns i bilaga 5, årsrapporten från Jämtlands läns landsting, vars disposition är helt i linje med föreskriftens krav. Rapporten är en av de fylligaste och tjänar sitt syfte.

Landstinget i Uppsala län har delgett den fylligaste årsrapporten (bilaga 6–9). Ingen explicit hänvisning görs till föreskriften, men innehållet svarar både mot dess krav och mer därtill. Framför allt är det värt att notera att Landstinget i Uppsala län knyter samman krav på central och lokal uppföljning, något som inte berörs i föreskriften. I lokal egenkontroll (bilaga 7–8) redovisas till exempel lokala riskanalyser som sedan sammanställs i årsrapporten på central nivå. Av rapporten framgår samtidigt att det återstår arbete med samordning och lokal förankring av egenkontrollen, till exempel avvikelsehantering. I övrigt täcker årsrapporten in flertalet efterfrågade punkter i föreskrifterna, även avvikelser i verksamheten och it-incidenter. Den motiverar revideringar av egenkontrollen och prioriteringar av åtgärder (bilaga 9). Årsrapporten visar samtidigt prov på ett traditionellt it-säkerhetsperspektiv och lämnar inget utrymme åt frågor om verksamhets- och processtyrning av vårdinformation och dokumentation. Inget nämns om verksamhetens säkerhets- och kvalitetskrav på vårdinformation. Däremot omnämns säkerhetsklassificering av fysiska datorer. Inget nämns om kvalitetsgranskningar. Egenkontrollen är inriktad på drift- och systemsäkerhet, åtkomst- och behörighetskontroller. I rapporten nämns att det återstår arbete kring förankring av egenkontrollen och att det finns osäkerhet i verksamheten hur avvikelser ska rapporteras på området. Det är tänkbart att det beror på det systemtekniska perspektivet med begränsad relevans för vården.

Varken Jämtlands läns landsting eller Landstinget i Uppsala län tar upp kravet på rapportering enligt SOSFS 2008:14 i sina riktlinjer på området. I Jämtlands fall sker rapporteringen på initiativ från beredskapschefen efter att kravet kom till personlig kännedom. I riktlinjen för Uppsala län betonas lokal egenkontroll och att den centrala informationssäkerhetsfunktionen ska sammanställa lokala uppgifter. Det finns dock inget i riktlinjen som motiverar en central årsrapport i linje med SOSFS 2008:14. Tvärtom, riktlinjen utelämnar kravet. Sambandet mellan riktlinjer och årlig rapportering är oklart även för övriga landsting. De

som har krav i riktlinjer har inte alla delgett en årsrapport. De som har delgett årsrapporter har inte alla explicita krav. Det är dessutom tveksamt om de som har delgett årsrapporter verkligen uppfyller kraven i SOSFS 2008:14.

I Västra Götalandsregionen ingår årsrapporten om informationssäkerhet i den årliga säkerhetsredovisningen (utdrag i bilaga 10). Den bygger på ett formulär om säkerhetsläget och insatser som besvaras av regionens 45 förvaltningar och bolag. Resultatet för hälso- och sjukvården, elva förvaltningar, redovisas separat. Cirka 25 frågor är av direkt relevans för it- och informationssäkerhet (bilaga 11). Flertalet avser generella säkerhetsbedömningar. Några frågor kan dock sägas tjäna kraven i SOSFS 2008:14. Säkerhetsredovisningen skiljer sig från andra landsting genom en centralt styrd uppföljning. Egenkontroll i Landstinget i Uppsala län är till exempel inte centralt styrd, även om det finns gemensamma lathundar, mallar och system för avvikelserapportering.

Styrkan med central styrning är systematik, standardisering och jämförbarhet. Svagheten är bristen på lokal utvärdering av kontroller, risker och incidenter. Frågeformuläret är brett och täcker in riktlinjer, utbildning och efterlevnad av regler. I huvudsak handlar det om generella självskattningar av säkerhetsläget, behov och brister avseende hela sjukhusförvaltningar. Nivån på generalisering gör det svårt att avgöra de kriterier och underlag som vägleder bedömningar, till exempel frågan om förvaltningen har identifierat de viktigaste processerna och informationsmängderna samt om skyddsvärd information är klassificerad. Frågor om hur detta arbete bedrivs i praktiken förblir obesvarade. Hur görs det? När? Var? Av vem? Abstraktionsnivån gör att flertalet frågor om kontrollresultat förblir obesvarade, till exempel lokal loggguppföljning, avvikelsehantering och kvalitetsgranskning.

4.2.2 Andra verksamhetsrapporter från landsting

Verksamhetsrapportering sker på många nivåer. Den högsta nivån utgörs av landstingens årsredovisningar. För verksamhetsåret 2013 var det tre av dessa som berörde informationssäkerhetsfrågor: Stockholm, Västra Götaland och Östergötland. I de två första fallen omnämns i korta och generella ordalag nya styrdokument, utbildningsinsatser och it-säkerhetsrisker. I Östergötlands årsredovisning omnämns egenkontrollen, hur stor andel av landstingets enheter som har använt kontrollverktyget RH-check år 2013 i jämförelse med 2012 (61 % respektive 37 %). I Västra Götalands fall är informationssäkerhet som en stående punkt, något som gissningsvis beror på regelbunden och systematisk säkerhetsredovisning. Detsamma gäller punkten RH-check i Östergötland.

Årsredovisningar från övriga landsting kan beröra informationssäkerhet, men då i förbigående i samband med andra frågor. Här är ett exempel hämtat från Gotlands årsredovisning:

> *Under året togs viktiga steg när förvaltningen inledde ett omfattande projekt inom e-hälsoområdet som bland annat omfattar digital hantering av olika tjänster,*

säkrare inloggning i verksamhetssystemen, tillgång till journaler och dokumentation via till exempel smarta telefoner och surfplattor.

Samtliga regioner och landsting har delgett en patientsäkerhetsberättelse 2013. I ett fall omnämns informationssäkerhet, Östergötland, kontrollverktyget RH-check. I övrigt berörs inte området explicit i patientsäkerhetsberättelser, även om det berörs sporadiskt inom ramen för andra frågor. Dessa listas som följer, genomgående kortfattade aktivitetsredovisningar:

Landstingen Blekinge, angående säker läkemedelshantering:

- Blekingesjukhuset har genomfört en stickprovskontroll, omfattande 20 journaler per klinik, för att kontrollera om det funnits ett särskilt utskrivningsmeddelande inklusive läkemedelslista och läkemedelsberättelse. Resultaten varierade alltifrån att knappt hälften av journalerna till att drygt 90 procent innehöll dylikt ”utskrivningsmeddelande”.

Landstinget Dalarna, angående läkemedelsfel i vårdens övergångar:

- Journalgranskning under två veckor riktat mot förekomst av läkemedelsberättelse, att innehållet är riktat till patienten och att patienten fått en läkemedelsberättelse vid utskrivning. Resultaten visade att 96 % av de granskade journalerna höll måttet.

Landstinget Gävleborg, angående anmälningar till patientnämnden:

- En tredubbling har skett av ärenden rörande journal- och sekretessfrågor.

Landstinget i Värmland, angående årets 64 lex Maria-anmälningar:

- Bristerna inom dokumentation handlar framför allt om avsaknad av journalanteckningar, ej dokumenterade uppgifter såsom anamnes, undersökningsfynd, konsultationer, telefonsamtal och riskbedömningar, vilket medför en begränsad spårbarhet i patientens vård och behandling.

Norrbottens läns landsting, angående loggkontroller:

- Loggkontroller enligt fastställd rutin genomförs regelbundet av personalens åtkomst till patientjournal (inga resultat delges).

Västerbottens läns landsting, angående uppföljning genom egenkontroll:

- Läkemedelslistans korrekthet granskas fyra gånger/år (primärvård, öppen- och slutenvård) (resultat redovisas).

Inhämtande eller genomgång av regionala verksamhetsrapporter har i några fall motiverat kompletteringar med lokal rapportering. Region Halland har till exempel beslutat att lägga ansvaret för årsrapporten enligt SOSFS 2008:14 på enskilda vårdgivare i deras lokala patientsäkerhetsberättelse. Hallands sjukhus redovisar mycket riktigt informationssäkerhetsarbetet i sin berättelse för 2013. Redovisningen är kortfattad och inriktad på frågor om it-säkerhet. Det saknas

information om verksamhetens logguppföljning, kvalitetssäkring och incidenthantering.

Generellt är lokal rapportering sällsynt. Om den finns är den kortfattad. Det gäller bland annat patientsäkerhetsberättelser från Karolinska och Sahlgrenska universitetssjukhusen. Karolinska lyfter fram nya satsningar på ledningssystem och samordning samt nämner driftproblem med TakeCare, journalsystemet. I Sahlgrenskas fall är it- och informationssäkerhet en kategori i avvikelsestatistiken. I ett fall har en lokal årsrapport påträffats som redovisar kontrollarbetet i praktiken, Värnamo sjukhus.

Värnamo sjukhus årsrapport redovisas i sjukhusledning och tar kortfattat upp olika säkerhetskontroller och organisationsfrågor, riskanalyser, åtgärder och avvikelser. Avvikelserapporteringen är till exempel strukturerad med avseende på informationssäkerhetsområdets fyra riskområden (tabell 3). Statistiken bör tolkas mot bakgrund av att antal avvikelser i första hand speglar rutiner och praxis för uppföljning hos personalen, inte att en organisation har större eller fler problem än andra organisationer.[61] Årsrapporten illustrerar att uppföljning av informationssäkerhetsfrågor förekommer på ledningsnivå, men också att det är sällsynt av allt att döma.

Tabell 3. Avvikelsestatistik i ledningsrapport om informationssäkerhet på Värnamo sjukhus

Typ av avvikelse	Antal
Riktighet	42
Sekretess	9
Spårbarhet	14
Tillgänglighet	43
Övrigt	65
Totalt	173

4.2.3 Kommunernas riktlinjer och rapporter

Av 290 kommuner har 209 delgett svar om informationssäkerhetspolicy eller riktlinjer. I 30 fall är svaret explicit att policy eller riktlinje saknas. I 72 fall har andra riktlinjer än de begärda delgetts, till exempel säkerhets- eller it-policy. I resterande 107 fall har explicit informationssäkerhetspolicy eller riktlinjer delgetts. Två av dessa är riktlinjer från socialförvaltningen, men där det saknas policy för kommunen i sin helhet. Utöver riktlinjer för informationssäkerhet har 23 kommunala vård- och omsorgsförvaltningar sänt riktlinjer för hantering av vårdinformation och dokumentation. Dessa behandlar inte generella frågor om styrning och uppföljning, utan består av enskilda regler och rutiner för

[61] För att styra och utvärdera säkerhetsinsatser är det mer värdefullt att jämföra andel avvikelser än absoluta antal, till exempel att andel avvikelser rörande riktighet och tillgänglighet dominerar (tabell 3). Avvikelsehantering diskuteras närmare i ett senare avsnitt.

hantering av vårdsystem och patientuppgifter. I en del fall berörs rutiner för logguppföljning av vårddokumentation. I det följande diskuteras policyer eller riktlinjer som explicit benämns informationssäkerhet.

Cirka 2 av 3 styrdokument (70 av 107) anger krav på årlig uppföljning, men utan specifika krav på rapportering. Tre styrdokument innehåller krav på central rapportering av informationssäkerhetsinsatser till kommunledningen. Ett dokument innehåller krav på central uppföljning och rapportering av säkerhetsincidenter. Mindre än hälften av styrdokumenten som ställer krav på uppföljning (30 av 70) preciserar att uppföljningsmål och plan formuleras inom ramen för årliga verksamhetsmål och planer. Efter kontakt med ansvarig nämnd eller förvaltning för vård och omsorg har 1 av 30 kommuner delgett sådana mål och planer.

En översiktlig genomgång visar att cirka hälften av riktlinjerna bygger på en mall för informationssäkerhetspolicyer och riktlinjer som har publicerats av Kommunförbundet Stockholms län (november 2010).[62] Det går inte att avgöra omfattningen på återanvändning i detalj eftersom mallen tjänar som grund för anpassning, utveckling och spridning av dokument mellan kommuner.

I fråga om uppföljning är det speciellt en del i policymallen som återkommer i kommunernas egna styrdokument:[63]

> ***Revidering och uppföljning***
>
> *Uppföljning är en viktig del i informationssäkerhetsarbetet. Uppföljningen ska bevaka:*
>
> - *att beslutade åtgärder är genomförda*
> - *att årliga mål är uppfyllda*
> - *att regler och riktlinjer följs*
> - *att systemsäkerhetsplaner och policydokument vid behov revideras.*

I mallen finns även förslag till årliga mål och planer för uppföljning, men det är krav som förekommer sparsamt i kommunernas styrdokument (cirka hälften av fallen). I mallen finns vidare en hänvisning till en vägledning från Kris- och beredskapsmyndigheten (KBM), föregångare till MSB: ”Basnivå för informationssäkerhet (BITS). KBM rekommenderar 2006:1”.[64] Vägledningen beskriver administrativa åtgärder för att uppfylla en grundläggande säkerhetsnivå på området. Den tar upp vikten av rutiner för rapportering av säkerhetsincidenter samt betydelsen av revision av informationssystem. Inget

---

[62] Pdf-dokument finns på följande hemsida:
http://www.ksl.se/svenska/vara-uppdrag/andra-verksamheter-inom-ksl/it-forum-stockholms-lan/informationssakerhetsarbete.html
[63] Pdf-mall för informationssäkerhetspolicy. IT-forum. Ibid.
[64] Engelsk version av vägledningen ”Basnivå för informationssäkerhet (BITS)”:
http://www.msb.se/Upload/Produkter_tjanster/Publikationer/KBM/Basic%20Level%20for%20Information%20Security.pdf

nämns generellt om värdet av eller krav på central uppföljning och rapportering av säkerhetskontroller och resultat. Det är tydligare uttryckt i en senare vägledning från MSB, ”Kommunens informationssäkerhet”, som utgår från aktuella internationella standarder, ISO/IEC 27000-serien.[65] Denna vägledning har hittills dock inte haft något genomslag på kommunernas styrdokument.

I tre fall har specifika riktlinjer för informationssäkerhet delgetts från nämnder med ansvar för vård- och omsorg. Dessa är inriktade på administrativ säkerhet, hantering, lagring, utelämnande och gallring av patientuppgifter, behörighets- och åtkomstkontroll, signering, logguppföljning och sekretess.

Totalt har 244 kommuner delgett svar på förfrågan om diarieförda rapporter om informationssäkerhet. I 123 fall kom svaret från en nämnd eller förvaltning inom vård, omsorg eller socialtjänst. I 22 fall kom svaret från it-förvaltningen. I resterande fall kom svaret från det centrala diariet eller kommunledningens centrala administration. I några fall uppges svaret följa på intern samordning mellan nämnder eller förvaltningar. Det är oklart hur ofta så har skett. I flera fall är flera personer cc:ade i ett svar, vilket tyder på att svaret har föregåtts av intern samordning utan att det sägs explicit.

Av 244 kommuner meddelade 137 (56,1 %) att de saknar diarieförda rapporter inom ämnesområdet. Ingen kommun delgav en årsrapport i linje med SOSFS 2008:14. I 15 fall var svaret explicit att kommunen inte kände till eller att de inte följde föreskriften. Flera kommuner hörde av sig på telefon och meddelade att de inte kände till föreskriften.

Av svarande kommuner har 44 delgett minst en revision om it-, informations- eller dokumentationshantering för perioden 2011–2013, inklusive 17 revisioner med inriktning specifikt på it- och informationssäkerhet (7,0 %). Innehållet i revisionerna diskuteras i ett senare avsnitt. Utöver revisioner har 8 kommuner delgett systemsäkerhetsanalyser och utredningar av enskilda säkerhetsfrågor, till exempel DNSSEC, nätverk och penetrationstester. Vidare har 15 kommuner delgett resultat från internkontrollen, framför allt logguppföljning och kontroll av behörigheter och användarkonton, men även generella kontroller, till exempel kännedom om informationssäkerhetspolicy på ledningsnivå (Malmö). I fråga om internkontroll utmärker sig Skellefteå genom att inkludera en rad kontrollpunkter för informationssäkerhet (bilaga 12). Det är värt att notera att kvalitets- och säkerhetskrav, dvs. *konfidentialitet, riktighet, tillgänglighet* och *spårbarhet*, strukturerar redovisningen.

Kommunernas och landstingens patientsäkerhetsberättelser liknar varandra till stora delar. Flertalet är inriktade på att beskriva och redovisa arbetet med

[65] Kommunens informationssäkerhet – en vägledning. 2012. Myndigheten för samhällsskydd och beredskap (MSB): https://www.msb.se/RibData/Filer/pdf/26420.pdf

nationella indikatorer för patientsäkerhet. I kommunala berättelser lämnas dock mer utrymme åt kvalitetsgranskning och loggguppföljning av journaler. Av 224 patientsäkerhetsberättelser från år 2013 berördes dessa två kontroller i 37 respektive 23 fall (16,5 % respektive 10,3 %). I flertalet fall nämns kontroller och resultat i några få meningar, till exempel *att loggguppföljning har genomförts enligt rutin utan anmärkning*. Redovisning av kvalitetsgranskning av journaler tenderar att vara något mer utförlig med motsatt resultat. Kvalitetsproblem är snarare regel än undantag, till exempel utebliven signering och ofullständiga vårdplaner. I ett par fall är kvalitetskontroller av utförligare karaktär. Alvesta och Osby redovisar systematiska kontroller. I tabell 4 återges en tabell i Osby, ett exempel på en sällsynt form av redovisning, en systematisk sammanställning av kontrollresultat i kvalitetsgranskningar. I rapporten kompletteras denna med redovisning av åtgärder, till exempel utbildning och nya rutiner, i andra fall kompetensutveckling för enskild personal.

Tabell 4. Återgivning av resultattabell i Osbys patientsäkerhetsberättelse 2013

	2011	2012	2013
Granskning av omvårdnadsjournaler	**Ja (%)**	**Ja (%)**	**Ja (%)**
1. Finns fullständiga uppgifter om patientens identitet?	100	100	100
2. Finns notering om omvårdnadsansvarig sjuksköterska?	78	80	93
3. Finns notering om patientansvarig läkare?	61	75	91
4. Finns notering om anhörig/närstående?	94	95	97
5. Finns notering om att lämna samtycke att lämna uppgifter till annan vårdgivare?	50	55	82
6. Finns aktuell vårdstatus?	33	40	56
7. Finns det en individuell vårdplan?	78	78	83
8. Är tidpunkten för vårdåtgärderna tydligt angivna?	94	100	100
9. Är omvårdnadsjournalen skriven på ett för patienten tydligt och lättförståeligt sätt?	100	100	100
10. Är journalen skriven på ett sätt som uppfattas som god journalföring?	100	100	100

4.2.4 Revisioner

Landstingen och kommunerna har delgett 72 revisioner för efterfrågade årtal 2011–2013. För att kontrollera underlaget genomfördes sökningar efter revisionsrapporter på hemsidorna för alla landsting och kommuner, inklusive landstings- och kommunrevisionens undersidor. Det innebar att ytterligare två rapporter kunde inkluderas för perioden. Därtill delgav landsting och kommuner 12 äldre revisioner samt 5 revisioner för 2014.

En del revisioner berörde informations- eller it-verksamhetens struktur. Andra revisioner var begränsade till it-säkerhet eller berörde specifika teknikfrågor. Efter granskning kunde mindre än hälften av revisionerna (38) sägas omfatta både organisatorisk och teknisk informationssäkerhet (lista på revisioner i bilaga 13). Efter klassificering och sammanställning av innehållet står det klart att it- och systemsäkerhetsperspektivet dominerar (tabell 12).

Den röda tråden är förekomst av riktlinjer, ansvarsroller och kontroller för system- och nätverkssäkerhet, behörighet och åtkomst. Riktlinjernas innehåll,

betydelse och kvalitet berörs sällan. Det gäller även informationsklassning. I vissa fall berörs personalens kännedom om riktlinjer, men inte i något fall går revisionerna in på säkerhetskultur, riskmedvetenhet och beteendemönster. Frågor om riskanalys och logguppföljning i verksamheten är sällsynta. Frågor om uppföljning och rapportering intar också en blygsam roll. I endast två fall berördes vårddokumentationens kvalitet.

Tabell 5. Innehållsanalys av 38 revisioner av generell informationssäkerhet i landsting och kommuner. Tabellen återger antal och andel (%) revisioner som granskar förekomst av 16 typer av säkerhetskontroller

Typ av säkerhetskontroll	Antal	%	Typ av säkerhetskontroll	Antal	%
Regelverk: policy, riktlinjer och formella krav	38	100 %	Verksamhetskontroller: leveransavtal och prestationer (interna och externa)	13	34 %
Ledning och styrning: roller, ansvar och revision	34	90 %	Kontinuitetshantering: reservrutiner och resurser	12	32 %
Systemutveckling och förvaltning: testning, redundans och uppdatering	30	79 %	Incidenthantering: störningsrutiner och resurser	7	18 %
Behörighetskontroller: autentisering, spärrar och loggar	29	76 %	Händelsekontroller: märkning, signering, loggning av aktiviteter	7	18 %
Informationsklassning: skyddsvärde och behov	22	58 %	Riskhantering: identifiering och prioritering av risker	6	16 %
Personkontroller: bakgrund och kompetens hos personal	22	58 %	Uppföljning: regelbunden resultatrapportering	6	16 %
Fysiska kontroller: it-miljöer och utrustning	21	55 %	Kvalitetskontroller: rätt information och korrekta data	2	5 %
Nätverkskontroller: brandväggar, antivirus och kryptering	19	50 %	Säkerhetskultur: medvetenhet och beteendemönster	0	0 %

4.2.5 Avvikelser i vårdverksamhet

Sjutton landsting har delgett dokumentation om system för avvikelsehantering och incidenthantering:

- 6 om både avvikelsehantering och incidenthantering
- 10 om bara avvikelsehantering
- 1 om bara incidenthantering.

