Reserapport
ISO/TC 215/WG 4

Security, Safety and Privacy

ISOTC 215 Karuizawa Meeting
2014-05-18 / 2014-05-23.
Svensk spegelkommitte ”SIS/TK 334/AG 3 Säkerhet och kvalitet”

Lämnade Arlanda 17/5 med sikte på att komma fram dagen innan mötet startade pga tidsskillnaden om sju timmar. Resan gick bra förutom lite löpträning i Kastrup pga första planet på Arlanda inte ville fungera.

Den fråga jag som ersättare för Rikard Lövström ombetts bevaka extra noga var ISO 27799, speciellt bilagan innehållande ett ”balance score card”. För övrigt följa med efter bästa förmåga som nybörjare på ISO-möte.

Dag 1
Beskriv bäst i reserapporten ”Mötesanteckningar Kariuzawa mw.pdf” utskickad av Lena Morgan (SIS) den 26 maj 2014 10:23. (De inledande föredragen var tillbakablickande på ett sätt som är svårt att hänga med i som ”rookie”.)

Trots detta, några allmänna reflektioner:

Den japanske värden visar på en stark satsning (föredraget ”IT-Strategy and Health IT Policy”) i riktning mot att Japan ska bli bäst på hälsoinformatik. Samtidigt var flera av de utmaningar och förbättringsåtgärder som beskrevs tämligen bekant materia ur svenskt perspektiv.

- Kostnadsexplosion för sjukvård. - Inget nytt under solen, allt fler åkommor kan vårdas på allt flera sätt, så ock i Sverige. Ökande medellivslängd och åldrande befolkning (den ”demografiska fällan”) - samma i Sverige som i Japan, om än kanske med olika magnitud.

- En journal, En patient. - Samma ambition i Sverige med ett antal initiativ i riktning mot konsolidering (regionalt i Stockholm med Take Care, nationellt med tex NPÖ). ”Myntets andra sida” inte minst konfidentialitetsperspektivet berördes mera kortfattat i slutet av föredraget. Dvs för vårdkedjor m m är naturligtvis stark integration önskvärt. Ur konfidentialitetsperspektiv ställer samma starka integration avgjort högre krav på bra säkerhetssystem.

- Systemintegration i sig är inte tillräckligt utan integration krävs även av informationen och framförallt (den regionala) användningen av informationen. - Noterar att scoopet så som jag uppfattade det var regionalt och inte nationellt så som fallet oftast är i Sverige. (Naturligtvis är det en hel del skillnad i befolkningsstorlek mm mellan Japan och Sverige.)

Nästa föredrag:
”Overview of Japanese Healthcare system”

Pekar på behovet av det som vi i Sverige kallar ”Avancerad sjukvård i hemmet, ASIH” och det avgörande behovet av en fungerande koppling mellan hälso- och sjuvårdsinformation.

Berättar om ”Privacy Protection Act” från 2005 som är otillräcklig och behöver revideras. Bl a pekas på att sanktionsmöjligheterna vid överträdelse är för svaga (samma i Sverige – Datainspektionens och IOV:s sanktionsverktyg?) att endast läkare är bundna av lagen ifråga och att information om tredje man inte skyddas tillräckligt. Det pekas även här på avvägningsproblemet mellan vårdkedjans behov och skydd av information (dvs balansen mellan tillgänglighet och konfidentialitet). Pekar också på behovet av att hantera kommunikation av vårdinformation med andra länder samt särskilt på att information om individers genetiska egenskaper måste ha ett extra starkt skydd.

Sessionen avslutas

Dag 2 Tisdag
WG4

Mötet börjar med ”Roll Call”. (Noterar att Bernd Blobel är närvarande. Arbetet med ”balanced scorcard” för ISO 27799 stannade upp under våren enligt uppgift bl a på grund av att Blobel inte var tillgänglig.)

Först gås igenom vad som publicerats sedan mötet i Sydney. Därefter informeras om att det blir gemensamt möte mellan WG4 och WG7 om bl a ISO 27799 samt att det blir genomgång av ”systematic review”, dvs femårsuppdatering av ISO 27799 under onsdag eftermiddag.

Det redogörs för ett förslag om hur man ska hantera uppdateringar av standarder i fortsättningen: Minst 5 länder måste efter 5 år använda standarden, annars tas den bort. Reflektion: Hur definierar man ”använda”? Tex, i SLL baseras styrdokument för informationssäkerhet på ISO 27002 – men hur mycket måste saker och ting ”baseras på”, eller kanske ”inspireras av” eller ”vägledes av” för att anses vara ”använt”? Kanske blir det så att kontrollen av vilka som använder snarare blir en omröstning om vilka som ”gillar” en standard?