I 4 av 16 system för avvikelsehanteringen 2013 ingick ”informationssäkerhet” som en avvikelsekategori, dvs. typ av ärende eller kategori av händelse. I 4 av 16 system var området en mixad kategori: ”it-/informationssäkerhet” (3) och ”informationssäkerhet/sekretess” (1). Efter 2013 har området tillkommit som unik och mixad kategori i ytterligare två system.

Sju landsting delgav statistik för 2013. Andelen avvikelser inom informationssäkerhet låg under 2 % för 4 av 7 (unik eller mixad kategori). För Landstinget i Jönköpings län, Västra Götalandsregionen och Östergötland ligger andelen avvikelser över 2 %.

Landstinget i Jönköpings län har i särklass den högsta rapporteringsgraden, drygt 20 % av avvikelserna 2013 klassades som informationssäkerhet. Vidare används kvalitets- och säkerhetskrav som underkategorier: *konfidentialitet, riktighet, tillgänglighet och spårbarhet* (tabell 6). Exempel på avvikelser för underkategorierna finns i en lathund (bilaga 14). Verksamhetsperspektivet är tydligt och står i kontrast till det mer traditionella it-perspektivet.

Tabell 6: Avvikelser inom informationssäkerhet i Landstinget i Jönköpings län för år 2013

Avvikelser inom informationssäkerhet	**Antal**	**Andel**
Riktighet	528	28,6 %
Sekretess	48	2,6 %
Spårbarhet	78	4,2 %
Tillgänglighet	518	28,0 %
Ospecificerat	675	36,5 %
Summa info.säk.	1 847	*20,6 %*
Totalt antal avvikelser i landstinget	*8 948*	

Avvikelsehanteringen av informationssäkerhet i Landstinget i Jönköpings län speglar ett medvetet och aktivt engagemang för verksamhetsrapportering av avvikelser på området, inte att landstinget skulle ha större problem än andra. I första hand är det ledning och styrning av avvikelserapportering som påverkar frekvenser av avvikelserapporter, inte faktiska problem. Underrapportering av avvikelser är utbrett och välkänt, varför ledningens prioriteringar är av stor vikt. Antalet rapporter kan därför inte tjäna som grund för jämförelser mellan landsting.[66] Försiktighet i jämförelser följer också av att landstingen använder sig av olika klassificeringssystem för avvikelser.

I Västra Götalandsregionen är andelen avvikelser för informationssäkerhet 6,6 % (3 395 av 51 595 avvikelser). I detta fall rör det sig om en mixad kategori: ”it-/informationssäkerhet”. Underkategorier visar att det stora flertalet avvikelser rör problem med tillgänglighet: inloggningsproblem, datorstopp,

[66] Noble, Douglas J., and Peter J. Pronovost. "Underreporting of patient safety incidents reduces health care's ability to quantify and accurately measure harm reduction." Journal of patient safety 6.4 (2010): 247-250.

långa svarstider, funktionsfel samt telefoni- och faxproblem. Underkategorin ”obehörig åtkomst” är sparsamt förekommande, 43 avvikelser. Samtidigt finns det en underkategori ”sekretess” under kategorin ”organisation, regler och resurser” med 105 avvikelser. Det illustrerar ett generellt problem på området, att risker och avvikelser av relevans för informationssäkerhet kan återfinnas i olika verksamhetsprocesser och system.

I avvikelsehanteringen i Landstinget i Östergötland finns det en unik kategori för informationssäkerhet med 5,1 % avvikelser för år 2013 (1 683 händelser på 32 871 ärenden).[67] Inga underkategorier ingår. It (informationsteknik) är en egen kategori. Den jämförelsevis höga andelen avvikelser på området speglar även i detta fall landstingets engagemang i kvalitetsledning, inte att det skulle vara mer drabbat än andra landsting.

Under 2013 var det bara två landsting som hade system för avvikelsehantering som omfattade underkategorier till ”informationssäkerhet”. Som redan har påtalats var Landstinget i Jönköpings län ett av dessa landsting, Region Halland var det andra. Deras underkategorier var följande: (1) *försummelse i efterlevnad av policy eller rutiner*, (2) *it-funktionsrelaterade problem* och (3) *sekretessbrott*. Dessa speglar ett traditionellt synsätt på informationssäkerhet, it-säkerhet och regelefterlevnad.

Från och med 2014 införde även Västra Götalandsregionen underkategorier till informationssäkerhet: (1) sekretess, (2) riktighet, (3) tillgänglighet och (4) spårbarhet. Informationssäkerhet särskiljs här från it och it-säkerhet.[68] För 2014 var antalet avvikelser på området sparsamt, 2,6 % av samtliga avvikelser. Däremot liknar fördelningen av avvikelser bland underkategorierna mönstret för Landstinget i Jönköpings län: sekretess 14 %, riktighet 31 %, tillgänglighet 21 %, spårbarhet 4 % och övergripande (ospecificerat) 30 %. Den låga andelen avvikelser tyder på att informationssäkerhet inte är omsatt i verksamhetskrav som kan skapa relevans i avvikelserapportering. Det återstår därför att se om risker och incidenter på området kan förankras i verksamheten. För tillfället saknas information om begreppsdefinitioner på området.

I landstingens avvikelsesystem finns det en rad avvikelsekategorier som är av relevans för informationssäkerhetsområdet, men som inte följs upp i statistik, sammanställningar eller analyser. För att exemplifiera följer nedan en lista på några avvikelsekategorier i Östergötlands system. De är kategorier på samma

[67] I Östergötlands patientsäkerhetsberättelse för 2013 uppges 32 305 avvikelser. I en separat statistikrapport hösten 2014 är antalet högre, 32 871. Diskrepansen är troligtvis en konsekvens av tidpunkten för utdrag. Antalet oavslutade ärenden från föregående år minskar över tid. Vidare, en och samma avvikelse, ett och samma ärende, kan rymma flera händelser, till exempel brister i läkemedelshantering och informationssäkerhet. Antalet händelser är därför större än antalet ärenden. I snitt går det 1,2 händelser på ett ärende.
[68] System: Platina respektive Medcontrol Pro.

systemnivå som informationssäkerhet (tabell 6). För år 2013 uppgick antalet händelser för dessa kategorier till 18 777, närmare 50 % av avvikelserna 2013. I princip kan några av dessa även vara klassade som informationssäkerhet, men flertalet är det inte. Ansvariga för avvikelseutredningar, verksamhetschefer, bedömer om och när en avvikelse faller inom informationssäkerhetsområdet. Det är oklart och tveksamt om det existerar någon sammanhållen uppföljning av avvikelser för vårdinformation och dokumentation. Avvikelsehantering är inriktad på patientsäkerhetsskador. Verksamhetsproblem och systemfel i informationshantering kommer i andra hand.

Tabell 6: Avvikelsekategorier i Östergötlands system (Synergi) av potentiell relevans för informationssäkerhet

Avvikelsekategori	Avvikelsekategori
Administration, ej patientrelaterad	Kund saknas på remiss
Information och kommunikation	Remisshanteringsfel
Samordnad vårdplanering	Underskrift saknas på remiss
Dokumentation	Remiss saknas
ID patient/kund fel/saknas	Provtagning/hanteringsfel
Förväxling	Provtagningsunderlag uttaget av beställare
Registreringsfel	IT (Informationsteknik)
Etikettfel	Medicinsk teknik
ROS (Remiss Och Svar)	

4.2.6 Orsaks- och händelseanalyser

Problemet med helhetssyn på kvalitet och säkerhet i vårddokumentation är än tydligare i orsaksanalyser. System för avvikelsehantering innehåller normalt även orsakskategorier. De varierar inte i lika hög grad som händelsekategorier. Ofta är källan Socialstyrelsens handbok för patientsäkerhetsarbete "Riskanalys och händelseanalys":[69]

- *Kommunikation & information (K)*
- *Utbildning & kompetens (U)*
- *Omgivning & organisation (O)*
- *Teknik, utrustning & apparatur (T)*
- *Procedurer, rutiner & riktlinjer (P).*

I handboken förklaras orsakskategorierna närmare. Brister i dokumentation och informationshantering kan vara en underkategori till samtliga kategorier, till exempel förväxling eller identitetsstöld (K), kunskapsluckor om it-system (U), kognitiv stress (O), systemfel (T) eller bristfällig rutin (P). Fyra landsting

[69] Webblänk till pdf-version av handbok:
http://www.socialstyrelsen.se/publikationer2009/2009-126-120

har delgett statistikuppgifter om orsakskategorier för år 2013, varav två har meddelat antalet avvikelser för varje kategori (tabell 7). Bristande riktlinjer och rutiner är i särklass den främsta orsaken till avvikelser. Det kan handla om att rutinen är eller upplevs bristfällig eller att den inte följs av ett eller annat skäl. Mönstret går igen i övriga landsting att döma av grafisk statistik.

I uppföljning av informationssäkerhetsfrågor kan det vara mer värdefullt att utvärdera orsakskategorier än avvikelsekategorier som bygger på begränsade system och olika tolkningar. Dels kan orsaksanalyser göra det möjligt att relatera patient- och informationssäkerhetsfrågor, om och när patient- och vårdavvikelser föranleder orsaksanalyser, dels kan orsaksanalyser vara en källa till osynliga och nya risker.

Tabell 7. Avvikelser 2013 klassificerade efter orsak

Orsakskategori för avvikelser	Västra Götaland		Östergötland	
Kommunikation & information (K)	13 994	27,1 %	4 100	18,4 %
Utbildning & kompetens (U)	1 786	3,5 %	992	4,4 %
Omgivning & organisation (O)	9 535	18,5 %	3 363	15,1 %
Teknik, utrustning & apparatur (T)	6 460	12,5 %	1 146	5,1 %
Procedurer, rutiner & riktlinjer (P)	19 901	38,5 %	12 700	56,9 %

Vid allvarligare avvikelser ska vårdgivaren genomföra händelseanalyser, dvs. grundligare utredningar av orsaker till vårdskador och möjliga åtgärder. För ändamålet finns det nationella it-stödet NITHA.[70] NITHA är en databas och ett metodstöd för standardisering, lagring och spridning av händelseanalyser mellan vårdgivare. I dagsläget finns det 455 slutförda analyser i den så kallade kunskapsbanken, där det går att söka och upprätta statistik på analyser. Analyserna kategoriseras efter typ av ärende (negativ händelse eller tillbud), typ av skada, typ av arbetsprocess där händelsen inträffade samt kategorier av orsaker på två nivåer.

I likhet med avvikelsehantering finns det typer och kategorier av händelser som berör informationssäkerhetsfrågor, men där det inte utan närmare analys går att bedöma relevansen. I tabell 8 återges frekvenser av analyser för de 20 typer av arbetsprocesser som ingår i NITHA. Flera typer är av relevans där det vore av värde med en närmare analys för att följa upp eventuella behov av åtgärder i informationssäkerheten, till exempel dokumentationshantering, identifikation, remisshantering med mera. Närmare information kan också erhållas genom de orsakskategorier som tillskrivs en händelse. De finns dels på samma generella nivå som i tabell 7 ovan, dels i form av 79 underkategorier. Några av dem är att betrakta som explicita informationssäkerhetsfrågor:

[70] Länk till webbsida: http://www2.lio.se/Startsida/Verksamheter/Halso--och-vardutvecklingscentrum/Utvecklings--och-patientsakerhetsenheten1/Patientsakerhet/For-sjukvarden/Verktyg-och-metoder/Handelseanalys-/Nitha/

- Brister avseende användargränssnitt, t.ex. display eller IT-program
- Brister avseende mjukvara
- Brister avseende tolkning av information
- Brister i agerande på tillgänglig information
- Brister i kontroll av identitet av person
- Brister i reservrutiner vid driftavbrott
- Brister i tillgång till journaluppgifter, ordination, PM m.m.

Tabell 8. Processkategorier i händelseanalys enligt NITHA (455 analyser 2015-01-22)

Typ av arbetsprocess	Antal	Typ av arbetsprocess	Antal
Behandling	143	Remisshantering	5
Diagnostik	111	Rådgivning	8
Dokumentationshantering	5	Service av fastighet	2
Handhavande av utrustning	5	Service av IT-utrustning	1
Identifikation	2	Service av medicintekniska produkter	2
Informationsöverföring	14	Svarshantering	1
Läkemedelshantering	29	Transport	2
Omvårdnad	52	Undersökning/utredning	40
Provhantering	6	Vårdplanering	2
Rehabilitering	3	Övervakning/observation	22

I egenskap av att vara nationell standard för händelseanalyser är det viktigt att reflektera över hur informationssäkerhetsfrågor beaktas i analysprocessen. Hur kan händelseanalyser tjäna som underlag för utvärdering av risker på området? I takt med att NITHA växer kan metodstödet också komma att påverka vårdens avvikelsehantering mer generellt, även om inte som nationell standard. Det kan till exempel påverka nationella granskningar och utvärderingar. Idag berörs inte informationssäkerhetsfrågorna explicit och det finns skäl att diskutera om och hur de kan beskrivas och göras relevanta i metodstödet.

4.2.7 It-incidenter

I kategorilistan för Östergötland (tabell 6) förekommer it och medicinsk teknik. I regel ingår de i landstingens system för avvikelsehantering och är att betrakta som tekniskt relaterade avvikelser i verksamheten. Det är dock oklart hur väl dessa fångar upp it-relaterade eller medicintekniska verksamhetsstörningar. Dessa kanaliseras inte sällan till it-förvaltningar, medicintekniska avdelningar eller enheter som använder sig av oberoende system för ärendehantering.

Sju landsting har delgett uppgifter om system för it-incidenthantering. Den generella rutinen är att enskilda it-användare gör felanmälan till det centrala it-stödet (servicedesk) som bedömer hur allvarligt ärendet är (tabell 9). Tre landsting, Västra Götalandsregionen (VGR), Landstinget Västernorrland (LVN) och Region Halland (RH), har delgett både dokumentation och statistik för år 2013. Närmare 161 000 ärenden registrerades i VGR. Ärendekategorier tre-i-topp var ”arbetsplats” (35,5 %), ”vårdapplikation och system” (23,6 %) och ”lösenord” (19,1 %). I LVN registrerades 8 562 ärenden med följande

tre-i-topp: ”serverdrift” (12,3 %), ”SYSteamCross” (5,2 %) och ”telefoni” (4,5 %). LVN använder mer finmaskiga incidentkategorier, varför andelen för den mest frekventa kategorin är jämförelsevis låg. It-avdelningen i Region Halland registrerade 42 110 ärenden, vars kategorier tre-i-topp var ”vårdsystem” (42 %), ”infrastruktur” (32 %) och ”teleservice” (10 %).

Tabell 9. Exemplifiering av kriterier för prioritering av it-ärenden i första linjens stöd (servicedesk) från Region Halland[71]

Prioritet	Beskrivning	Tidsgräns
5	Beställningar	20 arbetsdagar
4	Ej brådskande fel hos enskild användare som inte hindrar daglig verksamhet	10 arbetsdagar
3	Fel av enklare art som berör en mindre grupp eller allvarliga fel som berör enskilda användare	5 arbetsdagar
2	Systemavbrott som berör hel avdelning/förvaltning eller system med mer än 20 användare	8 timmar
1	Systemavbrott som berör större delen av användarna eller där människors liv och säkerhet kan påverkas	1 timme

I VGR krävde drygt 1 av 3 ärenden andra linjens stöd, expertstöd. I brist på uppgifter om prioritet kan det fungera som indikator på störningsnivån. Med andra ord är cirka 1 av 3 ärenden av ett något allvarligare slag. Det är i linje med Region Halland och LVN. Cirka 30 % av ärendena i Region Halland löstes inte av service desk (första linjen). LVN placerade 1 av 3 incidenter i prioritetsklass 1 eller 2 med ”serverdrift”, ”SYSteamCross” och ”bärbara” som tre-i-topp.

Även om landstinget omfattar fler verksamheter än vård indikerar statistiken i sin helhet att antalet ”it-incidenter i vården” är betydligt fler än ”it-relaterade verksamhetsavvikelser”, trots att it-incidenterna ofta berör vårdsystem och är av allvarligare slag. I VGR berör närmare 1 av 4 ärenden vårdapplikationer och system (cirka 40 000 ärenden), att jämföras med närmare 3 400 registrerade it-avvikelser. Det är oklart hur många av de senare som är registrerade som it-incidenter. Även om alla skulle vara det omfattar it-incidenterna inte alla avvikelser av relevans för informationssäkerheten i verksamheten. De första omfattar fel och problem med funktionalitet i it-system och tjänster och de senare berör verksamhetens informationshantering i sin helhet.

4.2.8 Klagomål från patienter

Patientklagomål är ytterligare en potentiell informationskälla till lägesbilder av informationssäkerhet i vården. Vanligtvis har vårdgivarna rutiner för hantering

[71] Källa: "Rutin: Incidenter IT (teknik) och IS (informationssäkerhet)". Region Halland. Dok ID: Incidenter IT/IS. Utgåva: 6 (2013-03-11).

av patientklagomål inom ramen för avvikelsehantering. Denna lider dock av en brist på standardisering. Landstingens patientnämnder har en mer samordnad hantering av patientklagomål med ett gemensamt system för ärendekategorier. Att döma av landstingens patientsäkerhetsberättelser är antalet ärenden till patientnämnder dessutom högre än antalet klagomål till vårdgivare.

I tabell 10 återges fördelningen av informationsrelaterade klagomål för 2014. De utgör cirka 17 % av samtliga patientklagomål till 17 av 21 patientnämnder. Det är i samma storleksordning som andelen avvikelser för ”informationssäkerhet” i Landstinget i Jönköpings län under 2013. Bristfällig vårdinformation till patienter eller närstående samt remisser och journalfrågor är de tre vanligaste klagomålen. Dessa typer av klagomål illustrerar att det inte går att avgöra om och när de berör regelrätta informationssäkerhetsfrågor, dvs. informationens konfidentialitet, riktighet, tillgänglighet och spårbarhet. För det krävs ett mer ingående analysarbete.

Tabell 10. Andel informationsrelaterade klagomål under 2014 till 17 patientnämnder som tillsammans hanterade totalt 28 308 klagomål[72]

Typ av klagomål	**%**	**Typ av klagomål**	**%**
Remiss/vårdbegäran	1,9 %	Information till patient eller närstående	4,2 %
Intyg	1,3 %	Informationsöverföring inom vårdgivare	0,7 %
Medicinskteknisk utrustning	0,7 %	Informationsöverföring mellan vårdgivare	0,4 %
Bruten sekretess/tystnadsplikt	0,7 %	Brister i hantering av remisser m.m.	3,3 %
Patientjournal/loggar	2,3 %	Övrig administrativ hantering	1,1 %
Dataintrång	0,7 %	*Summa andel informations-relaterade klagomål*	*17,3 %*

Två kategorier av klagomål är otvetydiga i relevans för informationssäkerhet i vården, nämligen *sekretess* och *dataintrång*. De motsvarar säkerhetskravet på konfidentialitet. I kontakter med patientnämnderna har det dock framkommit att olika klassifikationskriterier tillämpas. I ett fall saknades det uppgift om dataintrång. Förklaringen var att rutin och praxis, trots nationella riktlinjer, var att registrera sådana klagomål under ”sekretess”. Andra typer av klagomål kan rymma andra eller liknande kvalitets- och säkerhetsbrister. Patientjournal och loggar kan till exempel avse anmärkningar på både riktighet och tillgänglighet. Brister i hantering av remisser kan i princip rymma alla typer av kvalitets- och säkerhetskrav. I likhet med metodstödet för NITHA kan det vara fruktbart med en granskning av ärenden för att utvärdera om patientklagomål kan användas för att bedöma risker och behovet av säkerhetskontroller och åtgärder. I båda

[72] Förfrågan om uppgifter till patientnämnder skickades ut i januari 2015, varför tiden har varit kort för sammanställning och delgivande av uppgifter.

fallen är sökbarheten och systematiken i ärendehanteringen standardiserad, vilket gynnar och motiverar en närmare analys.

4.3 Enkätresultat

Enkäten ”Säker vårddokumentation” omfattar två grupper av respondenter, dels medlemmar i Läkarsekreterarnas och Sjukvårdsadministratörernas Förbund (LSF), dels ett urval av sjuksköterskor från SCB:s yrkesregister. Resultat för varje grupp redovisas parallellt under fyra teman som har väglett enkätens design: *riktighet, konfidentialitet, tillgänglighet* och *bakgrundsprofil*. Syftet med bakgrundsfrågor om respondenternas yrkesprofil är att ge ett sammanhang åt sakfrågorna. De kom sist i enkäten, men inleder resultatredovisningen. Allra först ska dock svarsfrekvenser och bortfall sammanfattas.

I november 2014 hade LSF 1 450 medlemmar. Antal svar på enkäten uppgår till 753, vilket ger en svarsfrekvens på 52 %. Bland svaren finns 20 personer som uppger att de inte är yrkesaktiva. De tackas efter första frågan. Bortfallet växer sedan fråga för fråga. För fråga 2 är bortfallet 45 svar (6,1 %). För den näst sista frågan som alla kan svara på (34) uppgår bortfallet till 96 svar (13,1 %). Den stegvisa ökningen av bortfallet beror på att frågorna var tvingande. Det gick inte att hoppa över frågor.

Orsaker till bortfall i LSF-enkäten är flera. Dels kan det handla om svårigheter att förstå enkäten, om problem med webbläsare och tekniska problem samt att det var tvingande att svara på frågorna vid ett och samma tillfälle, dels kan det bero på attityder och ointresse. En granskning av svarsmönster från november till december 2014 visar inga systematiska variationer i svar. Redovisningen av resultat för LSF-medlemmar utgår därför från att bortfallet är slumpmässigt. En närmare orsaksanalys är inte möjlig. Alla enkätsvar delgavs på webben och deltagandet var anonymt. Inga personliga nycklar eller adresser användes.

Urvalet i SCB:s enkät till sjuksköterskor baserar sig på SCB:s yrkesregister från 2012. Det innebär att urvalet rymmer ett fåtal personer som har under två års erfarenhet. Antal svar från yrkesaktiva är 2 712 (57 %). Svarsfrekvenser är högre bland äldre (> 50 år), 0,5–2 procent. Bortfallet för enskilda frågor i SCB-enkäten varierar mellan 0 och 2,4 %.

Skillnader i enkätdesign gör att det inte går att dra några slutsatser om orsaker till gruppernas bortfallstal. Alla enkätsvar från LSF-medlemmar delgavs på webben. Flertalet (84,5 %) i SCB:s enkät delgavs med den tryckta versionen. I webbenkäten till LSF-medlemmar var ordningen på frågor och svar tvingande. I SCB:s version kunde respondenter delge svar i valfri ordning.

4.3.1 Bakgrundsprofil

Andel respondenter med över 10 års yrkeserfarenhet inom vården är 86,5 % för LSF-medlemmar och 74 % för sjuksköterskor. LSF-medlemmar är också

mindre rörliga. Närmare 62 % har arbetat längre än 10 år på sin nuvarande arbetsplats. Motsvarande siffra är 35 % för sjuksköterskor.

Flertalet LSF-medlemmar arbetar i öppenvården (64 %). Bland sjuksköterskor arbetar flera i slutenvården (43 %) än i öppenvården (36 %).

Närmare 92 % av LSF-medlemmarna har landstinget som arbetsgivare; 5 % har privat arbetsgivare. Motsvarande siffror för sjuksköterskor är 72 % respektive 10 %; 16 % har kommunal arbetsgivare.

En större andel LSF-medlemmar än sjuksköterskor har gått en lärarledd kurs i informationssäkerhet, 32 % respektive 15 %. I båda grupperna har drygt hälften av dem med utbildning gått utbildningen de senaste fem åren.

4.3.2 Riktighet

Andel respondenter som känner till en rutin för kvalitetsgranskning av journalföring (fråga 2) är 38 % för LSF-medlemmar och 45 % för sjuksköterskor. Över hälften svarar ”nej” eller är osäkra.

Andel respondenter som kan uppge om kvalitetsgranskning av journalföring har genomförts på arbetsplatsen de senaste 12 månaderna (fråga 3 och 4) är 17 % för båda grupperna. Övriga (83 %) uppger (1) att granskning inte är gjord, (2) att de inte vet om så är fallet eller (3) att de inte kan komma ihåg när den senaste granskningen gjordes.

Andel respondenter som har fått återkoppling på en kvalitetsgranskning de senaste 12 månaderna (fråga 3, 5 och 6) är 12 % för båda grupperna.

Andel respondenter som uppger att felaktig vårddokumentation har förekommit på arbetsplatsen de senaste 12 månaderna uppgår till 43 % för LSF-medlemmar och 48 % för sjuksköterskor (fråga 17 och 18).

Andel respondenter som uppger att felaktig vårddokumentation har varit en patientsäkerhetsrisk de senaste 12 månaderna (fråga 17, 19 och 20) är 13 % för LSF-medlemmar, 22 % för sjuksköterskor. En förklaring till gruppskillnaden (9 %) kan vara att riskerna är högre i löpande informationsdelning på arbetsplatsen och patientnära kontakter.

4.3.3 Konfidentialitet

Andel respondenter som känner till en rutin för logguppföljning (fråga 7) är 70 % för LSF-medlemmar och 40 % för sjuksköterskor.

Andel respondenter som kan uppge om en logguppföljning har genomförts på arbetsplatsen de senaste 12 månaderna (fråga 8 och 9) är 39 % för LSF-medlemmar och 13 % för sjuksköterskor.

Andel respondenter som har fått återkoppling på en logguppföljning de senaste 12 månaderna (fråga 8, 10 och 11) är 20 % för LSF-medlemmar och 4 % för sjuksköterskor.

Det föreligger tydligare gruppskillnader i fråga om kännedom och erfarenhet av logguppföljning. En förklaring kan vara LSF-medlemmarnas tydligare ansvar för vårddokumentation.

Andel respondenter som uppger att obehörig åtkomst till vårddokumentation har förekommit de senaste 12 månaderna (fråga 21 och 22) är 3 % för båda grupperna.

Andel respondenter som uppger att obehörig åtkomst till vårddokumentation har varit en patientsäkerhetsrisk de senaste 12 månaderna (fråga 21, 23 och 24) är 0,2 % för LSF-medlemmar och 0,1 % för sjuksköterskor.

4.3.4 Tillgänglighet

Andel enkätrespondenter som känner till en reservrutin för journalföring (fråga 12) är 64 % för LSF-medlemmar och 54 % för sjuksköterskor.

Andel respondenter som uppger att de har följt en reservrutin för journalföring på arbetsplatsen de senaste 12 månaderna (fråga 13 och 14) är 14 % för LSF-medlemmar och 19 % för sjuksköterskor.

Andel respondenter som har följt och övat en reservrutin för journalföring de senaste 12 månaderna (fråga 13, 15 och 16) är 3 % för båda grupperna.

Andel respondenter som uppger att vårddokumentation har varit otillgänglig de senaste 12 månaderna (fråga 25 och 26) är 31 % för LSF-medlemmar, 40 % för sjuksköterskor.

Andel respondenter som uppger att otillgänglig vårddokumentation har varit en patientsäkerhetsrisk de senaste 12 månaderna (fråga 25, 27 och 28) är 6 % för LSF-medlemmar och 16 % för sjuksköterskor.

Sjuksköterskor bedömer tillgänglighetsrisker högre än LSF-medlemmar. Det är i linje med gruppskillnader i riskuppfattningar om oriktig information. I likhet med det kan förklaringen vara en reell skillnad i risk för grupperna.

4.3.5 Analys

I det här avsnittet sammanfattas analyser av hur bakgrundsprofil (fråga 30–35) samspelar med kännedom och erfarenhet av kontrollarbete och incidenter på arbetsplatsen. Analysunderlaget är en genomgång av korstabeller, dvs. tabeller som anger svarsfrekvenser för svarskombinationer på två eller flera frågor. Här redovisas bara signifikanta samband, dvs. samband som faller utanför SCB:s felmarginaler, eller som bedöms som påtagliga för gruppen LSF-medlemmar, där felmarginaler saknas.

Ledningsansvar och *lärarledd kurs i informationssäkerhet* visar generellt på starkare samband med kännedom och erfarenhet av kontrollarbete, risker och incidenter än övriga bakgrundsfrågor. Det går dock inte att avgöra vilken av dessa faktorer som är viktigare eftersom de också samspelar med varandra. Andelen respondenter som har gått en lärarledd kurs i informationssäkerhet är högre för personer med ledningsansvar än utan ansvar (tabell 11), 41 % högre

för LSF-medlemmar; 59 % högre för sjuksköterskor. De starkaste sambanden mellan ledningsansvar och informationssäkerhet sammanfattas i punktform nedan.

Tabell 11. Korstabell av svarsfrekvenser för fråga 32 och 34: *ledningsansvar* respektive *lärarledd kurs i informationssäkerhet*

		LSF-medlemmar		Sjuksköterskor	
	Ledningsansvar	Ja	Nej	Ja	Nej
	Ja	58 %	30 %	27 % (±4)	73 % (±4)
Lärarledd kurs	Nej	41 %	60 %	17 % (±2)	83 % (±2)
	Vet inte	1 %	10 %	14 % (±5)	86 % (±5)

Samband mellan bakgrundsprofil och informationssäkerhet

- Andel LSF-medlemmar som uppger förekomst av kvalitetsgranskning är 2,2 gånger större bland medlemmar med ledningsansvar än bland medlemmar utan ansvar. Motsvarande tal för sjuksköterskor är 1,6.
- Andel LSF-medlemmar som uppger förekomst av felaktig dokumentation är 1,2 gånger större bland medlemmar med ledningsansvar än utan. Motsvarande tal för sjuksköterskor är 1,1.
- Andel LSF-medlemmar som uppger förekomst av logguppföljning är 1,5 gånger större bland medlemmar med ledningsansvar än utan. Motsvarande tal för sjuksköterskor är 1,4.
- Andel LSF-medlemmar som uppger förekomst av logguppföljning är 1,3 gånger större bland medlemmar med en genomgången kurs i informationssäkerhet än bland de utan en kurs. Motsvarande tal för sjuksköterskor är 1,6.
- Andel LSF-medlemmar som uppger förekomst av obehörig åtkomst är 1,7 gånger större bland medlemmar med ledningsansvar än utan. Motsvarande tal för sjuksköterskor är 1,6.
- Andel LSF-medlemmar som uppger erfarenhet av aktiverade reservrutiner är 1,7 gånger större bland medlemmar med ledningsansvar än utan. Motsvarande tal för sjuksköterskor är 1,3.
- Andel LSF-medlemmar som uppger förekomst av otillgänglig dokumentation är 1,3 gånger större bland medlemmar med ledningsansvar än utan. Motsvarande tal för sjuksköterskor är 1,1.

Det genomgående mönstret är att kännedom och erfarenhet av kontrollarbete och incidenter samspelar med ledningsansvar och kompetens. I några fall väger ledningsansvar tyngre än utbildning. I andra fall går det jämt ut. I ytterligare några fall väger utbildning tyngre än ledningsansvar. Ytterligare ett mönster är att de relativa talen ovan tenderar att vara större för LSF-medlemmar än för sjuksköterskor. Vidare är kännedom om kontrollarbete generellt högre bland LSF-medlemmar. Möjliga förklaringar är att kontrollarbetet följer av ett mer fokuserat ansvar för vårddokumentation, alternativt personligt engagemang på området eller både och.

Övriga bakgrundsfaktorer uppvisar inte lika generella samband med sakfrågor om informationssäkerhet, även om det finns enskilda fall. Bland sjuksköterskor är till exempel andelen med erfarenhet av kvalitetsgranskning 1,4 gånger högre för dem med kommunal arbetsgivare än med landstinget som arbetsgivare.

5. Diskussion

Kartläggningen av vårdgivarnas uppföljning av informationssäkerhetsarbete har omfattat informationskällor, dokumentation och undersökningar av flera och varierande slag. Helhetsintrycket är att kvalitets- och säkerhetsarbetet är lågt prioriterat. Även om det finns undantag är det överlag svårt att urskilja ett sammanhållet kvalitets- och säkerhetsarbete av vårdinformation, system och dokumentation. Arbetet är motiverat av efterlevnad av lagkrav snarare än egen nytto- och riskbaserad kravställning. Det innebär en brist på egna strategiska prioriteringar samt oregelbunden och osystematisk uppföljning.

> *Det återstår mycket anpassning av system, regler och rutiner samt utbildning av personal för att klara patientdatalagens krav.*[73]

Symptomatiskt är att riskuppfattningar och kontrollinsatser inte går hand i hand. De verkar snarast frikopplade från varandra. Riskerna uppfattas till exempel vara störst för informationens riktighet, därefter dess tillgänglighet och sist dess konfidentialitet. Kännedomen om och erfarenheten av kontrollarbete är dock större i fråga om informationens konfidentialitet och tillgänglighet än för dess riktighet. Det speglar att kvalitets- och säkerhetsarbetet i första hand är regelstyrt, istället för riskbaserat. Det finns tydligare regler och rutiner för logguppföljning är för kvalitetsgranskning. Regelstyrt kontrollarbete bekräftas också av låg kännedom om och erfarenhet av kontrollarbete bland vårdpersonal, något som gör kontrollarbetet i sig verkningslöst. Det är genom återkoppling till personalen som kontrollarbetet kan få effekt på säkerhet och kvalitet. Det gäller i hög grad vårdgivarnas logguppföljning. Den görs idag enligt rutiner som i statistisk mening inte kan sägas vara effektiva, och som ingen utvärderar eller ifrågasätter. En typisk rutin kan sammanfattas som följer:

> *En gång per månad görs ett slumpmässigt urval om 10 % av behörig vårdpersonal. Åtkomst till journaler kontrolleras för en slumpmässig dag denna månad.*

Om de mest enkla reglerna tillämpas för att räkna på sannolikheter innebär denna rutin följande:

> *Sannolikheten att undgå upptäckt för en anställd som gör dataintrång varje dag under ett helt arbetsår är 0.28 (0.9^{12}).*[74]

> *Sannolikheten att undgå upptäckt för en anställd som gör ett enda dataintrång under ett helt år är 0.995 (0,9+0.1*20,43/21,43).*[75]

---

[73] eHälsa i landstingen. Rapport 2014. SLIT (Landstingens IT-strateger/IT-chefer): http://www.inera.se/Documents/OM_OSS/Styrdokument_o_rapporter/SLITrapport_2014.pdf

[74] Beräkningen är enkel multiplikation: 0,9 x 0,9 x … x 0,9 (tolv gånger).

I statistisk mening kan det inte råda några tvivel om att loggrutinen inte är speciellt effektiv. Det är bara en bråkdel av journalföringen som kommer med i urvalet. Därtill är den ineffektiv i andra hänseenden. Framför allt säger rutinen ovan inget om andra personalgrupper än vårdpersonal, till exempel it-personal. Dels har gruppen it-personal fysisk åtkomst och administrativa behörigheter till system, dels har den hög it-kompetens. En rimlig hypotes är därför att risken för dataintrång är som högst för denna grupp. Ändå lämnas it-personal och andra grupper utanför logguppföljning. I praktiken kan logguppföljning bara fylla en avskräckande funktion hos vårdpersonalen. Utan kännedom och erfarenhet av logguppföljning försvinner dock även den effekten.

Ingen vårdgivare har delgett någon utvärdering av dagens logguppföljning. Det är ett uttryck för vårdgivarnas generellt svaga styrning och uppföljning av informationssäkerhetsarbetet. Ett dominerande perspektiv är att området handlar om systemsäkerhet, dvs. insatser för att skydda informationssystem mot driftstörningar och obehörig åtkomst. Det bottnar i ett tekniskt säkerhetsperspektiv, att säkerhetsarbetet är detsamma som god it-säkerhet kompletterat med administrativa riktlinjer och rutiner. Med tanke på ett ständigt växande system- och nätverksberoende är perspektivet inte förvånande. Ändå är det snävt och utgör i sig en risk. Andra risker än tekniska förbises. Kontroller likställs med tekniska kontroller. När dessa är på plats behövs varken styrning eller uppföljning.

Informationsstyrning bör utgå från en generell riskhantering av information, riskbaserad kravställning på och uppföljning av verksamhetskritisk information. Det är dock svårt att urskilja några sådana initiativ i underlaget till denna kartläggning, precis som det är svårt att urskilja en sammanhållen kvalitetsledning av informationshantering, system och dokumentation. Det är anmärkningsvärt att dagens patientsäkerhetsarbete lägger så stor tonvikt på journalgranskning, att identifiera vårdskador genom att analysera journaler, men så liten tonvikt på kvalitetsarbetet i informationshantering.

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,[76] till exempel att genomföra regelbundna och systematiska riskanalyser, dvs. att utveckla och tillämpa kvalitets- och säkerhetskrav på verksamhetskritisk information, att

[75] Ett dataintrång kan undgå upptäckt på två sätt. Dels kan den anställda undgå urvalet (0,9), dels kan arbetsdagen ifråga undgå urvalet (20,43/21,43) om den anställda ingår (0,1), dvs. 0,1*20,43/21,43.
[76] Baker, W. H., & Wallace, L. (2007). Is information security under control?: Investigating quality in information security management. Security & Privacy, IEEE, 5(1), 36-44.

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.

I praktiken är det sällsynt med rapportering av kontroller, risker och incidenter med utgångspunkt i kvalitets- och säkerhetskrav på informationshantering. Som regel likställs konfidentialitet och riktighet med att genomföra regelstyrt kontrollarbete, dvs. logguppföljning och kvalitetsgranskning av felfrekvenser i journalhandlingar. Det är sällsynt att se skyddskraven användas i vårdgivarens uppföljning och rapportering, med några undantag, till exempel Landstinget i Jönköpings län och Skellefteå kommun. Det speglar en brist på samsyn på kravställning på informationssäkerhetsområdet.

Bristen på samsyn yttrar sig inte bara i verksamhetsrapportering, utan även i vårdgivarnas avvikelsehantering. Andel avvikelser och incidenter av relevans varierar mycket beroende på vårdgivare, system och verksamhet (vård kontra it). När informationssäkerhetsfrågor avgränsas till verksamhetens rapportering av systemsäkerhetsfrågor – frågor om åtkomst och drift – hamnar andelen på någon procent av alla avvikelser. När de vidgas till skyddskrav på information i verksamhetsprocesser kan de uppgå till 20 %. Då avses rapportering av explicita risker och incidenter på området. Därutöver finns det potentiellt avvikelser av relevans, men som formellt inte klassas som en informationssäkerhetsfråga. I den bästa av världar är rapportering och klassificering av risker, avvikelser och klagomål uttömmande, varför områdes- eller verksamhetsansvariga bara har att konsultera en viss typ av avvikelser. Mer troligt är dock att avvikelseanalyser och utvärdering måste bygga på ofullständig och oklar rapportering, varför ett visst mått av handpåläggning alltid krävs för att utvärdera risker och incidenter.

Problemet med styrning och samordning av informationssäkerhetsfrågor är inte ett exklusivt problem för vården. Riksrevisionen har påtalat liknande problem för statliga myndigheter. Myndigheternas rekommendationer på området är också motstridiga. Rådgivningen är i hög grad teknisk, samtidigt som kritiken ofta handlar om bristande ledning. Andras problem får dock inte dölja att vården har stora utmaningar på området, troligtvis större än andras. Verksamhetens natur kräver öppenhet i kommunikation. Det är ett krav som lätt hamnar i konflikt med kvalitets- och säkerhetskrav på information. Det är just av det skälet, potentiella konflikter i krav, som det behövs bättre ledning, styrning och samordning. 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.

Bilaga 1 Enkätfrågor och svar (LSF)

1. Arbetar du inom hälso- och sjukvården?

Svarsalternativ	Andel svar	Antal svar
Ja	97,3 %	733
Nej –> *Enkäten avslutas.*	2,7 %	20
Summa	100 %	753

Med "kvalitetsgranskning" avser vi en systematisk kontroll av vissa uppgifter i ett urval av patientjournaler, dvs. en genomgång och sammanställning av vilka uppgifter som är rätt och riktiga.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

2. Känner du till någon rutin för kvalitetsgranskning av journalföring?

Svarsalternativ	Andel svar	Antal svar
Ja	38,5 %	265
Nej	35,3 %	243
Osäker	26,2 %	180
Summa	100 %	688

3. Har det någon gång genomförts en kvalitetsgranskning av journalföring?

Svarsalternativ	Andel svar	Antal svar
Ja	33,7 %	232
Nej –> Gå till fråga 7	20,5 %	141
Vet ej –> Gå till fråga 7	45,8 %	315
Summa	100 %	688

4. När senast genomfördes en kvalitetsgranskning av journalföring?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	15,1 %	34
Mellan 1 och 3 månader	17,8 %	40
Mellan 4 och 6 månader	10,2 %	23
Mellan 7 och 12 månader	7,1 %	16
Över 12 månader sedan	12,0 %	27
Kommer inte ihåg	37,8 %	85
Summa	100 %	225

5. Har du någon gång tagit del av resultat från en kvalitetsgranskning av journalföring, i form av en muntlig eller skriftlig redovisning?