Generellt ang arbetssättet för WG4 fanns förslaget om att effektivisera och arbeta snabbare genom att öka antalet mindre arbetsmöten genom ökad användning Webex/ liknande.

Snabb omröstning om godkännande av agenda. Inga invändningar.
Snabb omröstning om att godkänna protokollet från mötet i Sydney. Liksom Tyskland och UK valde jag ”Abstain” eftersom jag inte var med i Sydney.

Därefter genomgång om vad som är ”på gång”. Det gick väldigt snabbt.

ISO/IS CD 21298 HI– Functional and structural roles
Genomgång av Tyskland (Blobel som haft en ledande roll). Sverige har röstat “Abstain” om detta tidigare så jag drog slutsatsen att detta inte var en central svensk fråga. Genomgång av kommentarer till senaste versionen av Blobels dokument. Lång diskussion bl a avseende

- Anpassning mot andra standards (UK) och utrymme för anpassningar till nationell lag vid implementation (UK).
- Kanada: Eventuell koppling till ISO 26000 och till ISO 17090 (PKI-standard), det handlar om terminologi som påverkar bl a vilka personalgrupper som ska omfattas.
- Australien: Synpunkter på begrepp såsom ”proxy”, ”agent” (ombud, utförare). Uppenbarligen en lång historisk diskurs. Relationen till HL7 fördes också på tal.
- Norge: Flera kommentarer ang terminologi (”patient” eller ”subject of care”).
- Därefter mer redaktionella ändringar.

Sessionen avslutas

Session Q2

”ISO/IS DIS 17090-4 Health informatics, -- Public key infrastructur”

Alla har röstat Ja eller Avstår sedan tidigare. Japan efterlyser ny standard för PKI (det är rätt svårt att förstå vad som sägs). Det förefaller som att mötet skjuter olika avgöranden till Berlin. Mötespunkten verkade ”ta slut” varpå diskussionen återgick till ”Functional and structural roles”. Lång diskussion.

“ISO/IS NP 16864 Health informatics, Data protection in trans-border flows of personal health information”

Detta visade sig bli ett ganska brett område som kom, eller kommer att, omfatta:
Project 16864 Merge ISO 22867, EN 14484 och EN 14485.
- Also align with ISO 27799 update
- EHR: PMAC, Roles Audit etc
- Pseudoanonymisation ISO 25237
- Patient consent
- Patient rights
- New Guidlines (patient summary mm). Det görs en referens till epSOS (fast utan namnet ”epSOS” nämns) och dess arkitektur med “Nationella kontaktpunkter” osv.

Next steps
Input kommer att efterfrågas (...hann inte skriva av allt)
“Luuc Posthuumus to circulate revised WD to the preliminary experts by 2014-07-07”. Om detta även gäller Sverige kanske vore det kanske idé att be den svenska delen av epSOS, dvs SepSOS kanske om synpunkter? Comments due by 2014-08-10. New Draft av Luuc Posthuumus 2014-08-24. Med tanke på att epSOS är ett svenskt EU-projekt kanske det är lämpligt att Sverige engagerar sig ytterligare i detta? Som synes ovan påverkas även ISO 27799. Uppfattar att detta fn inte en svensk fråga i och med att Sverige avstått vid röstning.

Det här arbetssättet (slå ihop standarder i större eller mindre utsträckning) förefaller peka på en ny trend inom ISO där det av flera skäl verkar gå mot sk metastandarder. Utvecklingen i den riktningen drivs dels av affärsmässiga skäl (mellan tex HL7 och ISO) och dels av utvecklingen med ökande komplexitet, snabbare utveckling osv. Metastandarder riktar sig mer mot UseCase/ Arketyper än standarder i den traditionella bemärkelsen där en och samma standard – där den, när den är tillämplig – ska kunna täcka in ett flertal UseCases?

Blobel nämnde epSOS, underförstått som någon slags europeisk ”lead” i ämnet, vilket förefaller som en rimlig tanke? Situationen inom EU är därmed ganska klar, enligt Blobel. Information och återkoppling från världen utanför EU är sålunda särskilt viktig.

Diskussion om ISO 17090 om PKI osv
Finns en svensk kommentar som mötesdeltagarna ställde sig lite frågande till:

”There is a mix of identity and role in the certificate”.