Svarsalternativ	Andel svar	Antal svar
Ja	53,3 %	120
Nej –> Gå till fråga 7	41,3 %	93
Vet ej –> Gå till fråga 7	5,3 %	12
Summa	100 %	225

6. När fick du senast ta del av resultat från en kvalitetsgranskning av journalföring?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	21,0 %	25
Mellan 1 och 3 månader	16,8 %	20
Mellan 4 och 6 månader	17,6 %	21
Mellan 7 och 12 månader	10,1 %	12
Över 12 månader sedan	22,7 %	27
Kommer inte ihåg	11,8 %	14
Summa	100 %	119

Med "logguppföljning" avser vi en regelbunden och systematisk kontroll av vem som har haft åtkomst till patientjournaler, att endast behöriga personer har haft åtkomst.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

7. Känner du till någon rutin för logguppföljning?

Svarsalternativ	Andel svar	Antal svar
Ja	70,3 %	469
Nej	18,3 %	122
Osäker	11,4 %	76
Summa	100 %	667

8. Har det någon gång genomförts en logguppföljning?

Svarsalternativ	Andel svar	Antal svar
Ja	67,0 %	447
Nej –> *Gå till fråga 12*	6,0 %	40
Vet ej –> *Gå till fråga 12*	27,0 %	180
Summa	100 %	667

9. När senast genomfördes en logguppföljning?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	27,6 %	123
Mellan 1 och 3 månader	22,7 %	101
Mellan 4 och 6 månader	3,8 %	17
Mellan 7 och 12 månader	3,8 %	17
Över 12 månader sedan	4,7 %	21
Kommer inte ihåg	37,3 %	166
Summa	100 %	445

10. Har du någon gång tagit del av resultat från en logguppföljning, i form av en muntlig eller skriftlig redovisning?

Svarsalternativ	Andel svar	Antal svar
Ja	47,0 %	209
Nej –> *Gå till fråga 12*	50,6 %	225
Vet ej –> *Gå till fråga 12*	2,5 %	11
Summa	100 %	445

11. När fick du senast ta del av resultat från en loggguppföljning?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	21,5 %	45
Mellan 1 och 3 månader	25,8 %	54
Mellan 4 och 6 månader	7,7 %	16
Mellan 7 och 12 månader	8,1 %	17
Över 12 månader sedan	23,0 %	48
Kommer inte ihåg	13,9 %	29
Summa	100 %	209

Med "reservrutiner" avses rutiner för att läsa eller skriva journaler när normala rutiner inte fungerar. Det kan bero på nödsituationer, tekniska problem eller andra oönskade händelser.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

12. Känner du till någon reservrutin för journalhantering?

Svarsalternativ	Andel svar	Antal svar
Ja	63,9 %	420
Nej	22,5 %	148
Osäker	13,5 %	89
Summa	100 %	657

13. Har du någon gång följt en reservrutin för journalhantering?

Svarsalternativ	Andel svar	Antal svar
Ja	35,3 %	232
Nej –> *Gå till fråga 17*	57,4 %	377
Vet ej –> *Gå till fråga 17*	7,3 %	48
Summa	100 %	657

14. När senast följde du en reservrutin för journalhantering?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	7,8 %	18
Mellan 1 och 3 månader	11,3 %	26
Mellan 4 och 6 månader	10,4 %	24
Mellan 7 och 12 månader	11,3 %	26
Över 12 månader sedan	44,2 %	102
Kommer inte ihåg	15,2 %	35
Summa	100 %	231

15. Har du någon gång övat en reservrutin för journalhantering?

Svarsalternativ	Andel svar	Antal svar
Ja	24,2 %	56
Nej –> *Gå till fråga 17*	73,6 %	170
Vet ej –> *Gå till fråga 17*	2,2 %	5
Summa	100 %	231

16. När fick du senast öva en reservrutin för journalhantering?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	7,1 %	4
Mellan 1 och 3 månader	12,5 %	7
Mellan 4 och 6 månader	3,6 %	2
Mellan 7 och 12 månader	7,1 %	4
Över 12 månader sedan	41,1 %	23
Kommer inte ihåg	28,6 %	16
Summa	100 %	56

Med "vårddokumentation" avser vi till exempel journalanteckningar, läkemedelslistor, provsvar och remisser.

Med ”patientsäkerhetsrisk” avser vi en möjlig orsak till potentiell patientskada, där orsak och skada fastställs genom professionell bedömning på arbetsplatsen.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

17. Har det hänt att vårddokumentation har varit felaktig?

Svarsalternativ	Andel svar	Antal svar
Ja	74,8 %	487
Nej –> *Gå till fråga 21*	6,8 %	44
Vet ej –> *Gå till fråga 21*	18,4 %	120
Summa	100 %	651

18. När fick du senast kännedom om felaktig vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	22,7 %	110
Mellan 1 och 3 månader	19,0 %	92
Mellan 4 och 6 månader	10,7 %	52
Mellan 7 och 12 månader	5,4 %	26
Över 12 månader sedan	9,5 %	46
Kommer inte ihåg	32,8 %	159
Summa	100 %	485

19. Har felaktig vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	Andel svar	Antal svar
Ja	25,4 %	123
Nej –> *Gå till fråga 21*	26,4 %	128
Vet ej –> *Gå till fråga 21*	48,2 %	234
Summa	100 %	485

20. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. felaktig vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	28,7 %	35
Mellan 1 och 3 månader	23,8 %	29
Mellan 4 och 6 månader	13,1 %	16
Mellan 7 och 12 månader	4,9 %	6
Över 12 månader sedan	9,0 %	11
Kommer inte ihåg	20,5 %	25
Summa	100 %	122

21. Har det hänt att obehöriga personer har tagit del av vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Ja	11,7 %	75
Nej –> *Gå till fråga 25*	29,1 %	187
Vet ej –> *Gå till fråga 25*	59,3 %	381
Summa	100 %	643

22. När fick du senast kännedom om obehörig åtkomst till vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	0,0 %	0
Mellan 1 och 3 månader	13,3 %	10
Mellan 4 och 6 månader	9,3 %	7
Mellan 7 och 12 månader	5,3 %	4
Över 12 månader sedan	42,7 %	32
Kommer inte ihåg	29,3 %	22
Summa	100 %	75

23. Har obehörig åtkomst till vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	Andel svar	Antal svar
Ja	8,0 %	6
Nej –> *Gå till fråga 25*	26,7 %	20
Vet ej –> *Gå till fråga 25*	65,3 %	49
Summa	100 %	75

24. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. obehörig åtkomst till vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	0,0 %	0
Mellan 1 och 3 månader	16,7 %	1
Mellan 4 och 6 månader	0,0 %	0
Mellan 7 och 12 månader	0,0 %	0
Över 12 månader sedan	33,3 %	2
Kommer inte ihåg	50,0 %	3
Summa	100 %	6

25. Har det hänt att vårddokumentation har varit otillgänglig? Med "otillgänglig" avses alla tänkbara situationer där vårddokumentation efterfrågas, men inte finns att tillgå – oavsett orsak.

Svarsalternativ	Andel svar	Antal svar
Ja	56,1 %	359
Nej –> *Gå till fråga 29*	18,9 %	121
Vet ej –> *Gå till fråga 29*	25,0 %	160
Summa	100 %	640

26. När fick du senast kännedom om otillgänglig vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	22,0 %	79
Mellan 1 och 3 månader	16,2 %	58
Mellan 4 och 6 månader	12,0 %	43
Mellan 7 och 12 månader	5,8 %	21
Över 12 månader sedan	12,5 %	45
Kommer inte ihåg	31,5 %	113
Summa	100 %	359

27. Har otillgänglig vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	Andel svar	Antal svar
Ja	16,4 %	59
Nej –> *Gå till fråga 29*	22,8 %	82
Vet ej –> *Gå till fråga 29*	60,7 %	218
Summa	100 %	359

28. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. otillgänglig vårddokumentation?

Svarsalternativ	Andel svar	Antal svar
Mindre än 4 veckor sedan	30,0 %	18
Mellan 1 och 3 månader	20,0 %	12
Mellan 4 och 6 månader	11,7 %	7
Mellan 7 och 12 månader	6,7 %	4
Över 12 månader sedan	13,3 %	8
Kommer inte ihåg	18,3 %	11
Summa	100 %	60

29. Hur lång erfarenhet har du av att arbeta inom svensk hälso- och sjukvård?

Svarsalternativ	Andel svar	Antal svar
Mindre än 2 år	2,5 %	16
Mellan 2 och 4 år	3,3 %	21
Mellan 5 och 10 år	7,7 %	49
Mer än 10 år	86,5 %	553
Summa	100 %	639

30. Hur länge har du arbetat på din nuvarande och huvudsakliga arbetsplats?

Svarsalternativ	Andel svar	Antal svar
Mindre än 2 år	11,0 %	70
Mellan 2 och 4 år	10,5 %	67
Mellan 5 och 10 år	16,9 %	108
Mer än 10 år	61,7 %	394
Summa	100 %	639

31. Vilken typ av arbetsplats jobbar du på?

Svarsalternativ	Andel svar	Antal svar
Öppen vård	63,6 %	405
Sluten vård	29,4 %	187
Vård och omsorg med boende	0,2 %	1
Annan vård och omsorg	6,9 %	44
Summa	100 %	637

32. Har du någon form av ledningsansvar på din arbetsplats?

Svarsalternativ	Andel svar	Antal svar
Ja	13,0 %	83
Nej	87,0 %	554
Summa	100 %	637

33. Vilken typ av arbetsgivare har du?

Svarsalternativ	Andel svar	Antal svar
Kommunal	2,0 %	13
Landsting eller region	91,8 %	585
Statlig	0,6 %	4
Privat	5,3 %	34
Annan arbetsgivare	0,2 %	1
Summa	100 %	637

34. Har du gått någon lärarledd kurs i informationssäkerhet?

Svarsalternativ	Andel svar	Antal svar
Ja	33,9 %	216
Nej –> *Enkäten avslutas.*	57,6 %	367
Vet ej –> *Enkäten avslutas.*	8,5 %	54
Summa	100 %	637

35. Hur lång tid har gått sedan du sist gick en lärarledd kurs i informationssäkerhet?

Svarsalternativ	Andel svar	Antal svar
Högst 12 månader	12,5 %	27
1 till 2 år	18,1 %	39
3 till 5 år	24,1 %	52
Över 5 år	22,7 %	49
Kommer inte ihåg	22,7 %	49
Summa	100 %	216

Bilaga 2 Enkätfrågor och svar (SCB)

1. Arbetar du inom hälso- och sjukvården?

Svarsalternativ	%, viktad andel	Antal svar
Ja	92 (±1)	2 679
Nej –> *Enkäten avslutas.*	8 (±1)	220
Summa	100	2 899

Med "kvalitetsgranskning" avser vi en systematisk kontroll av vissa uppgifter i ett urval av patientjournaler, dvs. en genomgång och sammanställning av vilka uppgifter som är rätt och riktiga.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

2. Känner du till någon rutin för kvalitetsgranskning av journalföring?

Svarsalternativ	%, viktad andel	Antal svar
Ja	45 (±2)	1 212
Nej	31 (±2)	811
Osäker	24 (±2)	642
Summa	100	2 665

3. Har det någon gång genomförts en kvalitetsgranskning av journalföring?

Svarsalternativ	%, viktad andel	Antal svar
Ja	37 (±2)	987
Nej –> Gå till fråga 7	18 (±1)	458
Vet ej –> Gå till fråga 7	46 (±2)	1 219
Summa	100	2 664

4. När senast genomfördes en kvalitetsgranskning av journalföring?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	10 (±2)	110
Mellan 1 och 3 månader	17 (±2)	179
Mellan 4 och 6 månader	8 (±2)	84
Mellan 7 och 12 månader	11 (±2)	114
Över 12 månader sedan	17 (±2)	179
Kommer inte ihåg	37 (±3)	315
Summa	100	981

5. Har du någon gång tagit del av resultat från en kvalitetsgranskning av journalföring, i form av en muntlig eller skriftlig redovisning?

Svarsalternativ	%, viktad andel	Antal svar
Ja	64 (±3)	684
Nej –> Gå till fråga 7	29 (±3)	235
Vet ej –> Gå till fråga 7	7 (±2)	58
Summa	100	977

6. När fick du senast ta del av resultat från en kvalitetsgranskning av journalföring?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	12 (±2)	93
Mellan 1 och 3 månader	15 (±3)	113
Mellan 4 och 6 månader	11 (±2)	78
Mellan 7 och 12 månader	12 (±2)	94
Över 12 månader sedan	24 (±3)	177
Kommer inte ihåg	27 (±3)	132
Summa	100	687

Med "logguppföljning" avser vi en regelbunden och systematisk kontroll av vem som har haft åtkomst till patientjournaler, att endast behöriga personer har haft åtkomst.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

7. Känner du till någon rutin för logguppföljning?

Svarsalternativ	%, viktad andel	Antal svar
Ja	40 (±2)	1 074
Nej	40 (±2)	1 084
Osäker	20 (±2)	532
Summa	100	2 690

8. Har det någon gång genomförts en logguppföljning?

Svarsalternativ	%, viktad andel	Antal svar
Ja	33 (±2)	892
Nej –> *Gå till fråga 12*	15 (±1)	380
Vet ej –> *Gå till fråga 12*	53 (±2)	1 410
Summa	100	2 682

9. När senast genomfördes en logguppföljning?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	13 (±2)	125
Mellan 1 och 3 månader	16 (±2)	151
Mellan 4 och 6 månader	6 (±1)	58
Mellan 7 och 12 månader	5 (±1)	51
Över 12 månader sedan	9 (±2)	81
Kommer inte ihåg	52 (±3)	419
Summa	100	885

10. Har du någon gång tagit del av resultat från en logguppföljning, i form av en muntlig eller skriftlig redovisning?

Svarsalternativ	%, viktad andel	Antal svar
Ja	34 (±3)	346
Nej –> *Gå till fråga 12*	59 (±3)	507
Vet ej –> *Gå till fråga 12*	7 (±2)	42
Summa	100	895

11. När fick du senast ta del av resultat från en loggguppföljning?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	10 (±3)	45
Mellan 1 och 3 månader	13 (±3)	57
Mellan 4 och 6 månader	9 (±3)	42
Mellan 7 och 12 månader	8 (±2)	35
Över 12 månader sedan	25 (±4)	102
Kommer inte ihåg	36 (±4)	62
Summa	100	343

Med "reservrutiner" avses rutiner för att läsa eller skriva journaler när normala rutiner inte fungerar. Det kan bero på nödsituationer, tekniska problem eller andra oönskade händelser.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

12. Känner du till någon reservrutin för journalhantering?

Svarsalternativ	%, viktad andel	Antal svar
Ja	54 (±2)	1 459
Nej	34 (±2)	922
Osäker	12 (±1)	314
Summa	100	2 695

13. Har du någon gång följt en reservrutin för journalhantering?

Svarsalternativ	%, viktad andel	Antal svar
Ja	41 (±2)	1 085
Nej –> *Gå till fråga 17*	52 (±2)	1 402
Vet ej –> *Gå till fråga 17*	7 (±1)	192
Summa	100	2 679

14. När senast följde du en reservrutin för journalhantering?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	10 (±2)	121
Mellan 1 och 3 månader	12 (±2)	135
Mellan 4 och 6 månader	11 (±2)	129
Mellan 7 och 12 månader	12 (±2)	144
Över 12 månader sedan	37 (±3)	427
Kommer inte ihåg	17 (±2)	129
Summa	100	1 085

15. Har du någon gång övat en reservrutin för journalhantering?

Svarsalternativ	%, viktad andel	Antal svar
Ja	23 (±2)	267
Nej –> *Gå till fråga 17*	73 (±3)	778
Vet ej –> *Gå till fråga 17*	4 (±1)	41
Summa	100	1 086

16. När fick du senast öva en reservrutin för journalhantering?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	11 (±3)	40
Mellan 1 och 3 månader	7 (±3)	28
Mellan 4 och 6 månader	6 (±3)	21
Mellan 7 och 12 månader	5 (±2)	20
Över 12 månader sedan	29 (±5)	102
Kommer inte ihåg	41 (±5)	59
Summa	100	270

Med "vårddokumentation" avser vi till exempel journalanteckningar, läkemedelslistor, provsvar och remisser.

Med "patientsäkerhetsrisk" avser vi en möjlig orsak till potentiell patientskada, där orsak och skada fastställs genom professionell bedömning på arbetsplatsen.

Frågorna avser din kännedom och erfarenhet från din nuvarande och huvudsakliga arbetsplats.

17. Har det hänt att vårddokumentation har varit felaktig?

Svarsalternativ	%, viktad andel	Antal svar
Ja	75 (±2)	2 000
Nej –> *Gå till fråga 21*	9 (±1)	252
Vet ej –> *Gå till fråga 21*	16 (±1)	428
Summa	100	2 680

18. När fick du senast kännedom om felaktig vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	29 (±2)	580
Mellan 1 och 3 månader	18 (±2)	370
Mellan 4 och 6 månader	8 (±1)	169
Mellan 7 och 12 månader	8 (±1)	167
Över 12 månader sedan	11 (±1)	222
Kommer inte ihåg	25 (±2)	495
Summa	100	2 003

19. Har felaktig vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	%, viktad andel	Antal svar
Ja	48 (±2)	954
Nej –> *Gå till fråga 21*	31 (±2)	624
Vet ej –> *Gå till fråga 21*	21 (±2)	416
Summa	100	1 994

20. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. felaktig vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	26 (±3)	283
Mellan 1 och 3 månader	18 (±2)	190
Mellan 4 och 6 månader	9 (±2)	89
Mellan 7 och 12 månader	7 (±2)	72
Över 12 månader sedan	12 (±2)	110
Kommer inte ihåg	28 (±3)	212
Summa	100	956

21. Har det hänt att obehöriga personer har tagit del av vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Ja	9 (±2)	227
Nej –> *Gå till fråga 25*	45 (±2)	1 201
Vet ej –> *Gå till fråga 25*	46 (±2)	1 231
Summa	100	2 659

22. När fick du senast kännedom om obehörig åtkomst till vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	14 (±4)	44
Mellan 1 och 3 månader	7 (±3)	22
Mellan 4 och 6 månader	7 (±3)	21
Mellan 7 och 12 månader	6 (±3)	19
Över 12 månader sedan	26 (±5)	76
Kommer inte ihåg	40 (±5)	46
Summa	100	228

23. Har obehörig åtkomst till vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	%, viktad andel	Antal svar
Ja	8 (±2)	29
Nej –> *Gå till fråga 25*	45 (±5)	121
Vet ej –> *Gå till fråga 25*	47 (±5)	96
Summa	100	246

24. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. obehörig åtkomst till vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	7 (±5)	7
Mellan 1 och 3 månader	4 (±3)	3
Mellan 4 och 6 månader	6 (±4)	7
Mellan 7 och 12 månader	3 (±3)	2
Över 12 månader sedan	12 (±6)	6
Kommer inte ihåg	69 (±8)	5
Summa	100	30

25. Har det hänt att vårddokumentation har varit otillgänglig? Med "otillgänglig" avses alla tänkbara situationer där vårddokumentation efterfrågas, men inte finns att tillgå – oavsett orsak.

Svarsalternativ	%, viktad andel	Antal svar
Ja	60 (±2)	1 618
Nej –> *Gå till fråga 29*	25 (±2)	663
Vet ej –> *Gå till fråga 29*	15 (±1)	395
Summa	100	2 676

26. När fick du senast kännedom om otillgänglig vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	31 (±2)	511
Mellan 1 och 3 månader	19 (±2)	308
Mellan 4 och 6 månader	11 (±2)	189
Mellan 7 och 12 månader	6 (±1)	99
Över 12 månader sedan	11 (±2)	174
Kommer inte ihåg	22 (±2)	332
Summa	100	1 613

27. Har otillgänglig vårddokumentation någon gång varit en risk för patientsäkerheten?

Svarsalternativ	%, viktad andel	Antal svar
Ja	44 (±2)	708
Nej –> *Gå till fråga 29*	27 (±2)	435
Vet ej –> *Gå till fråga 29*	30 (±2)	465
Summa	100	1 608

28. När fick du senast kännedom om en patientsäkerhetsrisk p.g.a. otillgänglig vårddokumentation?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 4 veckor sedan	27 (±3)	224
Mellan 1 och 3 månader	18 (±3)	142
Mellan 4 och 6 månader	11 (±2)	88
Mellan 7 och 12 månader	6 (±2)	43
Över 12 månader sedan	9 (±2)	66
Kommer inte ihåg	30 (±3)	146
Summa	100	709

29. Hur lång erfarenhet har du av att arbeta inom svensk hälso- och sjukvård?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 2 år	0 (±0)	9
Mellan 2 och 4 år	7 (±1)	175
Mellan 5 och 10 år	18 (±1)	439
Mer än 10 år	74 (±1)	2 083
Summa	100	2 706

30. Hur länge har du arbetat på din nuvarande och huvudsakliga arbetsplats?

Svarsalternativ	%, viktad andel	Antal svar
Mindre än 2 år	20 (±2)	523
Mellan 2 och 4 år	20 (±2)	506
Mellan 5 och 10 år	25 (±2)	674
Mer än 10 år	35 (±2)	1 005
Summa	100	2 708

31. Vilken typ av arbetsplats jobbar du på?

Svarsalternativ	%, viktad andel	Antal svar
Öppen vård	36 (±2)	979
Sluten vård	43 (±2)	1 128
Vård och omsorg med boende	9 (±1)	242
Annan vård och omsorg	11 (±1)	299
Summa	100	2 648

32. Har du någon form av ledningsansvar på din arbetsplats?

Svarsalternativ	%, viktad andel	Antal svar
Ja	18 (±1)	483
Nej	82 (±1)	2 221
Summa	100	2 704

33. Vilken typ av arbetsgivare har du?

Svarsalternativ	%, viktad andel	Antal svar
Kommunal	16 (±1)	448
Landsting eller region	72 (±2)	1 947
Statlig	1 (±0)	16
Privat	10 (±1)	265
Annan arbetsgivare	1 (±0)	15
Summa	100	2 691

34. Har du gått någon lärarledd kurs i informationssäkerhet?

Svarsalternativ	%, viktad andel	Antal svar
Ja	15 (±1)	402
Nej –> *Enkäten avslutas.*	79 (±2)	2 128
Vet ej –> *Enkäten avslutas.*	7 (±1)	171
Summa	100	2 701

35. Hur lång tid har gått sedan du sist gick en lärarledd kurs i informationssäkerhet?

Svarsalternativ	%, viktad andel	Antal svar
Högst 12 månader	15 (±3)	78
1 till 2 år	15 (±3)	82
3 till 5 år	14 (±3)	73
Över 5 år	22 (±3)	106
Kommer inte ihåg	34 (±4)	60
Summa	100	399

Bilaga 3 Forskningspublikationer om vårdrelaterad informationssäkerhet

Brandt, Patrik, Östlund, Louise & Wennberg, Louise (2004). Informatisk forskning om riskanalysprocess applicerad på Apoteket AB:s kundcenterverksamhet.

Brandt, Patrik, Révay, Peter & Wennberg, Louise (2004). System thinking on Risk Analysis. SABI 2004: Business Systems - Environmental Contexts.

Eriksson, Henrik & Hansson, Jonas (2006). Integration of Management Systems. Theoretical and practical implications. The Asian Journal on Quality. 7:2, s. 69–82.

Eriksson, Nomie (2008). Implementation of an Electronic Patient's Record in Process Oriented Healthcare. The 3rd Nordic Workshop on Health Management and Organization. Between Public and Private, 4-5 december Uppsala. Sub-theme 3: Making professional work transparent.

Götherström, Christine, Hamrin, Elisabeth & Gullberg, Mats (1995). Development of a tool for measuring the concept of good care among patients and staff in relation to Swedish legislation. International Journal of Nursing Studies. 32:3, s. 277–287.

Harnesk, Dan, Lindström, John, Keller, Christina, Wiberg, Mikael, Ågerfalk, Pär J. & Eriksson Lundström, Jenny (2012). Materializing organizational information security. Nordic Contributions in IS Research: Third Scandinavian Conference on Information Systems, SCIS 2012, Sigtuna, Sweden, August 17–20, 2012. Proceedings. 124.

Hammar, Tora, Ekedahl, Anders & Petersson, Göran (2014). Implementation of a shared medication list: physicians' views on availability, accuracy and confidentiality. *International Journal of Clinical Pharmacy*. 36:5, s. 933–942

Hedström, Karin, Karlsson, Fredrik & Kolkowska, Ella (2013). Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale. Information Management & Computer Security. 21:4, s. 266–287.

Hedström, Karin, Kolkowska, Ella, Karlsson, Fredrik & Allen, J. P. (2011). Value conflicts for information security management. Journal of strategic information systems. 20:4, s. 373–384.

Hoffmann, Robert, Kowalski, Stewart, Jain, Rohan & Mumtaz, Majid (2011). E_Universities Services in the New Social Eco-systems: Security Risk Analysis: Using Conversational Agents to Help Teach Information Security Risk Analysis.

Kolkowska, Ella, Hedström, Karin & Karlsson, Fredrik (2009). Information security goals in a Swedish hospital. Security, assurance and privacy: organizational challenges. Article no. 16.

Lindström, John & Hägerfors, Ann (2009). A model for explaining strategic IT- and information security to senior management. International Journal of Public Information Systems. 5:1.

Lindström, John (2009). Models, methodology and challenges within strategic information security for senior managements. Luleå tekniska universitet.

Perjons, Erik A, Wangler, Benkt, Wäyrynen, Jaana & Åhlfeldt, Rose-Mharie (2005). Introducing a process manager in healthcare: An experience report. Health Informatics Journal. 11:1, s. 45–61.

Pourasghar, Faramarz (2009). Role of information technology on documentation and security of medical data. Stockholm: Karolinska Institutet, Department of Learning, Informatics, Management and Ethics (Lime).

Söderström, Eva, Åhlfeldt, Rose-Mharie & Eriksson, Nomie (2011). Trusting Digitized Patient-Related Information: The Need for a New Approach. Proceedings of the 5th International Symposium on Human Aspects of Information Security and Assurance (HAISA 2011). s. 119–129.

Söderström, Eva, Åhlfeldt, Rose-Mharie & Eriksson, Nomie (2009). Standards for information security and processes in healthcare. Journal of Systems and Information Technology. 11:3, s. 295–308.

Söderström, Eva, Åhlfeldt, Rose-Mharie & Eriksson, Nomie (2008). Standardisation as a Means to Improve Information Security in Process-Oriented Distributed Healthcare. Proceedings (ed.) Kai Jacobs and Eva Söderström. Presented at the 13th European Academy for Standardization (EURAS), 2008-06-16–17, Skövde Sweden. 2008:ABI Band 40, s. 233–243.

Wennberg, Louise, Brandt, Patrik & Révay, Peter (2006). Information security - an application of a systems approach. Kybernetes. 35:6, s. 786–796.

Weyns, Kim (2011). IT Dependability Management in Governmental Organisations. Department of Computer Science, Lund, Sweden.

Åhlfeldt, Rose-Mharie (2009). Informationssäkerhetsbrister i en distribuerad hälso- och sjukvård påverkar patientens säkerhet och integritet. Svensk Medicinsk Rätt. 17:1, s. 19–21.

Åhlfeldt, Rose-Mharie (2008). Information Security in Distributed Healthcare: Exploring the Needs for Achieving Patient Safety and Patient Privacy. Stockholm University.

Åhlfeldt, Rose-Mharie (2006). Information Security in a Distributed Healthcare Domain: Exploring the Problems and Needs of Different Healthcare Providers. Skövde/Stockholm: School of Humanities and Informatics, University of Skövde/Department of Computer and Systems Science, Stockholm University.

Åhlfeldt, Rose-Mharie (2006). Information Security in a Heterogeneous Healthcare Domain. Interoperability of Enterprise Software and Applications: INTEROP-ESA'2005. s. 103–114.

Åhlfeldt, Rose-Mharie (2006). Information Security Issues in Healthcare: an Experience Report. Skövde University Studies in Informatics: Knowledge in Organisations I.:1, s. 147–158.

Åhlfeldt, Rose-Mharie (2002). Information Security in Home Healthcare. Conference Proceedings of AiCE2002, Sydney, September 30th, 2002: Third Australian Institute of Computer Ethics Conference: Computer Ethics: Its impact upon Australia. s. 6–15.

Åhlfeldt, Rose-Mharie & Ask, Lena (2004). Information Security in Electronic Medical Records: A case study with the user in focus. 2004 Information Resources Management Association International Conference. s. 345–347.

Åhlfeldt, Rose-Mharie, Backlund, Per, Wangler, Benkt & Söderström, Eva (2005). Security Issues in Health Care Process Integration: Research-in-Progress Report. 2nd INTEROP-EMOI Open Workshop on Enterprise Models and Ontologies for Interoperability: INTEROP-EMOI 05. s. 363–366.

Åhlfeldt, Rose-Mharie & Huvala, Isto (2014). Patient Safety and Patient Privacy when Patient Reading their Medical Records. Safe and Secure Cities: 5th International Conference on Well-Being in the Information Society, WIS 2014, Turku, Finland, August 18-20, 2014. Proceedings. s. 230–239.

Åhlfeldt, Rose-Mharie, Spagnoletti, Paolo & Sindre, Guttorm (2007). Improving the Information Security Model by using TFI. New Approaches for Security, Privacy and Trust in Complex Environments: Proceedings of the 22nd IFIP TC-11 International Information Security Conference (SEC 2007). s. 73–84.

Åhlfeldt, Rose-Mharie & Söderström, Eva (2010). Patient Safety and Patient Privacy in Information Security from the Patient's view: A case study. Journal of Information System Security. 6:4, s. 71–85.

Åhlfeldt, Rose-Mharie & Söderström, Eva (2008). Information Security Problems and Needs in Healthcare: A Case Study of Norway and Finland vs Sweden. Enterprise Interoperability III: Proceedings of the International Conference on Interoperability of Enterprise Software and Applications (INTEROP-ESA '2008). s. 41–53.

Åhlfeldt, Rose-Mharie & Söderström, Eva (2007). Information Security Problems and Needs in a Distributed Healthcare Domain: A Case study. The Twelfth International Symposium on Health Information Management Research (iSHIMR 2007). s. 97–108.

Bilaga 4 Avhandlingar av svenska forskare om informationssäkerhet (LIBRIS)

Abbas, Haider (2010). Options-based security-oriented framework for addressing uncertainty issues in IT security. Diss. Stockholm: Kungliga Tekniska högskolan.

Almgren, Magnus (2008). Techniques for improving intrusion detection. Diss. Göteborg: Chalmers tekniska högskola.

Almgren, Magnus (2005). Intrusion detection and protection of application servers. Lic.-avh. Göteborg: Chalmers tekniska högskola.

Andersson, Christer (2007). Design and evaluation of anonymity solutions for mobile networks. Diss. Karlstad: Karlstads universitet.

Andersson, Christer (2005). Enhancing privacy for mobile networks: examples of anonymity solutions and their analysis. Licentiatavhandling Karlstad: Karlstads universitet.

Angulo, Julio (2012). Usable privacy for digital transactions: exploring the usability aspects of three privacy enhancing mechanisms. Licentiatavhandling Karlstad: Karlstads universitet.

Askarov, Aslan (2009). Policies and mechanisms for securing information release. Diss. Göteborg: Chalmers tekniska högskola.

Axelsson, Stefan (2005). Understanding intrusion detection through visualisation. Diss. Göteborg: Chalmers tekniska högskola.

Bakari, Jabiri Kuwe (2007). A holistic approach for managing ICT security in non-commercial organisations: a case study in a developing country. Diss. Stockholm: Stockholms universitet.

Bakari, Jabiri Kuwe (2005). Towards a holistic approach for managing ICT security in developing countries: a case study of Tanzania. Lic.-avh. Stockholm: Stockholms universitet.

Berthold, Stefan (2014). Inter-temporal privacy metrics. Diss. Karlstad: Karlstads universitet.

Berthold, Stefan (2011). Towards inter-temporal privacy metrics. Licentiatavhandling Karlstad: Karlstads universitet.

Björck, Fredrik (2005). Discovering information security management. Diss. Stockholm: Stockholms universitet.

Boldt, Martin (2010). Privacy-invasive software. Diss. Karlskrona: Blekinge tekniska högskola.

Boldt, Martin (2007). Privacy-invasive software: exploring effects and countermeasures. Licentiatavhandling Ronneby: Blekinge tekniska högskola.

Brandt, Patrik & Wennberg, Louise (2004). Informatisk forskning om riskanalysprocess applicerad på Apoteket AB:s kundcenterverksamhet. Lic.-avh. Ronneby: Blekinge Tekniska Högskola.

Brüer, Jan-Olof (1983). Information security in a computerized office. Linköping: Dep. of electrical engineering [Inst. för systemteknik], Univ.

Burbeck, Kalle (2006). Adaptive real-time anomaly detection for safeguarding critical networks. Licentiatavhandling Linköping: Linköpings universitet.

Buschle, Markus (2014). Tool support for enterprise architecture analysis: with application in cyber security. Diss. Stockholm: Kungliga Tekniska högskolan.

Carrara, Elisabetta (2005). Security for IP multimedia applications over heterogeneous networks. Licentiatavhandling Stockholm: Kungliga Tekniska högskolan.

Casmir, Respickius (2005). A dynamic and adaptive information security awareness (DAISA) approach. Diss. Stockholm: Stockholms universitet.

Chaula, Job Asheri (2006). A socio-technical analysis of information systems security assurance: a case study for effective assurance. Diss. Stockholm: Stockholms universitet.

Chen, Yinru (2003). Protection profile analysis and security target for an intrusion detection system. Lic.-avh. Luleå: Luleå tekniska univ.

Dayarathna, Rasika (2013). Discovering constructs and dimensions for information privacy metrics. Diss. Stockholm: Stockholms universitet.

Dayarathna, Rasika (2007). Towards comparing personal information privacy protection measures. Lic.-avh. Stockholm: Stockholms universitet.

Duma, Claudiu (2005). Security and trust mechanisms for groups in distributed services. Diss. Linköping: Linköpings universitet.

Erlandsson, Fredrik (2014). On social interaction metrics: social network crawling based on interestingness. Lic. Karlskrona: Blekinge Tekniska Högskola.

Finne, Thomas (1998). A decision support system for improving information security. Diss. Turku: Turku Centre for Computer Science.

Fåk, Viiveke (1978). Data security by application of cryptographic methods. Linköping: Dep. of electrical engineering [Inst. för systemteknik, Linköpings univ.].

Hagström, Åsa (2006). Understanding certificate revocation. Licentiatavhandling Linköping: Linköpings universitet.

Hansson, Hans A. (1991). Time and probability in formal design of distributed systems. Elsevier Science Inc. New York, NY, USA.

Hedin, Daniel (2007). Language based covert channel avoidance. Licentiatavhandling Göteborg: Chalmers tekniska högskola.

Henke, Ferdinand (1986). Die Datenschutzkonvention des Europarates. Diss. Trier: Univ.

Herzog, Almut (2007). Usable security policies in runtime environments. Diss. Linköping: Linköpings universitet.

Holm, Hannes (2014). A framework and calculation engine for modeling and predicting the cyber security of enterprise architectures. Diss. Stockholm: Kungliga Tekniska högskolan.

Iqbal, Sarfraz (2014). Designing the online educational information security laboratories. Licentiatavhandling Luleå: Luleå tekniska universitet.

Jacobsson, Andreas (2008). Privacy and security in Internet-based information systems. Diss. Karlskrona: Blekinge tekniska högskola.

Jacobsson, Andreas (2004). Exploring privacy risks in information networks. Lic.-avh. Ronneby: Blekinge tekniska högskola.

Johansson, Erik (2005). Assessment of enterprise information security: how to make it credible and efficient. Diss. Stockholm: Kungliga Tekniska högskolan.

Johnson, Henric (2005). Toward adjustable lightweight authentication for network access control. Diss. Karlskrona: Blekinge tekniska högskola.

Jonsson, Erland (1995). A quantitative approach to computer security from a dependability perspective. Diss. (sammanfattning) Göteborg: Chalmers tekniska högskola.

Kajtazi, Miranda (2013). Assessing escalation of commitment as an antecedent of noncompliance with information security policy. Diss. Växjö: Linnéuniversitetet.

Kapidžić Cicović, Nada (1997). Extended certificate management system: design and protocols. Diss. Stockholm: Kungliga Tekniska högskolan.

Karresand, Martin (2008). Completing the picture: fragments and back again. Licentiatavhandling Linköping: Linköpings universitet.

Kasun De Zoysa, T. Nandika (2003). A model of security architecture for multi-party transactions. Diss. Stockholm: Univ.

Konrad, Peter (1998). Geschäftsprozess-orientierte Simulation der Informationssicherheit: Entwicklung und empirische Evaluierung eines Systems zur Unterstützung des Sicherheitsmanagements. Zugl.: Köln, Univ. Diss.

Kowalski, Stewart (1994). IT insecurity: a multi-disciplinary inquiry. Diss. Stockholm: Kungliga Tekniska högskolan.

Kvarnström, Håkan (2004). On the implementation and protection of fraud detection systems. Diss. Göteborg: Chalmers tekniska högskola.

Larson, Ulf E. (2009). On adapting data collection to intrusion detection. Diss. (sammanfattning) Göteborg: Chalmers tekniska högskola.

Larson, Ulf E. (2006). Aspects of adapting data collection to intrusion detection. Licentiatavhandling Göteborg: Chalmers tekniska högskola.

Lindqvist, Ulf (1999). On the fundamentals of analysis and detection of computer misuse. Göteborg: Chalmers tekniska högskola.

Lindskog, Stefan (2005). Modeling and tuning security from a quality of service perspective. Diss. Göteborg: Chalmers tekniska högskola.

Lindström, John (2009). Models, methodology and challenges within strategic information security for senior managements. Diss. Luleå: Luleå tekniska universitet.

Lorentzen, Charlott (2014). On user perception of authentication in networks. Diss. Karlskrona: Blekinge Tekniska Högskola.

Lorentzen, Charlott (2011). User perception and performance of authentication procedures. Licentiatavhandling Karlskrona: Blekinge tekniska högskola.

Lundin Barse, Emilie (2004). Logging for intrusion and fraud detection. Diss. Göteborg: Chalmers tekniska högskola.

Lundin, Reine (2012). Guesswork and entropy as security measures for selective encryption. Diss. Karlstad: Karlstads universitet.

Lundin, Reine (2007). Towards measurable and tunable security. Licentiatavhandling Karlstad: Karlstads universitet.

Magnusson, Christer (1999). Hedging shareholder value in an IT dependent business society: the framework BRITS. Diss. Stockholm: Univ.

Magnusson Sjöberg, Cecilia (1992). Rättsautomation: särskilt om statsförvaltningens datorisering. 1. uppl. Diss. Stockholm: Univ.

Martucci, Leonardo A. (2009). Identity and anonymity in ad hoc networks. Diss. Karlstad: Karlstads universitet.

Martucci, Leonardo A. (2006). The identity-anonymity paradox: on the relationship between identification, anonymity and security in mobile ad hoc networks. Licentiatavhandling Karlstad: Karlstads universitet.

Mellstrand, Per (2007). Informed system protection. Diss. Karlskrona: Blekinge tekniska högskola.

Mwakalinga, Jeffy (2011). A framework for adaptive information security systems: a holistic investigation. Diss. Stockholm: Kungliga Tekniska högskolan.

Nilsson, Dennis K. (2009). How to secure the connected car. Diss. Göteborg: Chalmers tekniska högskola.

Nilsson, Dennis K. (2008). Security aspects of wireless vehicle-to-infrastructure environments. Licentiatavhandling Göteborg: Chalmers tekniska högskola.

Nissen, Jörgen (1993). Pojkarna vid datorn: unga entusiaster i datateknikens värld. Diss. Linköping: Univ.

Nohlberg, Marcus (2008). Securing information assets: understanding, measuring and protecting against social engineering attacks. Diss. Stockholm: Stockholms universitet.

Näckros, Kjell (2005). Visualising security through computer games: investigating game-based instruction in ICT security: an experimental approach. Diss. Stockholm: Stockholms universitet.

Näckros, Kjell (2001). Game-based instruction within IT security education. Lic.-avh. Stockholm: Univ.

Oscarson, Per (2007). Actual and perceived information systems security. Diss. Linköping: Linköpings universitet.

Oscarson, Per (2001). Informationssäkerhet i verksamheter: begrepp och modeller som stöd för förståelse av informationssäkerhet och dess hantering i verksamheter. Lic.-avh. Linköping: Univ.

Pourasghar, Faramarz (2009). The role of information technology on documentation and security of medical data. Diss. Stockholm: Karolinska institutet.

Pulls, Tobias (2012). Privacy-preserving transparency-enhancing tools. Licentiatavhandling Karlstad: Karlstads universitet.

Raza, Shahid (2013). Lightweight security solutions for the internet of things. Diss. Mälardalens högskola.

Rodhe, Ioana (2008). Query authentication and data confidentiality in wireless sensor networks. Licentiatavhandling Uppsala: Uppsala universitet.

Seipel, Peter (1977). Computing law: perspectives on a new legal discipline. Diss. Stockholm: Univ.

Shahzad, Raja Muhammad Khurram (2013). Classification of potentially unwanted programs using supervised learning. Lic. Karlskrona: Blekinge tekniska högskola.

Siponen, Mikko T. (2002). Designing secure information systems and software: critical evaluation of the existing approaches and a new paradigm. Diss. Oulu: Univ.

Sommestad, Teodor (2012). A framework and theory for cyber security assessments. Diss. Stockholm: Kungliga Tekniska högskolan.

Tarimo, Charles N. (2006). ICT security readiness checklist for developing countries: a social-technical approach. Diss. Stockholm: Stockholms universitet.

Tarimo, Charles N. (2003). Towards a generic framework for implementation and use of intrusion detection systems. Lic.-avh. Stockholm: Univ.

Trolin, Mårten (2005). Two topics in cryptography: lattice problems and the security of protocols. Lic.-avh. Stockholm: Kungliga Tekniska högskolan.

Vapen, Anna (2011). Contributions to web authentication for untrusted computers. Licentiatavhandling Linköping: Linköpings universitet.

Verendel, Vilhelm (2010). Some problems in quantified security. Licentiatavhandling Göteborg: Chalmers tekniska högskola.

Vuković, Ognjen (2014). Cyber-security in smart grid communication and control. Diss. Stockholm: Kungliga Tekniska högskolan.

Weyns, Kim (2011). IT dependability management in governmental organisations. Diss. Lund: Lunds universitet.

Weyns, Kim (2008). Dependability of IT systems in emergency situations: theory and practice. Licentiatavhandling Lund: Lunds universitet.

Wilander, John (2013). Contributions to Specification, implementation and execution of secure software. Diss. Linköping: Linköpings universitet.

Wilander, John (2005). Policy and implementation assurance for software security. Licentiatavhandling Linköping: Linköpings universitet.

Yngström, Louise (1996). A systemic-holistic approach to academic programmes in IT security. Diss. Stockholm: Univ.

Zhang, Ge (2012). Unwanted traffic and information disclosure in VoIP networks: threats and countermeasures. Diss. Karlstad: Karlstads universitet.

Zhang, Ge (2009). Towards secure SIP signalling service for VoIP applications: performance-related attacks and preventions. Licentiatavhandling Karlstad: Karlstads universitet.

Zuccato, Albin (2005). Holistic information security management framework: for electronic commerce. Diss. Karlstad: Karlstads universitet.

Zuccato, Albin (2002). Towards a systemic-holistic security management. Lic.avh. Karlstad: Univ.

Åhlfeldt, Rose-Mharie (2006). Information security in a distributed healthcare domain: exploring the problems and needs of different health care providers. Licentiatavhandling Stockholm: Stockholms universitet.

Åhlfeldt, Rose-Mharie (2008). Information security in distributed healthcare: exploring the needs for achieving patient safety and patient privacy. Diss. Stockholm: Stockholms universitet.

Bilaga 5 Årsrapport – Jämtlands läns landsting

Informationssäkerhetsberättelse 2013
Anna-Lena Alfreds
Jämtlands läns landsting
2014-02-12

1 Informationssäkerhetsarbete 2013

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.

Under en period 2011–2012 fanns ingen utsedd ansvarig för informationssäkerhet i landstinget och arbetet har därmed blivit eftersatt. Vid internkontroll av landstingets säkerhetsarbete i februari 2013 gjorde landstingsstyrelsen observation att det fanns stora brister i landstingets informationssäkerhetsarbete. Landstingsdirektören gavs i uppdrag att stärka informationssäkerhetsarbetet (landstingsstyrelsens protokoll 20130219). Fr.o.m. 2013 har beredskapschefen tillika varit informationssäkerhetssamordnare. Landstingets informationssäkerhetsgrupp har påbörjat arbete för att bygga upp ett ledningssystem för informationssäkerhet och driva landstingets arbete avseende informationssäkerhet framåt. Avdelade resurser har inte motsvarat behovet och relativt mycket arbete återstår. Det börjar finnas en grund och struktur för arbetet, men fördelning av och gränsdragning för IT- och informationssäkerhetsfrågor behöver ses över.