Sekreteraren säger - ”det var ju meningen” ungefär. Jag kan inte ta ställning då jag inte känner till bakgrunden.

Mötet beslutade att den svenska reservationen mot mixning av roll och identitet enligt ovan skulle avslås.

Rejected: 'This is included [både roll och ID alltså] specifically to support the healthcare uses of the PKI. Without this extension it would not be healthcare specifik.' Jag kunde inte argumentera för detta eftersom jag inte känner till bakgrunden. Dock var beslutet inte slutgiltigt eftersom ytterligare en remissomgång förutskickades. Istället tog vi upp detta i korridorsmöte i pauser enligt nedan:

Dag 2 Onsdag

Angående gårdagens fråga om att mixa ID med Roll i PKI Certifikat och den svenska invändningen mot detta: Tog kontakt med Mikael Wintell som ursprungligen förde fram reservationen. Mikael förklarade bakgrunden, nämligen att det kan hända att en person kan ha flera olika roller fördelade över sin arbetstid. Talade med Lori (Conveyer i WG4) om detta som sa att detta är en gammal fråga och att det andra synsättet går ut på att Rollen handlar om en yrkescertifiering tex läkarlegitimation.

Vi försökte få till en formell diskussion inom ramen för WG4 om detta, av praktiska skäl gick inte det. Istället säkrades att Conveyer för WG4 (Lori Reed-Fourquet, lfourquet@ehealthsign.com) fick kontaktinformation ang den svenska reservationen mot att blanda ID och Roll i certifikat. Vi ordnade ett korridormöte där Lori förstod att den svenska invändningen har substans. Den svenska synen på detta kommer att förmedlas per e-post så snart som möjligt.

Nästa ämne
"ISO/TS 17975 Health informatics, Principles and data -requirements for consent in the collection, use or disclosures of personal health information". Jag har ingen instruktion och ser inga svenska reservationer i "N598 ISO DTS 17975 ISO comments collated" eller ställningstaganden så jag lyssnar och noterar.

Föredragande (Elaine) går igenom nuvarande kommentarer (23 sidor, det hanns inte igenom med balanserad detaljnivå).

Det talas om att frågan om Consent inte går att behandla (Ger) därför att det är en rörlig måltavla. I kommentarerna görs hänvisningar till att nya dataskyddsdirektivet och att anpassningar måste göras mot detta (Alignment) när dataskyddsdirektivets innehåll klarnar.

Hittills verkar det (enligt Blobel, Ger) finnas enighet i Europa om att patientens samtycke ska finnas och att samtycket ska grundas på att patienten tar ett informerat beslut. Hur detta ska genomföras praktiskt, tekniskt är ännu en öppen fråga. Ett slags förslag till ramverk för detta är "HL7 Version 3 DAMMR Composite Privacy Consent Directive" men även där måste tillämpningen/ anpassning ske i relation till nationell lag.

Det talades också om hur samtycket ska dokumenteras (med eller utan digital signatur/ motsvarande). Diskussionen landade i att samtycket ska vara autentiserat – på vilket sätt samtyckets autenticitet ska uppnås är en annan fråga som inte diskuteras här).

Frågan kom upp om det bör arbetas fram en detaljerad modellbeskrivning eller inte. (Fick en direkt fråga och kunde naturligtvis inte på stående fot svara på det för svensk del – det var nog ett litet test misstänker jag. Utgår från att det är bäst att inte säga för mycket.)

Det talades också en hel del om "narrative standards" och kulturer. Frågan var om modellbeskrivningen borde uttryckas diagrammatiskt eller i text. Okänt om det finns ett svenskt

ställningstagande dels till om det bör tas fram en modellbeskrivning eller inte. Dels om en sådan i så fall bör utformas grafiskt eller i text.

I en del av dokumentet kommenteras graden av granularitet för 'Consent'. Detta sluter an till en svensk diskussion där läkarkåren i Sverige ifrågasätter rätten att spärra sådan journalinformation som innehåller förskrivna mediciner eftersom det försvårar möjligheten att ta ansvar för egna förskrivningar (om man alltså inte kan se vet vilka andra mediciner patienten redan fått förskrivna).

Dokumentet ska till en 2nd DTS "ballot" igen i Berlin. Dokumentet har varit ute i 6 veckor sedan tidigare. Det verkar som om det ska bli en formell modell som deltagaren från Australien kommer att ta fram.