1.1 Policy

Landstingsfullmäktige fastställde i juni en ny informationssäkerhetspolicy. Beslut är också taget att begreppet informationsägare skall användas i landstinget och att det följer verksamhetsansvaret.

1.2 Ledningssystem för informationssäkerhet (LIS)

Beslut är taget att informationssäkerhet skall vara en integrerad del av landstingets ledningssystem och att informationssäkerhetsarbetet så långt det är möjligt skall följa standarden i ISO 27001.

Arbete har påbörjats med framtagande av styrande dokument för att uppfylla kraven för informationssäkerhet enligt ISO 27001:2006. Arbetet som ingår i projektet Insidan och ledningssystemet är omfattande och har inte hunnit slutföras under 2013. Under våren 2014 ska en s.k. GAP-analys genomföras för att tydliggöra vad som återstår. Analysen finns med som en aktivitet i den handlingsplan för informationssäkerhet som arbetats fram.

1.3 Informationssäkerhetsgruppens arbete

Ett relativt omfattande arbete har genomförts för att klargöra ISO-standardens krav, inventera befintliga styrande dokument samt behov av ytterligare regler och rutiner som behöver utarbetas. Sammanfattningsvis har följande dokument och arbete gjorts under 2013:

- Ansvar, roller och organisation avseende informationssäkerhet har utarbetats och fastställts av landstingsdirektören.
- En handlingsplan för informationssäkerhetsarbetet 2014–2015 har arbetats fram.
- En workshop har anordnats för att utarbeta regler för webbanvändning, där medarbetare från IT, personalstaben och kommunikationsstaben deltagit. Reglerna beräknas slutföras under 2014.
- Arbete är påbörjat för framtagande av modell för riskbedömning och riskhantering inom området.
- Regler för loggguppföljning är under framtagande med avsikt att gälla generellt för landstingets olika IT system.
- En riskanalys avseende systemförvaltningsmodellens tillämpning ur ett informationssäkerhetsperspektiv har genomförts under året.
- Försök har gjorts med att starta upp arbetet med BITS-analyser (basnivå för informationssäkerhet). Vårdsystemet OBSTETRIX och passersystemet M5 har fått stöd för att genomföra sina BITS-analyser. En mer omfattande planering och resursfördelning måste göras för de kommande åren för att arbeta systematiskt och sätta fart på BITS-arbetet.
- Regler för SMS-påminnelser har utarbetats.
- Landstingsövergripande regler och rutiner för id-kontroll och id-märkning har arbetats fram och kommer att gå ut på en bred remiss i början av 2014.
- En översyn av datalagrets tillämpning och användning pågår i syfte att arbeta fram regler för hantering av personuppgifter.

1.4 Handlingsplan informationssäkerhet 2014–2015

Syftet med handlingsplanen är att med ledningens stöd på ett strukturerat sätt öka kännedom om informationssäkerhet i landstingets verksamheter så att styrande lagar och beslutad policy efterlevs och förverkligas. Förutom att arbeta fram regler och rutiner är en viktig åtgärd att genomföra grundläggande utbildning för alla medarbetare samt riktad utbildning till nyckelfunktioner. Vidare behövs arbete med BITS-analyser göras för att uppnå den beslutade basnivån för informationssäkerhet i landstingets olika IT-system. Arbete med kontinuitetsplanering behöver stärkas så att verksamheten kan fungera när störningar och avbrott i viktiga IT-system uppstår.

1.5 Tillsyn Datainspektionen

1.5.1 Spärrhantering

I början av 2013 skickades en komplettering in avseende en tillsyn som Datainspektionen påbörjade 2011 angående patienters rätt till spärr enligt patientdatalagen (LS/936/2011). Inspektionen avsåg systemen VAS, Obstetrix, Meddix, 1177 Rådgivningsstöd, Raindance, Megacare, Kundrad.

Landstinget levde inte upp till kraven enligt patientdatalagen. Datainspektionens beslut meddelades 2013-05-01 och där föreläggs Landstinget att omgående vidta åtgärder för att leva upp till kraven i patientdatalagen i system som fortfarande inte går att spärra, och lämpligen i samband med detta upprätta en tidsplan. Några av bristerna har åtgärdats, för andra är tidsplanen förskjuten bl.a. p.g.a. byte från VAS till COSMIC.

1.5.2 Behörighetshantering

Datainspektionen genomförde 2013 en tillsyn avseende behovs- och riskanalys samt riktlinjer för obehörig åtkomst i huvudjournalsystemet. Frågorna gällde huruvida Landstinget har en dokumenterad behovs- och riskanalys för behörighetstilldelning samt om det finns skriftliga riktlinjer som definierar obehörig åtkomst som stöd för utförande av loggkontroller. Svar skickades in 2013-10-17. Inget beslut har ännu tilldelats. Informationssäkerhetsgruppens bedömning är att Landstinget behöver göra en övergripande behovs- och riskanalys för behörighetstilldelning samt skapa riktlinjer för behörigheter/obehörig åtkomst i COSMIC.

1.6 Riskanalys systemförvaltning

En riskanalys avseende systemförvaltningsmodellen och dess tillämpning har genomförts i syfte att identifiera risker och brister ur ett informationssäkerhetsperspektiv. En enkät skickades ut till systemansvariga för 19 av landstingets verksamhetskritiska system. Risker har identifierats, orsaker har analyserats och åtgärder har föreslagits för att komma till rätta med identifierade brister. Riskanalysen kan här läsas i sin helhet: [raderad länk till dokument på landstingets intranät].

1.7 SITHS-kortsrevision

Internrevision visar att chefers kännedom om hur SITHS-kort hanteras och administreras är god med hjälp av assistenter och sekreterare. Däremot noterades bristande kunskap om kortens betydelse som värdehandling hos användare t.ex. förekommer att SITHS kort lämnas kvar i datorer på behandlingsrum och expeditioner även när patienter fanns kvar ensamma i rummet.

1.8 Incidenter och avvikelser

Under 2013 har 65 avvikelser rapporterats där informationssäkerhet angivits i orsakssammanhang. Det handlar oftast om information som ej finns tillgänglig (42 st.) exempelvis p.g.a. driftstopp eller störningar i IT system eller att gällande rutiner ej följts för rapportering, remisshantering, journalanteckningar. 10 avvikelser berör sekretess där t.ex. kallelser och fakturor har skickats till fel patient, personuppgifter har e-postats, fax med patientuppgifter skickats fel.

Det går inte att dra några större slutsatser av materialet då det finns klara brister gällande kvalitetssäkring. Av användarnas rapportering kan man dock konstatera att vården har ett högt IT-beroende och att även korta avbrott, driftstörningar ger stor påverkan i arbetet. Ett arbete behöver göras för att på ett systematiskt och strukturerat sätt kunna arbeta med avvikelser i förebyggande och kvalitetssäkrande syfte.

2 Planerade och prioriterade åtgärder 2014

Inför 2014 omfördelas resurser inom samordningskansliet för att stärka fortsatt arbete med informationssäkerhet. Arbetet kommer att följa handlingsplanen för informationssäkerhet samt aktivitetsplanen för arbetet med att bygga upp ledningssystemet avseende informationssäkerhet. En s.k. GAP-analys för detta planeras genomföras under våren.

Det är viktigt att beslut och ställning tas till föreslagna åtgärder och risker/brister som framkommit avseende systemförvaltningsmodellen och dess tillämpning. Ett annat prioriterat område är att arbetet med BITS-analyser återupptas och kommer igång. Ansvaret finns idag hos systemägarna men bedömningen är att det finns behov av vägledning och metodstöd för att komma framåt, vilket betyder att resurser måste avsättas i samordningskansliet för detta.

Planering för 2014 års interna kontroll/riskanalys är att se över området logguppföljning på en landstingsövergripande nivå. En GAP-analys planeras också för processen för behörighetshantering.

Utbildning av nyckelfunktioner såsom chefer (via ledningsgrupper) och vårdutvecklare (kvalitetsgranskare i avvikelsesystemet) ska prioriteras 2014.

Kravställning vid upphandling och införande av molntjänster behöver utarbetas. En modell för informations- och systemklassning behöver arbetas fram. Viktigt är också att arbetet med klassificering och riktlinjer för informationssäkerhetsavvikelser genomförs.

Det är också av stor vikt att informationssäkerhetsaspekter beaktas vid införandet av nya vårdadministrativa systemet COSMIC.

Bilaga 6 Årsrapport – Landstinget i Uppsala län

Rapport informationssäkerhet 2013
Fredrik Rosenberg
Landstinget i Uppsala län

2014-03-19

Viktiga åtgärder inom Informations- och it-säkerhetsområdet under 2013

Beredskap
MSI införde på beställning av LLK en beredskapslinje för grundläggande infrastruktur. Den innefattar inte användarsupport men det har varit en handfull ärenden som kan hänföras till beredskap kväll, helg eller natt.

Utbildning
Ett sammanfattande dokument har skapats som tar upp det viktigaste gällande informations- och it-säkerhet med fokus på användare. Det är tänkt som stöd vid introduktioner och arbetsplatsträffar. Den interaktiva säkerhetsutbildningen har också kompletterats med mer material om informationssäkerhet. Säkerhetsutbildningarna för chefer har nu också ett avsnitt om informationssäkerhet.

Ett stort antal föreläsningar har också genomförts i ämnet Patientdatalagen och vad som gäller vid åtkomst till patientuppgifter. Bedömningen är att intresset för dessa har ökat i och med att frågorna blivit aktualiserade i media.

Kontinuitet
Tomas Roland har via säkerhetsenheten fått i uppgift att arbeta med kontinuitetsplanering, då det ligger nära katastrof- och beredskapsområdet. För informationssäkerheten är detta bra och detta arbete ska bland annat utmynna i ett arbetssätt och en mall gällande hur man inom LUL skapar en kontinuitetsplan för sitt system. Första steget är att göra en kontinuitetsplan för Cosmic och öva denna under året. En grundläggande del av en kontinuitetsplan är reservrutiner, men även hur man efter avbrott ska kunna återställa verksamheten. Informationssäkerhetsansvarig deltar i detta arbete.

Redundansalternativ i nät
Olika redundansalternativ har testats gällande redundans av nätverk. Det har visat sig att det är svårt att skapa redundanslösningar till enskilda verksamheter belägna utanför Uppsala tätort. Orsaken är att det ofta bara går en fiber till orten och att det då inte finns möjlighet att nå verksamheten med två skilda fiberkopplingar. En redundans blir då omöjlig eller mycket kostsam om lokalisationen ligger avsides. Därför testas andra typer av redundans, såsom via kopparkablar och via 4G-nätet. Arbete kommer att fortsätta under 2014.

Gemensamma regelverk för it-säkerhet
Under 2013 har ett regelverk kring it-säkerhet tagits fram. Dock ej fastställts. Det syftar till att skapa en gemensam grund och en lägstanivå gällande området it-säkerhet. Orsaken är att

vi inom LUL har flera aktörer som driftar egna system. Exempel på detta är UL, LSU, LRC och FTV. Ur informationssäkerhetsperspektiv är en centraliserad drift önskvärd. I brist på detta är gemensamma regelverk nödvändiga.

Segmentering
Arbetet fortsätter att segmentera nätet och på så sätt särskilja olika typer av utrustning. Detta gäller framför allt medicinteknisk utrustning och utrustning med lägre säkerhetsnivå.

Klassificering av datorer
På beställning av it-direktören har en klassificering gällande olika typer av datorer tagits fram. Den ger en bas för hur datorerna ska skyddas och hur de får kopplas in. För it-säkerheten kan denna åtgärd få stort genomslag. Speciellt för medicinteknisk utrustning.

Sårbarhetsscanning
Sårbarhetsscanning som ett led av kontroll av LUL:s perimeterskydd har skett under hösten 2013. Ett mindre antal dåligt uppdaterade servrar har identifierats i scanningen. Ingen av dessa innehåller patientdata och de bedömdes inte heller utgöra en möjlig väg in i nätet. Glädjande i scanningen var att de servrar (den stora merparten) som hanterats enligt landstingets standard klarat sig mycket bra i scanningen. De mest akuta systemen är åtgärdade och gällande övriga system pågår åtgärd.

Logganalys
Ett nytt loggverktyg har testats i pilotdrift och utvärdering sker under 2014. Det syftar till att förbättra driftsäkerheten gällande utlämnande av loggar samt i nästa steg förbättra den systematiska loggranskningen.

Granskningar av projektet Journalen på nätet
Projektet eJournal och Sustains har granskats ett antal gånger. Både Sustains-lösningen, som syftar till att ge patienter direktåtkomst till sin journal hos Landstinget i Uppsala län, och eJournalen som är den nationella lösningen för att erbjuda samma sak men från fler landsting. Vissa brister har hittats men generellt har lösningarna ansetts som säkra och välgjorda. De brister som framkommit har åtgärdats.

Spärrar och loggar
Att landstinget har en gemensam enhet för att hantera spärrar och loggar har ansetts som en stor fördel av exempelvis Datainspektionen. De flesta landsting är på väg mot detta. Ca 250 patienter har valt att spärra sin journal. Det är färre än exempelvis Karolinska som har ca 1 500 patienter som har spärrat. Tolkningen är att med bra information till patienterna undviks en del spärrar. För tillgängligheten anses spärrarna av verksamheten vara en nackdel. Lagstiftaren har tagit detta i beaktande. Patientdatalagen kommer att revideras och tecken tyder på att det blir en patientsäkrare hantering av spärrarna.

Det s.k. Nora-fallet rönte stort massmedialt intresse, åtminstone initialt, och ett stort antal ur personalen anklagades för att olovligen ha gått in i hennes journal. Utredningen visade att så inte var fallet och åklagaren valde att lägga ner utredningen.

Ett mycket stort antal patienter har tagit del av sin loggrapport via Mina vårdkontakter. Detta har resulterat i ett mycket litet antal anmälningar, där den gemensamma faktorn är att det har funnits en personlig koppling.

Med erfarenhet från Nora-fallet och patienternas granskningar av loggrapporterna kan man på goda grunder anta att s.k. ”tjuvläsning” av journaler inte är utbrett på det sätt som media gärna vill framhålla. Troligen är det mycket sällsynt.

Skydd av medicinsk utrustning
Ett stort problem är den CE-märkta medicinska utrustningen som ofta måste stå i kontakt med Internet. Dessa utrustningar, där en del är en vanlig dator, får inte patchas eller skyddas hur som helst för att CE-märkningen ska gälla. Olika lösningar testas. En i form av en liten brandvägg som kan sättas framför den aktuella utrustningen och på så sätt skydda både den och resten av nätet. En annan lösning som testas är s.k. vitlistningsprogramvara. En vitlistningsprogramvara tillåter bara det som är vitlistat att köras på den aktuella klienten. Kommer annan programvara in kommer den inte att kunna köras, exempelvis skadlig kod. Det har dock varit mycket svårt att verifiera att dessa vitlistningsprogramvaror fungerar som de ska och att inga patientrisker uppkommer.

SSO, förenklad inloggning
Projekt pågår att införa en förenklad inloggning, företrädesvis med kort. Vid en övergång till tvingande kortinloggning höjs säkerhetsnivån avsevärt. Ett stort hinder för detta är dock funktionsinloggningarna, som används både på vårdavdelningar och i exempelvis operationssalar. Det finns dock bara ett mycket litet antal funktionsinloggningar i Cosmic som i sig kommer åt begränsat med information. Både funktionsinloggningar och 1-faktorsautentisering (användarnamn och lösenord) har potential att ge brister i spårbarheten.

Bedömd hotbild mot landstinget gällande intrång

Intrångsförsök
Bedömningen är att hotbilden gällande intrångsförsök i första hand gäller s.k. missnöjesaktioner. Patienter som i sitt tycke blivit felbehandlade eller andra som anser att landstinget i någon fråga agerat oetiskt. I ett sådant scenario kan det tänkas att en aktör vill hämnas på landstinget genom att försöka ta sig in och stjäla känsliga uppgifter för att sedan skapa opinion gentemot landstinget. Dessa händelser får också mycket stort medialt genomslag. Det finns också exempel på när olika grupperingar utfört överbelastningsattacker gentemot företags nätverk i syfte att störa kommunikationen. Återigen handlar det oftast om missnöjesaktioner. Dessa har setts mot exempelvis Polismyndigheten och riksdagen.

Ett annat scenario är att information om patienter stjäls i syfte att sälja information. Detta scenario är hypotetiskt då vi inte känner till att det skett inom något svenskt landsting, men är teoretiskt möjligt.

Bedömningen är att landstinget är förhållandevis väl rustat mot intrångsförsök från Internet.

Några allvarliga händelser i omvärlden 2013

Nedan följer tre händelser som är ganska representativa för vad som kan hända. Driftavbrotten skedde trots att det är mycket stora aktörer inblandade som förväntas ha kontroll över både sin drift och sina backuplösningar. Ddos-attacken är representativ på grund av att den passar i den hotbild som finns och att man numera kan köpa en överbelastningsattack på nätet, som kommersialiserad tjänst.

2013-04-03 Driftavbrott Sjunet

Hela infrastrukturen kring Sjunet drabbades vilket gjorde att Sjunet gick ner helt. Sjunet räknas som ett driftsäkert nät och används för kommunikation mellan aktörer inom hälso- och sjukvården. Landstinget i Uppsala län drabbades ganska lindrigt då de system som drabbades, t.ex. Pascal inte under en begränsad tid var kritiska för verksamheten.

2013-09-16 Ddos-attack mot Skånetrafiken

En överbelastningsattack satte Skånetrafikens system ur spel under ett antal timmar. Bland annat påverkades möjligheten att betala med kort samt företagets hemsida.

2013-12-31 Brand hos en stor it-leverantör

En brand hos en leverantör av it-system får stora konsekvenser för SJ, SL och Posten. Branden skedde i ett serverrum och vid försök till återställning upptäcks en bugg i en programvara som används för att återställa driften. Efter en vecka var Postens hemsida fortfarande inte i full drift.

Avvikelser i Medcontrol

Under 2013 registrerades 9 säkerhetsärenden i MedControl som kan hänföras till området informationssäkerhet:

13LUL-0308-S Förlust av trådlöst nät
13LUL-0286-S Autosvar från mail gått till fel adress
13LUL-0250-S Driftproblem p.g.a. byte till Windows 7
13LUL-0243-S Förlust av nätverk
13LUL-0207-S Driftavbrott operationsplanerare
13LUL-0146-S Driftproblem p.g.a. byte till Windows 7
13LUL-0128-S Driftavbrott Pascal (dosordination)
13LUL-0088-S Personnummer i adressboken
13LUL-0030-S Problem SITHS-kort

Inget av dessa ärenden indikerar något övergripande problemområde inom LUL. Samtliga ärenden är hanterade.

Egenkontroll 2013 – verksamheter

Egenkontroll har funnits som begrepp inom Landstinget i Uppsala län under ett antal år. Under 2013 gjordes en ansats att få ett gemensamt sätt att utföra dessa egenkontroller. Tidigare granskningar har visat att det inom PV, Hoh och LE funnits arbetssätt som går att

applicera på hela landstinget. En grupp bildades som har till uppgift att gemensamt revidera den checklista som ligger till grund för egenkontrollen. Checklistan innehåller både grundläggande processer som exempelvis reservrutiner och utbildning, men också anpassade delar vars innehåll beror på förändringar i omvärlden eller behov av att säkerställa att rutiner är kända. Vid nya riktlinjer eller andra styrande dokument kan innehållet i checklistan ändras för att spegla detta.

Checklistan revideras under maj månad för att sedan skickas ut till verksamheten direkt efter sommaren. Verksamheterna har sedan fram till årsskiftet att genomföra och dokumentera egenkontrollen.

För 2013 har fokus varit att få igång egenkontrollarbetet på Akademiska sjukhuset, vilket bedömdes som viktigast.

Delar av egenkontrollen, erfarenheter och trender, redovisas i respektive förvaltnings årsredovisning. Denna sammanställning fokuserar istället på risker och riskområden som har redovisats i egenkontrollerna. Målet är att få fram risker och riskområden som finns på många eller samtliga delar av landstinget och hantera dessa som gemensamma risker.

Förvaltningarna
Inom PV, HoH och LE finns en längre tradition av att genomföra egenkontroller. Inom dessa förvaltningar görs detta i hög utsträckning. Inom övriga förvaltningar behöver insatser göras. Vissa förvaltningar utför inte egenkontroller medan andra har andra kontrollmekanismer. Målet är att hela landstinget framöver ska göra på samma sätt.

Urval av risker och riskområden som lyfts fram:

- Användningen av e-post som kommunikationssätt gentemot patienten
- Otydligheter i avvikelsehanteringen gällande var avvikelser ska rapporteras
- Behov av information kring patientdatalagen och vem som får göra vad
- Avbrottsrutiner finns inte alltid, med undantag av Cosmic.
- Bildhantering.

Akademiska sjukhuset
Då egenkontroll inte tidigare fungerat som återkommande metod för att kontrollera informationssäkerheten gjordes 2013 ett omtag som bland annat innebar att en något förenklad checklista tagits fram. Denna checklista fokuserar på ett antal strategiskt viktiga områden som utbildning, reservrutiner, behörigheter och risker. Den är baserad på den checklista som används av övriga förvaltningar och kommer framöver vara lika för alla verksamheter.