Slut på sessionen

Gemensamt möte WG1 och WG4

"ISO / WD 13606-4 Health informatics, EHR Communication Part 4 – Security, Joint Meeting with WG1 D. Kalra - WG1 Lead"

Föredragande D. Kalra

Verkar egentligen handla om spärrhantering, exempel på olika kategorier, scenarier och situationer där olika typer av journaldata ska/ ska inte accessas av rätt/ fel tex personalkategori / befattningshavare. Klassning av patientdata egentligen men mycket mer granulärt än klassning enligt RKT – 1-3 eller så.

Sedan samma sak fast med logg som svarar på frågan "vem har tittat på min journal". Går längre än vad som presenterats i Sverige? Tex redogörelse (i patientens logg) för vilka filter och policys som varit inblandande när information har accessats.

Samma sak med loggen över loggacesser, dvs vem, hur, när, varför - har tittat i loggen.

Nytt

- "Purpuse of use"
- "Audit log model" (som ska svara på frågan om vem som bad om logginformation)
- ISO TS 27789 Audit trails for electronic health records
- ISO 22600 "Priveledge Managment and Acess Control" (PMAC).
  Ambitionsnivå: Att informationen ska vara läsbar för människor. Ambitionsnivån är inte att denna "access control" ska ge tillräckligt underlag för forensiska ändamål.

Sedan gick diskussionen ner i detaljer (med syfte att hitta avgränsningar).
Därefter utsågs arbetsgrupp med vad som verkar vara "de som brukar göra jobbet"?

Slut på sessionen

WG4
Eftermiddag

"EN-ISO/IS 27799 Health informatics, Information security management in health
2.8 discuss in context of 80000- series"

Historisk genomgång av tillkomst och relation till 27000-serien.

80001 – nära relation till 27799. Målet är att harmonisera dessa standarder och att undvika att samma sak dubbleras i båda standarderna. För att nå dit föreslås att vissa delar av 80001 flyttas in till 27799 därför att 27000 är så välkänd. Det uttalas tydligt att det inte är ett mål att avveckla ISO 80001.

Genomgång av uppdateringen av 27799. Ross Fraser föredragande. Inledningsvis inte så mycket om nyheter utan mera vad de olika kapitalen innehåller. Därefter diskuteras olika förslag om via olika administrativa vägar skicka vidare 27799 inom ISO.

Ett annat förslag är att det ska ske ett parallellt uppdateringsarbete av 80001 och 27799. Beslut om det förslaget hänsköts till Berlin. Inget om annexet/ balanserade styrkortet i 27799.

Därefter en lång genomgång av hur 80001 mappar mot andra standards såsom 27799, 27002 m fl. Diskussionen gled sedan över till ”framework for Reassurance”. Under diskussionens slut kom det en fråga från rysk sida om huruvida virtuella medicintekniska utrustningar omfattades. Oklart om det blev något svar på frågan.

Nästa session
ISO/TR 17791

Avvikelserapportering, incidentrapportering
AHRQ Common Formats
Detta var alltså en kort presentation av ett förslag till ett nytt ”Work Item” för ICO/TC215 att överväga.

Därefter följde en diskussion om ramverk och principer för utveckling av mjukvara. Gemensamma principer, definitioner och termer. Arbetsgruppen efterlyste återkoppling.
Björn-Eric Erlandsson deltar i arbetet.

Presentation av AHIMA.org om säker hantering av 'Copy and Paste – konsekvenser för hälso- och sjukvårdsinformation'. AHIMA undrade om WG4 var intresserat av detta. Inga större reaktioner. Intrycket var att flera ansåg att greppet var lite smalt.

Dag 3 Torsdag
WG4

Uppdateringen av 27799
Ross Fraser föredragande av läget (videolänk)

Task Groupe Update
Genomgång av Revision Rules

”Essention requirements should not be over-empathised by Shall”. Detta uppfattar jag som ett inlägg i diskussionen om hur pass normativt 27799 bör uttrycka sig. Fn verkar åsikten vara att det något mjukare ”should”/ ”bör” ska användas snarare än ”Shall”/ ”skall”.

Rikard Lövström tackades för arbetet med Annexet / balanserade styrkortet.

Frågan om BYOD kom upp

Blobel: 'Mobila device och BOYD = nya problem'

Fraser: Nya idéer inom gruppen i mars sedan månad.
Fraser: Det finns idéer i gruppens dokument om detta.
Bloobel: 'detta håller på att bli en het fråga i flera länder'

Därpå följde diskussion om tidsplanering mm, när det ska ske ”ballots”.
Försökte skriva av men det gick för fort

Resolution ang PWI 27799 – Submit CD for Ballot
Instructs PL to provide CD-text to WG4 Convenor senast 2014-05-23
Instructs WG4 secretary to post on WG4 Comitty for a three week review no later than 2014-05-25
…
Secreterare submittar till TC215 senast 2014-06-30
TC 215 sekretary launch 2 månads CD ballot senast 2014-07-21

Rimligen publiceras tidplan på ISO eller så får vi be om det.
Noterar att det talades om att korta ner tiden för ”review”.

Mötet övergick till att titta på kommentarer ang Systematic review 2011. Uppfattade att tre länder vid den tiden skickat in kommentarer: Kanada, Nederländerna och Australien och att kommentarerna i allmänhet var av redaktionell natur.

Summa summarum:

- Genomgång av historik och läge, vad som gjorts, vad som återstår
- Enda kommentaren under mötet: Blobels oro för BYOD som Fraser hävdade redan tagits upp, kommenteras och kläckts idéer ikring i Mars då Blobel inte var med.
- Administrativa beslut om tidplaner osv inför Berlin

Ross Fraser: Det behövs förmodligen en till telefonkonferens innan Berlin, reaktion på Ballots och liknande.

Tillbaka till ”Next step” osv

Ross Fraser efterfrågade expertis/ erfarenhet av att skicka patientdata skickas över internet, alltså erfarenhet av vad som behövs ur säkerhetsperspektiv (eventuellt hade Australien information om detta). Reflektion: Möjligen har Sverige något att tillföra eftersom det numera i Sverige förekommer att patienter tar del av sin journalinformation över internet? Alternativt den svenska användningen av röntgenläkare på andra sidan jordklotet?

Det efterfrågades även hjälp avseende ”Assessment of and decision on information security events”. Incidenthantering. Erfarenhet av rapportering kring problem med privacyläckage och liknande. Den tyske delegaten sa att han eventuellt kunde få fram någon erfarenhet kring detta.

”Availability”, Ross Fraser frågade om det finns något specifikt att säga om detta mer än det uppenbara. (Förmodligen efterfrågas policys, riktlinjer och utredningar?)

(Ganska långt och intressant samtal med Blobel i pausen. Avstamp i BOYD-problemet och landning i senare tids skriverier om Edward Snowden mm.)

Nästa session WG4

Health informatics — Components of education to ensure health information privacy

Genomgång av dokument (missade början)

Dokumentet mest orienterat mot Asien?

Släpper detta dels därför att det sägs vara mest utanför EU
Dels därför att, som det påpekas i diskussionen, det blir så detaljerat att det förmodligen krockar med alla möjliga lagar i olika länder. Avvakta och se om detta växer till sig?

WG4 Q3

Genomgång av
WG4 N624 ISO CD 21549-5 Patient Healthcare - Identification Comments and answers Functions

Först avseende patientidentitet
ISO/IS 21549-5 HI – Patient healthcard data – Part 5: Identification data. Därefter avseende medicinsk patientdata på kort. ISO/IS 21549-7 HI – Patient healthcard data – Part 7: Medication data. (N/A då vi i Sverige såvitt känt är inte har patientdata på kort?)

WG4 Q4

Mer diskussion om funktionella och strukturella roller.

Slut

Respektive land har ett eget möte där röstningsförfarande stäms av.
Därefter slutmöte med röstning.

Redogörelse för svenska röstförfarandet finns i annan reserapport. ”Mötesanteckningar Kariuzawa mw.pdf” utskickad av Lena Morgan (SIS) den 26 maj 2014 10:23.

Övergripande intryck:
Inom WG4 förefaller det vara en ganska begränsad krets som driver på arbetet. Det verkar också finnas mer eller mindre starka personligheter som tenderar att styra diskussionen – även om Convenor är med på noterna. Sålunda har Tyskland ett starkt inflytande tillsammans med Australien och USA. Mycket handlar förmodligen också om hur länge man suttit med, med den trygghet i gruppen som det ger. En hel del delegater är tämligen tysta. Det kan naturligtvis också ha med uppbackning hemifrån att göra. Det talas informellt om industrins inflytande. Även om funderingen är lätt att följa synes inget sådant, i alla fall inte med de ovana ögon.

Anteckning av
Anders Egnell