På Kirurg- och onkologdivisionen fungerar detta som tänkt och svar från samtliga verksamhetsområden har inkommit. På övriga divisioner varierar utfallet från att ca hälften svarat till att ingen gjort det. Insatser för att förbättra detta resultat kommer att göras under 2014.

Risker och riskområden som lyfts fram

- Behovet av tydligare riktlinjer kring vem som får läsa journal och i vilket syfte
- Sekretessrisker p.g.a. lyhörda och trånga lokaler
- Svårigheter att upphöra med faxande av patientuppgifter. Framför allt i akuta skeden. Reservrutiner finns för Cosmic men man har det inte alltid för andra system som är viktiga.

Sammanfattningsvis kan sägas att det ur de risker som framkommit inte tydligt finns något riskområde som sticker ut. I takt med att egenkontrollen mer görs utifrån ett strukturerat arbetssätt är bedömningen att antalet identifierade risker kommer att öka.

Bilaga 1: Egenkontroll checklista HoH
Bilaga 2: Egenkontroll checklista Akademiska sjukhuset 2013

Bilagorna 1 och 2 avser bilagor till landstingets originalrapport. I denna rapport ersätts dessa med en aktuell bilaga som avser 2015 (bilaga 7-8 i denna rapport).

Bemanning och organisation

Rollen som it-säkerhetsansvarig saknas inom LUL. Bedömning av informationssäkerhetsansvarig är att det behövs någon som har den tekniska kompetensen i området på ett djupare plan och som i samråd med informationssäkerhetsansvarig aktivt kan arbeta med befogenheter för att it-säkerheten upprätthålls.

Fokusområden 2014

Områden som behöver särskilt fokus under 2014 är angivna som egen bilaga.

Bilaga 3: Fokusområden Informationssäkerhet 2014 (bilaga 9 i denna rapport).

Bilaga 7 Egenkontroll 2014 – Landstinget i Uppsala län

Egenkontroll 2014 – bilaga 1–2 till Rapport informationssäkerhet 2013
Egenkontrollen, som beskrivs i dokumentet Styrande riktlinjer för informationssäkerhet, ska genomföras årligen för att säkerställa att en lämplig nivå av informationssäkerhet upprätthålls.

Syftet med egenkontrollen är säkerställa att landstinget hanterar information på ett korrekt sätt. En viktig del är att risker ska identifieras så att dessa antingen kan hanteras direkt inom enheten alternativt lyftas upp som landstingsgemensamma risker och därmed hanteras centralt. Därutöver måste landstinget vid olika tillsyner från exempelvis Datainspektionen, revisorer eller Inspektionen för vård och omsorg (IVO) kunna redovisa att dessa egenkontroller verkligen genomförs. Nedanstående underlag och checklista är ett stöd för att genomföra denna.

Respektive förvaltning, förslagsvis via it-chef/it-ansvarig, ansvarar för att

- checklistan för egenkontroll skickas ut till förvaltningens/divisionens verksamhetschefer eller motsvarande
- svaren på dessa samlas in senast 31/12
- resultatet skickas till informationssäkerhetsansvarig för landstinget senast 31/1-2015

Själva checklistan revideras årligen av en arbetsgrupp med representanter från olika delar av landstinget. Resultatet av egenkontrollerna används både till att kontinuerligt förbättra informationssäkerheten inom landstinget och till att förbättra själva checklistan för nästkommande år. Målet är att det ska vara enkelt för verksamheten. Frågor kan besvaras av Fredrik Rosenberg, informationssäkerhetsansvarig LUL.

Underlag och föreslagna aktiviteter
1 Introduktion och utbildning
Nya medarbetare ska genomgå utbildning i de system som är relevanta för uppdraget. I samband med införandet av nya program eller programversioner ska alla medarbetare ges möjlighet till utbildning.

Exempel på områden inom It- och informationssäkerhetsområdet är att känna till reservrutiner, hur man ska hantera datorn, vad man gör om datorn får virus etc.

Via den obligatoriska interaktiva säkerhetsutbildningen som finns i PingPong ges medarbetare en grund i informationssäkerhet. En sammanfattning av de viktigaste punkterna i landstingets regelverk finns i dokumentet ”Informations- och it-säkerhet för anställda”.

Länk: Informations- och it-säkerhet för anställda (raderad länk till landstingets intranät)

Övriga styrande dokument inom informationssäkerhet och it-säkerhet finns i databasen för styrande dokument.

Länk: Styrande dokument (raderad länk till landstingets intranät)

Reservrutiner för den aktuella verksamheten måste också delges nya och befintliga medarbetare.

Föreslagna aktiviteter:

- Tillse att alla nya medarbetare får en introduktionsutbildning som även innefattar informationssäkerhet
- Tillse att alla medarbetare känner till dokumentet ”Informations och it-säkerhet för anställda”
- Inkludera informationssäkerhetsfrågor på arbetsplatsträffar.

2 Användaradministration

Behörighetstilldelningen ska baseras på er behovs- och riskanalys så att inte behörigheter ges slentrianmässigt. Grunden är att behörigheten endast ska omfatta det som behövs för att tilldelade arbetsuppgifter ska kunna utföras. Det är verksamhetschefen som ansvarar för att behörighetstilldelningen är korrekt. Det operativa arbetet med att tilldela behörigheter är dock ofta delegerat till annan.

Behörighetstilldelningen är lika viktig vid nyanställning som när en anställning avslutas. När en anställning upphör ska användarens behörigheter tas bort. Detsamma gäller då medarbetare byter arbetsplats inom landstinget.

Behörighetstilldelningen ska kontrolleras och vid behov revideras med jämna mellanrum så att det säkerställs att medarbetare har rätt behörighet i de olika system som de använder.

HSA-katalogen, Hälso- och sjukvårdens adressregister, är en grund för behörighetstilldelning och information i andra system. Det är informationen från HSA-katalogen som visas på bl.a. 1177.se och landstingets webbplatser. Det viktigt att alla medarbetare har korrekta uppgifter inlagda i HSA-katalogen.

Föreslagna aktiviteter:

- Säkerställ att alla behörighetsgrupper är korrekta och att alla medarbetare har korrekta behörigheter
- Tillse att rutin finns för att lägga till, ändra och ta bort behörigheter vid förändring av anställningsförhållanden
- Tillse att det finns en utsedd person med ansvar att hålla HSA-katalogen uppdaterad.

3 Lösenord och säkerhetskoder

Lösenordsregler inom Landstinget i Uppsala län anger en standard för hur varje enskild individ skapar ett starkt lösenord, skyddar sitt lösenord samt hur ofta respektive lösenord ska förnyas.

Säkerhetskoder för e-tjänstekort skickas alltid till folkbokföringsadressen och ska förvaras som en värdehandling.

Lösenord och säkerhetskoder är personliga och ska hanteras som sekretessbelagd information.

Hantering av lösenord är beskrivet i dokumentet ”Lösenordsregler inom Landstinget i Uppsala län”. Länk: Lösenordsregler inom Landstinget i Uppsala län (raderad länk till landstingets intranät)

Föreslagna aktiviteter:

- Tillse att alla medarbetare har kännedom om dokumentet ”Lösenordsregler inom Landstinget i Uppsala län”.

4 Driftsavbrott och reservrutiner

Reservrutiner för planerade och oplanerade driftsavbrott ska finnas. Den verksamhet som bedrivs ska kunna bedrivas i beslutad omfattning även under ett driftsavbrott. Det krävs att den information som är kritisk för verksamheten identifieras och att lämpliga reservrutiner tas fram.

Föreslagna aktiviteter:

- Säkerställ att kunskap finns om vilken information och vilka informationsbärande system som är kritiska för att kunna bedriva verksamheten
- Tillse att reservrutiner finns och att dessa hålls uppdaterade och att all personal känner till dessa.

5 Tillgång till information i vårdsystem

Denna fråga gäller endast verksamheter som har direkt eller indirekt kontakt med patientinformation.

För att få ta del av patientuppgifter krävs att åtkomsten har stöd i patientdatalagen. Landstinget i Uppsala län har riktlinjer som förtydligar och konkretiserar patientdatalagen. För att kontrollera om åtkomster som gjorts haft stöd sker loggkontroller. Viss del av loggkontrollen förväntas ske i verksamheten. Exempelvis då en känd person vårdas på enheten ska en logg begäras från CESÅ för att säkerställa att ingen olovligen gått in i dennes journal.

Det är viktigt att all personal är informerad att loggning sker.

Hur landstinget hanterar loggrapporter och dataintrång finns beskrivet i dokumentet ”Regelverk avseende hantering av loggrapporter för vårdsystem samt åtgärder vid dataintrång”.

Länk: Regelverk avseende hantering av loggrapporter för vårdsystem samt åtgärder vid Dataintrång (raderad länk till landstingets intranät)
Vilka regler som gäller vid åtkomst till patientuppgifter finns beskrivet i dokumentet ”Riktlinjer för åtkomst till patientuppgifter i journal”.

Länk: Riktlinjer för åtkomst till patientuppgifter i journal (raderad länk till landstingets intranät)

Föreslagna aktiviteter:

- Tillse att alla medarbetare känner till dokumenten ovan
- Tillse att rutiner finns för att göra extra loggkontroller då exempelvis en person med högt nyhetsvärde vårdas
- Säkerställ att alla medarbetare känner till att loggning sker.

6 Mobila it-enheter

Dokumentet ”Riktlinjer för mobila enheter” beskriver användande och anslutning av iPhones, surfplattor och andra mobila it-enheter till landstingets system och infrastruktur. Riktlinjerna syftar till att säkerställa en korrekt hantering av landstingets information. I dokumentet beskrivs bl.a. användarens egna ansvar för lagring och backup av information.

Länk: Riktlinjer för mobila enheter (raderad länk till landstingets intranät)

Föreslagna aktiviteter:

- Tillse att rutiner finns att alla som får en mobil enhet blir informerade om dokumentet ”Riktlinjer för mobila enheter”.

7 Identifierade risker

God 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 divisioner/förvaltningar där systematiska fel verkar ligga bakom lyfts sedan som landstingsgemensamma risker och hanteras därefter.

Föreslagna aktiviteter:

- Tillse att riskanalyser görs vid förändrade arbetssätt eller byte av tekniska stöd
- Tillse att möjligheter ges för medarbetare att framföra risker de identifierat
- Säkerställ att rutiner finns för att hantera/åtgärda identifierade risker
- Sammanställ identifierade risker i Egenkontrollen.

8 Informationssäkerhetsnivå

I Landstingets IT-policy står att vi ska ha en säkerhetsnivå som är väl avvägd, motiverbar och accepterad. Informationssäkerhetsnivån blir en produkt av lagar och förordningar samt verksamhetens egna krav. Därtill kommer landstingsgemensamma regler och riktlinjer.

Föreslagna aktiviteter:

- Gör en bedömning av huruvida nivån på informationssäkerheten på enheten är avvägd, motiverad och accepterad.

Bilaga 8 Checklista egenkontroll – Landstinget i Uppsala län

Checklista Egenkontroll 2014 – bilaga Rapport informationssäkerhet 2013
Denna ska fyllas i och återsändas till it-ansvarig senast 2014-12-31.

Gäller verksamhet/avdelning/enhet:
Ifylld av:

1. Introduktion och utbildning

Är alla medarbetare medvetna om styrande dokument inom området It- och informationssäkerhet?	JA	NEJ
Har alla nyanställda medarbetare deltagit i en introduktionsutbildning?	JA	NEJ

Kommentar:

2. Användaradministration

Är alla uppgifter i HSA-katalogen aktuella?	JA	NEJ
Har behörighetstilldelningen kontrollerats och vid behov reviderats under året?	JA	NEJ

Kommentar:

3. Lösenord och säkerhetskoder

Hanteras lösenord och säkerhetskoder enligt gällande regler?	JA	NEJ

Kommentar:

4. Driftsavbrott och avbrottsrutiner

Finns avbrottsrutiner för verksamhetskritiska system, exempelvis Cosmic, T4, RIS/PACS, Landlord, Trafikinformationssystem etc?	JA	NEJ
Är befintliga avbrottsrutiner kända på arbetsplatsen?	JA	NEJ

Kommentar:

5. Åtkomst till vårddokumentation

Är "Riktlinjer för åtkomst till patientuppgifter i journal" känd på arbetsplatsen?	JA	NEJ
Känner medarbetare till att åtkomst till patientuppgifter loggas?	JA	NEJ
Är "Regelverk avseende hantering av loggrapporter för vårdsystem samt åtgärder vid dataintrång" känd på arbetsplatsen?	JA	NEJ

Kommentar:

6. Mobila it-enheter

Får medarbetare som nyttjar mobila it-enheter information om riktlinjerna?	JA	NEJ

Kommentar:

7. Identifierade risker

Vilka specifika risker har enheten/verksamheten identifierat som kan hota information med avseende på sekretess, spårbarhet eller tillgänglighet?

Svar:

Har enheten identifierat områden eller arbetsprocesser där det allmänt anses finnas en förhöjd informationssäkerhetsrisk? Om ja, vilka?	JA	NEJ

Svar:

8. Informationssäkerhetsnivå

Anser ni er ha rätt informationssäkerhetsnivå för er enhet? Om nej, vad behöver åtgärdas?	JA	NEJ

Svar:

Bilaga 9 Fokusområden 2014 – Landstinget i Uppsala län

Bilaga till Rapport informationssäkerhet 2013

2014-03-19

Fokusområden Informations-/IT-säkerhet 2014

Dessa områden kommer insatserna under 2014 att fokusera på. De är valda genom omvärldsanalys och genom sådant som framkommit i olika revisioner/granskningar.

Inre säkerhet
Landstinget har under senare år investerat ganska mycket i det s.k. perimeterskyddet, vilket är skyddet mot omvärlden. Vi har nu stora möjligheter att filtrera olika typer av trafik, detektera intrång och stoppa olika typer av skadlig kod. Detta är gjort enligt scenario att någon försöker hacka sig in utifrån.

Nästa scenario är att någon försöker ta sig in i våra system från insidan. Det förutsätter förstås fysisk åtkomst till nätet, vilket gör att en inkräktare fysiskt behöver befinna sig på plats. Det är dock ett möjligt scenario och ett område som ska belysas och om behov finns förstärkas.

Möjliga åtgärder som kan behövas är utökningar i krypteringsmekanismer för trafik internt samt fortsatt segmentering av system internt. Andra områden är accesskontroll av enheter och separation i hur olika enheter ansluter till det trådbundna nätverket.

Känsliga uppgifter i ekonomihanteringen
En stor del av den vård som utförs sker på uppdrag av andra landsting som i sin tur ska betala för vården. I den betalningsprocessen innefattas att det betalande landstinget behöver information om vilken patient det gäller samt vilka åtgärder som utförts. Det för att känsliga uppgifter, med stöd av patientdatalagen, hanteras av ekonomipersonal och lämnas ut till andra landsting. Tidigare har insatser gjorts för att säkerställa att minsta möjliga mängd av känsliga uppgifter lämnas ut. Dock finns behov att säkerställa att detta görs på ett korrekt sätt och att överföringen av uppgifterna till andra landsting sker säkert.

Styrande dokument
Landstingets styrande dokument inom informationssäkerhetsområdet bör kompletteras med mer detaljerade riktlinjer kring it-säkerhet. Landstingets it-miljö är till stora delar centraliserad och den mesta driften sker inom MSI. Dock sker delar av driften av FTV, UL m.fl. Det måste vara tydligt att dessa enheter lyder under samma regelverk som övriga landstinget. Gemensamma riktlinjer ska säkerställa detta. Informationsklassning är ett annat område 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.

Funktionskonton

För att kunna införa SSO och kortinloggning i större skala behöver vi få en bättre kontroll på och möjligen också bättre riktlinjer kring användandet av funktionsinloggningar. Frågor som ska belysas är i vilka situationer funktionsinloggningar får användas, hur spårbarhet ska upprätthållas och till vad de får användas.

SCADA-system

Värme, ventilation, vatten och el är exempel på system som styrs av datorer, s.k. SCADA-system. Det finns ökade krav på att dessa är anslutna till Internet och de blir då utsatta för samma problematik som medicintekniska system. Produkterna är ofta CE-märkta och har ibland en gammal plattform som bas. Arbete pågår att säkerställa att dessa enheter är logiskt skilda från det övriga nätverket. Frågan bör dock lyftas till säkerhetsavdelningen då it-säkerhetsfrågorna måste få en naturlig plats när man riskanalyserar tillgång till vatten, el osv.

Informationssäkerhet i upphandling

Det finns troligen förbättringspotential gällande informationssäkerhet i upphandlingar. Upphandlingsavdelningen är målgruppen och målet är en förhöjd kunskapsnivå kring hur säkerhetskrav tas fram i upphandlingsprocessen.

Egenkontroll

Fortsatt arbete i att sprida processen kring egenkontroll. Fokus både på verksamheterna och på förvaltningsobjekten.

Bilaga 10 Utdrag ur Västra Götalandsregionens säkerhetsredovisning 2013

Följande är ett utdrag ur rapporten ”Redovisning av säkerhetsarbetet och säkerhetsläget i Västra Götalandsregionens verksamheter 2013”.

Författare: Jan S Svensson, Västra Götalandsregionen

Datum: 2014-03-11

Utgångspunkter

Säkerhetsarbetet i Västra Götalandsregionens verksamheter ska bedrivas på ett säkert, systematiskt och ändamålsenligt sätt. Regionfullmäktige har under 2013 fastställt Regional strategi[77] med sju strategiska mål för säkerhetsarbetet i Västra Götalandsregionens verksamheter 2013–2016. Strategin innehåller sju strategiska mål med framgångsfaktorer och aktiviteter samt inriktning för hur säkerhetsarbetet ska bedrivas. Målet för Västra Götalandsregionens samlade regelverk kring säkerhet är att bidra till ökad trygghet, god informationshantering, ökad effektivitet, ökad patientsäkerhet och robusthet i verksamheterna så att kriser och oönskade händelser kan hanteras på ett bra sätt.

Beredning

Redovisningen i denna rapport bygger på sammanställning av inkomna svar på frågor i en webbaserad enkät som skickats ut till 45 förvaltningar och bolag. Enkäten omfattar i huvudsak frågor kring de sju strategiska mål som regionfullmäktige fastställt under 2013. Enkäten omfattar också frågor kring krishanteringsförmåga, regiongemensamma risker, personsäkerhet och informationssäkerhet. I enkäten finns också särskilda frågor till verksamheter inom hälso- och sjukvård. Dessa frågor är kopplade till Socialstyrelsens föreskrifter bland annat vad gäller spärr av vårddokumentation och behörigheter.

Alla förvaltningar och bolag har besvarat frågor i aktuell webbenkät. Totalt berör enkäten kring säkerhetsarbetet 51 126 anställda i Västra Götalandsregionen. VGR IT ingår organisatoriskt i regionkansliet men har lämnat eget enkätsvar som berör 556 personer. Regionkansliets redovisning i övrigt berör 463 personer varav 297 tillhör ledningskansliet.

Utöver denna rapport redovisas säkerhetsarbetet i Västra Götalandsregionens årsredovisning för 2013. Som komplement till denna rapport finns två särskilda presentationer med samlade och detaljerade svar på enkätfrågor. En presentation innehåller svar från alla 45 verksamheter och bolag och en presentation innehåller frågor och svar från 11 verksamheter inom hälso- och sjukvård.

Sammanfattning av säkerhetsarbetet i Västra Götalandsregionen

Den samlade bilden av säkerhetsarbetet och säkerhetsläget i Västra Götalandsregionens verksamheter är att läget i huvudsak är stabilt men det finns utvecklingspotential inom flera

[77] Regional strategi för säkerhetsarbetet i Västra Götalandsregionens verksamheter 2013–2016, fastställd av regionfullmäktige 14 maj 2013, § 86, dnr RS 572-2011.

områden. Västra Götalandsregionens verksamheter har under senare år haft problem med IT-säkerheten. En övergripande handlingsplan för informationssäkerhet har under året beslutats av regionstyrelsen. Jämfört med tidigare år kan 2013 betraktas som planernas och strategiernas[78] år vilket innebär många aktiviteter som ökar IT-säkerheten. Det handlar om uppgradering av IT-system och befintlig IT-infrastruktur men också om utbildningsinsatser och andra åtgärder som på sikt ökar robustheten och IT-säkerheten i verksamheterna. Under året har planerade aktiviteter börjat genomföras och aktiviteter fortsätter att genomföras under 2014.

Trots problem med IT-säkerheten, nya hot och risker, är bedömningen att vidtagna åtgärder under året, planerade aktiviteter och strategier brutit en negativ trend kring IT, eller åtminstone bromsat upp denna trend. IT-säkerheten ökar successivt när planerade åtgärder genomförs och när IT-säkerheten ökar försvåras bland annat dataintrång och skadlig kod i våra IT-system.

Intresse och förståelse för säkerhetsfrågor har ökat under året i flera verksamheter. Fler säkerhetsaktiviteter och fler risk- och sårbarhetsanalyser (RSA) har genomförts under 2013 än under tidigare år. Arbetet med säkerhetsfrågor i sjukvårdens verksamheter har bedrivits på ett strukturerat och systematiskt sätt. Ändamålsenliga rutiner och processer finns ofta etablerade. När det gäller övningar kring kris- och katastrofledning finns det utvecklingspotential för många verksamheter. Intresset inom hälso- och sjukvården kring administrativa säkerhetstjänster har ökat under året.

Användning av sociala medier innebär ökade möjligheter för Västra Götalandsregionen att sprida information och komma i kontakt med invånarna. Samtidigt innebär sociala medier en ökad risk när exempelvis skadlig och felaktig information får snabb och okontrollerad spridning som kan innebära hot och risker som inte är förutsägbara.

Informationssäkerhet

Information är en viktig tillgång för alla verksamheter i Västra Götalandsregionen och den måste kommuniceras, förstås, skyddas på ett säkert sätt. Flödet av information har under 2013 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. Under 2013 har en övergripande handlingsplan för informationssäkerhet beslutats av regionstyrelsen. 52 mnkr avsattes för ett genomförande av denna handlingsplan varav 41 mnkr är kopplade till finansiering av IT-säkerheten. I handlingsplanen finns i huvudsak följande aktiviteter och åtgärder:

- Åtgärder som innebär att Västra Götalandsregionen medverkar och stödjer nationellt informationssäkerhetsarbete inom vård- och omsorgssektorn.

[78] Exempelvis Handlingsplan för arbetet med informationssäkerhet i VGR, Regional strategi för säkerhetsarbetet i Västra Götalandsregionens verksamheter 2013–2016, IS/IT-strategi för perioden 2014–2106, IT-säkerhetsstrategi, förslag på ny säkerhetspolicy och förslag (remissversion) på nya riktlinjer för informationssäkerhet.

- Åtgärder som förstärker ägarstyrning genom revidering av ledningssystem för informationssäkerhet (LIS), förankring i nämnder och styrelser, utformning av regelverk inom det medicintekniska området och regelverk för tekniska system.
- Åtgärder som förstärker verksamhetsstyrningen genom funktion för operativt säkerhetsarbete.
- Informationssäkerhetsutbildning till tekniker och särskild högskolebaserad uppdragsutbildning för införande av ledningssystem i den egna verksamheten.
- Åtgärder som ökar säkerhetskulturen inom VGR IT.
- Interaktiv utbildning i informationssäkerhet för anställda i hälso- och sjukvård.

IT-säkerheten har förbättrats under året

IT-säkerhet är en komplex verksamhet och resurser till ökad IT-säkerhet är viktigt. För att förbättra säkerheten har en del nödvändiga uppgraderingar av IT-system och IT-infrastruktur genomförts under 2013. Utöver ny IS/IT-strategi, som fastställts av regionledningen, har också en IT-säkerhetsstrategi och en handlingsplan för IT-säkerhet tagits fram. Under året har några nya byggstenar för ökad IT-säkerhet kommit på plats:

- Införandet av Single Sign On (SSO) på sju system under året och ytterligare 20 system nästa år som innebär minskade inloggningstider och bättre användarupplevelse.
- Påbörjat projekt med säker identitetshantering som innebär automation för behörigheter och säkra identiteter på behörigheter och användare. Automatiserat hela vägen för tre system som automatiskt skapar behörigheter när attest gjorts av en chef.
- Säkrare nät innebär att modernt skydd finns på trådlös och trådbunden kommunikation. Under året har 97 procent av Västra Götalandsregionens trådlösa kommunikation flyttats till ett säkert certifikatbaserat nät.
- Etablerat hela processen för larmhantering för IT-system.
- Investeringar i Windows 7, inklusive Office 2013, har effektiviserat och gjort den personliga arbetsplatsen säkrare.

Bilaga 11 Enkätfrågor i Västra Götalandsregionens säkerhetsredovisning

Del 2 Allmänna frågor

16. Mål 7 – De viktigaste processerna och informationsmängderna är identifierade

	1	2	3	4	5	
Stämmer inte alls	☐	☐	☐	☐	☐	Stämmer helt

17. Mål 7 – Förvaltningens skyddsvärda information har klassificerats

	1	2	3	4	5	
Stämmer inte alls	☐	☐	☐	☐	☐	Stämmer helt

18. Mål 7 – Skyddsvärd information lagras och kommuniceras internt och externt (via exempelvis e-post) på ett säkert och tillfredsställande sätt

	1	2	3	4	5	
Stämmer inte alls	☐	☐	☐	☐	☐	Stämmer helt

19. Mål 7 – Det finns rutiner som kan tillämpas vid IT-avbrott

	1	2	3	4	5	
Stämmer inte alls	☐	☐	☐	☐	☐	Stämmer helt

Del 6 – Informationssäkerhet

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 regelverk, rutiner, omfattning av övervakning och kontroll samt revision och uppföljning.

34. Säkerhetsarbetet i VGR styrs av ett regelverk som består av policy, strategi, riktlinjer, mål, anvisningar, instruktioner och beskrivningar. Detta regelverk behöver utvecklas.

	1	2	3	4	
Stämmer inte alls	☐	☐	☐	☐	Stämmer helt

35. Ange exempel på hjälp/stöd som skulle underlätta det egna/lokala säkerhetsarbetet och som borde a) utvecklas, b) förtydligas eller c) avvecklas.

☐ a) Följande behöver utvecklas: [UTRYMME FÖR FRIA SVAR]
☐ b) Följande behöver förtydligas: [UTRYMME FÖR FRIA SVAR]
☐ c) Följande kan avvecklas: [UTRYMME FÖR FRIA SVAR]

☐ Inget behöver utvecklas, förtydligas eller avvecklas

☐ Frågan är inte relevant för min förvaltning

36. Regler, råd och anvisningar för hur säkerhetsarbetet ska bedrivas är komplexa och omfattande och behöver förenklas.

	1	2	3	4	
Stämmer inte alls	☐	☐	☐	☐	Stämmer helt

37. Mål 7 – arbetet med informationssäkerhet är att säkerställa att information finns tillgänglig när den behövs, att den är korrekt, att obehöriga inte har tillgång till den (konfidentialitet) och att den kan spåras. Innebörd och konsekvenser av dessa mål är kända för all personal.

	1	2	3	4	
Stämmer inte alls	☐	☐	☐	☐	Stämmer helt

38. IT-säkerheten har förbättrats under 2013.

☐ Nej, IT-säkerheten har inte förbättrats

☐ Ja, IT-säkerheten har förbättrats bland annat genom följande åtgärder: [UTRYMME FÖR FRIA SVAR]

39. Personalen behöver utbildning i informationssäkerhet

	1	2	3	4	
Stämmer inte alls	☐	☐	☐	☐	Stämmer helt

40. Informationssäkerhet och olika utbildningsområden. Ange viktiga och mindre viktiga områden. 6 står för viktigaste område/områden och 1 står för minst viktigt område/områden.

	1	2	3	4	5	6
Policy, riktlinjer och anvisningar	☐	☐	☐	☐	☐	☐
Rutiner och instruktioner	☐	☐	☐	☐	☐	☐
Övervakning och kontroll	☐	☐	☐	☐	☐	☐

Revision och uppföljning	☐	☐	☐	☐	☐	☐
Grundläggande om säkerhetskultur	☐	☐	☐	☐	☐	☐
Grundläggande om administrativ säkerhet	☐	☐	☐	☐	☐	☐
Grundläggande om fysisk säkerhet	☐	☐	☐	☐	☐	☐
IT-säkerhet och hur vi kommunicerar information på ett säkert sätt	☐	☐	☐	☐	☐	☐
IT-säkerhet och hur vi skyddar informationen på ett säkert sätt	☐	☐	☐	☐	☐	☐
Grundläggande om IT-säkerhet	☐	☐	☐	☐	☐	☐

41. Den regionala säkerhetsstrategin för perioden 2013–2016 är ett stöd i arbetet med säkerhetsfrågor.

	1	2	3	4	
Stämmer inte alls	☐	☐	☐	☐	Stämmer helt

42. Övriga synpunkter och kommentarer på säkerhetsarbetet och säkerhetsläget 2013.

☐ Kommentar säkerhetsarbetet: [UTRYMME FÖR FRIA SVAR]
☐ Kommentar säkerhetsläget: [UTRYMME FÖR FRIA SVAR]
☐ Inga synpunkter eller kommentarer

Bilaga 12 Internkontroll – Skellefteå kommun

Informationssäkerhet

Ett av kontrollmomenten enligt nämndens internkontrollplan handlar om hur pass känd och förankrad nämndens informationssäkerhetspolicy är i organisationen. En enkät har skickats ut till 30 chefer (10 på varje avdelning).

Fråga, %	2013	2012
Känner till att vi har en informationssäkerhetspolicy	36	40
Har tagit del av informationssäkerhetspolicyn	36	40
Har informerat sin personal	24	16

För att göra policyn ännu mera känd kommer den att informeras om på chefsdagar och genom olika informationskanaler på nya Insidan.

Verksamhetssystemet Procapita

Rutin för anställdas tillträde/ändringar/avslut i IT-system finns i nämndens Informationssäkerhetspolicy som är utlagd på Insidan. I systemet skapas en logg när en person läst, sparat, makulerat, felmarkerat och/eller tagit bort. Vilka urvalsparametrar som användaren angett vid sökning kan också spåras.

Systemansvariga utför kontinuerliga kontroller genom att aktiviteter kontrolleras löpande. Systemansvariga kontrollerar även logg vid anmodan eller misstanke från verksamhetsansvarig gällande brott mot sekretesslagen. Vid anmärkningar kontaktas aktuell användare och verksamhetsansvarig. Vid överträdelse görs numera alltid en lex Sarah-anmälan av berörd systemförvaltare. Rapport över genomgångna loggar och eventuella avvikelser inlämnas årligen till systemägaren (chefscontroller) som underlag för utvärdering av rutinen.

Individ- och familjeomsorg

Avdelningen kontrollerar löpande tillgänglighet, riktighet, sekretess och spårbarhet. Systemförvaltaren ger löpande behörigheter i systemet och går vid behov igenom sekretessregler och arbetssätt i systemet. I samband med genomgång av löpande loggning kontrolleras tillgänglighet, sekretess och spårbarhet. Loggningen sker både systematiskt och slumpmässigt. Det är bara systemförvaltare och enhetschefer som har behörighet att ta bort felaktiga anteckningar och dokument (riktighet) i verksamhetssystemet. Under 2013 har fram till dags dato inga överträdelser av vikt kunnat påvisas. Ett antal loggningar har visat att handläggare har varit in i andra journaler, dessa är utredda och klargjorda.

Loggning av användare i Procapita VoO (äldre- och handikappomsorg)

Kontrollen av 10 slumpmässigt utvalda användare per månad visade på avvikande datatrafik för 1 användare (januari–september 2013). Vid avvikelse meddelas verksamhetsansvarig som då inleder dialog med användaren. Den användare som denna gång haft avvikande datatrafik konstaterades inte ha haft något uppsåt att kontrollera utan överträdelsen berodde till fullo på okunskap om systemets funktion. Felet är nu rättat och information/utbildning har lämnats till berörda personer.

Handikappomsorg

Styrande dokument för kvalitet som avser hantering av personuppgifter, ärendeuppgifter, journalföring och liknande ska innehålla regler om uppgifter i dokumentationen:

Informationen är åtkomlig/användbar för den som är behörig (tillgänglighet)

Här tillämpas en strikt behörighetssättning. Den anställde får bara behörighet där den jobbar och det är den anställdes chef som beslutar och beställer behörigheten. Den risk som finns är att cheferna kan glömma att meddela avslut vilket kan leda till att personalen har för stora behörigheter under en tid. Detta har upptäckts vid ett antal tillfällen. Systemansvariga fortsätter att informera cheferna om rutinen via Insidan och på chefsträffar.

Informationen är oförvanskad (riktighet)

Baspersonalen har en automatisk signatur när de sparar ner text vilket innebär att den som läser informationen kan se vem som skrivit vad. Handläggarna har inte denna automatiska signatur vilket gör att det inte som läsare av utredningen går att se vem som skrivit. Om man är inne i systemet så går det att se vem som senast sparade texten men här finns en brist genom att det är möjligt att skriva över någon annans text.

Handläggarna har källhänvisning vid de tillfällen då de refererar till tredje part, t.ex. läkare, samt ett inskannat dokument som stödjer detta. Baspersonal har inte det. Är det en uppgift från annan så ska källan uppges. Det saknas idag en rutin som reglerar detta vilket det även gjorde vid 2012 års internkontroll. Av 10 kontrollerade utredningar under 2013 hade 8 en källhänvisning.

Informationen är sekretessbelagd (sekretess)

Som tidigare påpekats finns en strikt behörighetssättning. Den anställde får bara behörighet där den jobbar och det är personens chef som beslutar och beställer behörigheten. Det finns också reglerat vad varje roll får möjlighet att se och göra. En brist är att det i dagsläget inte går att stänga av en användare från en specifik journal. Det innebär att om du har tillgång till en enhet så har du också tillgång till alla brukare som ingår i den enheten.

Informationen kan entydigt härledas till en identifierad användare (spårbarhet)

I Procapita skapas en logg vid läst, sparat, makulerad, felmarkerad och tagit bort. Loggning utförs enligt rutin som finns utlagd på Insidan.

Hälso- och sjukvård

Styrande dokument som avser hantering av personuppgifter, ärendeuppgifter, journalföring och liknande ska innehålla regler om uppgifter i dokumentationen:

Informationen är åtkomlig/användbar för den som är behörig (tillgänglighet)

Genom övertagandet av hemsjukvården har hälso- och sjukvårdpersonal inom äldreomsorgen fått bredare behörigheter som inkluderar dokumentation inom både äldre- och handikappomsorgen. Främst till följd av att nattpersonalen täcker upp för brukare inom båda avdelningarna. Hälso- och sjukvårdspersonal som endast arbetar dagtid inom handikappomsorgen har bara behörigheter till handikappomsorgens brukare. Det är

cheferna inom hälso- och sjukvården som gör beställningar av behörigheter. Rutiner för de anställdas tillträde/ändringar/avslut finns utlagt på Insidan. Den risk som finns är att cheferna kan glömma att meddela avslut vilket kan leda till att personalen har för stora behörigheter under en tid. Systemansvariga fortsätter att informera cheferna om rutinen via Insidan och på chefsträffar.

Informationen är oförvanskad (riktighet)
Personalens dokumentation kan sparas utan signering och ändras av samma person inom 14 dagar, därefter blir texten låst.

Informationen är sekretessbelagd (sekretess)
Det finns idag inte möjlighet att stänga av en användare från en specifik journal, har personen tillgång till hela äldreomsorgen så innebär det tillgång till samtliga brukare inom äldreomsorgen.

Informationen kan entydigt härledas till identifierad användare (spårbarhet)
I Procapita skapas en logg vid läst, sparat, makulerad, felmarkerad och tagit bort. Loggning utförs enligt rutin. Loggningsrutinen finns utlagd på Insidan.

Intraphone (SoL)
Intraphone är ett IT-stöd som syftar till att samla in data för när insatser utförts och vilka insatser som utförts. Varje användare i systemet har behörighet till det arbetslag man jobbar i/ska hantera information från. Varje användare har också en användarroll i Intraphone.

Informationen är åtkomlig/användbar för den som är behörig (tillgänglighet)
Varje person har en eller flera roller beroende på vilka åtaganden man har i Intraphone. Personen ska enbart ha en relevant roll för det arbete som ska utföras. Dokument som beskriver roller och behörigheter finns framtaget. Det finns ett delat ansvar mellan rollen som s.k. Intraphonist och ledning när det gäller behörighetssättning av personal. Stickprov visar att det finns behov av att påminna Intraphonister och ledning att ta bort behörigheter på rollen personal när vårdrelationen till brukaren inte längre finns kvar.

Informationen är oförvanskad (riktighet)

- Användare i systemet har sin egen unika pinkod och s.k. Yubikey vilket gör att man kan se vem det är som redigerat/skapat en rapport.
- Det går att logga och se vem som ändrat/skapat behörigheter i rollen ledning och Intraphonist.
- När rollen personal loggar in i Intraphone används en gemensam Yubikey som är kopplad till arbetslaget man har behörighet till. Varje person har dock sitt eget unika användarnamn och unika pinkod.
- När insatsrapporterna registreras, oavsett teknik, används alltid personens egen unika kod.
- När det gäller dubbelbemanning kan man skapa den medföljande personalens insatsrapport efter att man fått dennes kod. Dock godkänner och redigerar den medföljande personen sin egen rapport.

Stickprov visar att av 10 kontrollerade dubbelbemanningsrapporter hade 8 stycken skapat rapport även till sin kollega. Av dessa var alla 10 godkända av den medföljande som inte skapat rapporten.

Informationen är vid behov sekretessbelagd (sekretess)

- Rollerna Ledning och Intraphonist, som ger behörigheter till övrig personal, har enbart behörighet till de arbetslag de själva har behörighet till. Dokument som beskriver hur arbetslagen är kopplade till respektive brukarorganisation finns framtagen.
- Det finns idag inte möjlighet att stänga av en användare från en specifik brukare. Har man tillgång till ett arbetslag som är kopplat till brukarorganisationen så har man tillgång till alla brukare inom den brukarorganisationen.

Informationen kan entydigt härledas till identifierad användare (spårbarhet)
Det skapas loggningar på allt som kan härledas till insatsrapporterna. Även historikposter på behörighetsförändringar samt integrationer med Procapita. På insatsrapporterna loggas en mängd information. Loggning i Intraphone sker enligt rutin två gånger per år och protokollförs.

TimeCare
Informationen är åtkomlig/användbar för den som är behörig (tillgänglighet)
Det finns en strikt behörighetssättning som innebär att en person bara har behörighet där den arbetar samt att det är personens chef som beställer behörigheten. Om cheferna glömmer att meddela avslut har personalen för stora behörigheter. Chefer har behörighet till eget område och samarbetskollega. Användaren har bara behörighet till sig själv och schemaansvarig (SAG) har behörighet till chefens grupper.

Informationen är oförvanskad (riktighet)
Chef och baspersonal registrerar frånvaro i TimeCarePool efter uppgifter i Personec P och TimeCarePlanering. Personal- och schemaansvarig (SAG) gör ett schema som sedan ska godkännas av chefen som också är den som exporterar/importerar till lönesystemet. Den risk som finns är att chefen inte kollar av schemat och felaktigheter uppstår.

Informationen är vid behov sekretessbelagd (sekretess)
I systemet finns möjligheten att visa att anställd har skyddad identitet. Det innebär att personens namn och telefonnummer döljs vid utskrift av rapporter. Kunder i TimeCarePool har endast kundnummer. I TimeCarePlanering finns namn, person- och anställningsnummer.

Informationen kan entydigt härledas till identifierad användare (spårbarhet)
I TimeCare loggas ett stort antal händelser som kan härledas till en identifierad användare. Bedömningen är att loggningen är tillräcklig.

Bilaga 13 Urval av revisioner

Landstingsrevisioner

Tillämpningen av informationssäkerheten inom vården, Stockholms läns landsting, 2012
Översyn av informationssäkerheten, Västra Götalandsregionen, 2012
Informationssäkerheten i Landstinget i Kalmar län, 2010
Övergripande IT- och informationssäkerhet, Landstinget Dalarna, 2011
Journalsystem och informationssäkerhet, Landstinget Västernorrland, 2012
Granskning av vårdgivarens informationssäkerhet, Västerbottens läns landsting, 2012

Kommunrevisioner

It-säkerhet, Bengtsfors, 2009
It-revision, Burlöv, 2010
It-revision, Båstad, 2010
It-säkerhet, Finspång, 2010
It-säkerheten, Haninge, 2010
It- och informationssäkerhet, Helsingborg, 2012
Informationssäkerhet, Hofors, 2014
It-verksamheten, Hylte, 2014
Informationssäkerhet, Järfälla, 2010
It-hanteringen, Katrineholm, 2012
It-revision, Kungsbacka, 2014
Informationssäkerhet, Lerum, 2011
Informationssäkerhet, Lycksele, 2010
It-granskningar, Malmö, 2013
It-säkerhet och behörighetskontroller, Mölndal, 2011
Informationssäkerhet, Nacka, 2011
Informationssäkerhet, Ovanåker, 2013
It-granskning, Stenungsund, 2006
Informationssäkerhet, Solna, 2011
Informationssäkerhet, Strängnäs, 2014
Generella it-kontroller, Svedala, 2011
It-säkerhet, Söderhamn, 2006
It- och informationssäkerhet, Södertälje, 2012
Informationssäkerhet, Timrå, 2013
It-säkerhet, Trollhättan, 2013
It-säkerheten, Uddevalla, 2013
Informationssäkerhet, Umeå, 2011
It-revision, Upplands-Väsby, 2014
It- och informationssäkerhet, Vetlanda, 2013
It-verksamheten, Vänersborg, 2007
Informationssäkerhet, Ånge, 2013
It-säkerheten, Östhammar, 2009

Bilaga 14 Lathund för informationssäkerhet – Landstinget i Jönköpings län

Exempel på avvikelser avseende informationssäkerhet:

Riktighet

- Felaktiga personuppgifter, t.ex. felaktigt personnummer, adress, telefonnummer
- Felaktig information på exempelvis remiss
- Förväxling i journal, t.ex. information skrivs på fel patient i journalen
- Felaktig information skickas ut till patienten – tid, undersökning, förberedelse etc.
- Fel journal från arkivet
- Felaktig information publicerad på intranät/Internet.

Sekretess

- Felfaxning av journal
- Uppgifter kring patient lämnats ut till fel person
- Diskussion kring patienter i reception, risk för avlyssning
- Posthantering – skyddade personuppgifter
- Posthantering – journaler skickas i internkuvert
- Utskrifter på fel skrivare
- Fel behörighet till användare
- Användare lånat ut sin behörighet.

Spårbarhet

- Avsaknad av loggfiler – försvunna/förstörda/ej utlämnade.

Tillgänglighet

- Patientinformation saknas
- Uppgifter kring patient hamnat på avvägar, t.ex. inskrivet i fel journal
- Ingen tillgång till journaluppgifter, t.ex. ej dikterade diktat, ej inskrivna diktat.