Magisteruppsats
Datavetenskap
Uppsats nr: MCS-2003:24
Oktober 2003

Kravspecifikation för Informationssäkerhetsarbete till Hälso- och Sjukvårdssystem

IMIS – en fallstudie

Christina Olsson
Malin Almström

Institutionen för
Programvaruteknik och Datavetenskap
Blekinge Tekniska Högskola
Box 520
372 25 Ronneby
Sweden

Denna uppsats är inlämnad till Institutionen för Programvaruteknik och Datavetenskap på Blekinge Tekniska Högskola som en deluppgift för magisterexamen i Datavetenskap. Uppsatsen är ekvivalent med 20 veckors heltidsstudier.

Kontaktinformation:
Författare: Christina Olsson
Adress: Hökamåla skola, 370 30 Rödeby
E-mail: christina.f.olsson@swipnet.se

Författare: Malin Almström
Adress: Ronnebygatan 47, 371 33 Karlskrona
E-mail: malin.almstrom@karlskrona.net

Handledare BTH:
Guohua Bai
Institutionen för Programvaruteknik och Datavetenskap

Institutionen för
Programvaruteknik och Datavetenskap
Blekinge Tekniska Högskola
Box 520
372 25 Ronneby
Sweden

Internet : www.bth.se/ipd
Tele : +46 457 385 000
Fax : + 46 457 271 25

ABSTRACT

During 2001-2002 a prototype, IMIS (Integrated Mobile Information System) was developed at BTH (Blekinge University of Technology) to demonstrate how mobile IT-systems can be used in healthcare. The prototype was based on the activity theory of Engeström.

An ongoing project started in spring 2003. The purpose of the project is further development of IMIS with special focus in the diabetes healthcare. Participants in the project are scientists and students at BTH, ALMI Företagspartner, Blekinge FoU-enhet, Barndiabetesförbundet Blekinge, Blekinge Diabetesförening, Vårdcentralen Ronneby and Vårdcentralen Sölvesborg.

The goal of IMIS is to develop a secure communication platform, which follows requirements from caretaker and caregiver as well as the Swedish laws regulating digital information and healthcare.

The output of this master thesis is a requirement specification of information security for healthcare where IMIS has been used as a case study. The requirements specification follows the international standard SS-ISO/IEC 17799.

Nyckelord:
Informationssäkerhet
Hälso- och sjukvårdssystem
IMIS (Integrated Mobile Information System)
Diabetesvård

Innehållsförteckning

1 INLEDNING

1.1 Bakgrund

E-Health är en stor utmaning för dagens samhälle. Den stora utmaningen innebär att utveckla säkra informationssystem som kommer att underlätta och effektivisera framtidens hälso- och sjukvård. Mycket forskning pågår inom eHealth i USA [26] och i Europa [24].

Diabetessjukvården i Blekinge försöker hitta nya lösningar som ska underlätta och förbättra den nödvändiga kommunikationen mellan patienter och diabetessköterskor. Detta arbete har pågått under några år. Bland annat så har det genomförts en undersökning som visar att sjukdomen diabetes kommer att öka så mycket så det kommer att behövas teknisk hjälp för att vårdbehovet ska kunna tillgodoses i framtiden [29]. Nu startar ett samarbete mellan Blekinge FoU-enhet, BTH (Blekinge Tekniska Högskola), Hjort & Partner, diabetessköterskor och diabetespatienter. Samarbetet ska resultera i utvecklandet av en kommunikationsplattform som ska förenkla samarbetet mellan diabetespatienter och diabetessköterskor.

På BTH har tidigare utvecklats en kommunikationsplattform som kallas IMIS (Integrated Mobile Information System), den ska nu anpassas till diabetesvården, diabetespatienters och diabetessköterskors behov. IMIS baseras på Engeströms Aktivitetsteori [3].

Säkerhet i informationssystem är bara en del av informationssäkerhet. Information finns både inuti och omkring en dator och den ska skyddas på vilket sätt den än transporteras. Den totala säkerheten är aldrig bättre än den svagaste länken i informationens väg. Information är en affärstillgång i en organisation och för att den ska bibehålla sitt värde måste den skyddas på följande sätt [11], [13]:

Sekretess – säkerställande av att informationen är tillgänglig endast för dem som är behöriga att ta del av och använda den.

Riktighet – skydd av informationen så att den är och förblir korrekt och fullständig.

Tillgänglighet – säkerställande av att användarna har tillgång till informationen när den behövs.

Ytterligare en viktig egenskap är spårbarhet som innebär möjligheten att i efterhand identifiera genomförda händelser.

Ett annat sätt att ange hur information ska skyddas är genom *confidentiality, integrity* och *availability* (CIA) [4].

Carelink är en organisation som grundades år 2000 av Landstingsförbundet, Kommunförbundet, Privatvårdens Arbetsgivarförbund och Apoteket AB. Syftet med Carelink är att utveckla IT-stödet för den svenska hälso- och sjukvården. Ett önskvärt mål är att digital kommunikation mellan olika parter ska underlättas. Ett väldigt viktig område när det gäller denna typ av kommunikation är informationssäkerheten. Den största delen av information som behandlas inom hälso- och sjukvård behöver skyddas, den kan vara sekretessbelagd utav lagar och det är av avgörande betydelse att den inte kan förvanskas. Det är även viktigt att den alltid är tillgänglig. I det arbete som bedrivs inom Carelink angående informationssäkerhet används den internationella standarden SS-ISO/IEC 17799, Ledningssystem för Informationssäkerhet, som bas.

1.2 Syfte

Arbetet ska resultera i en kravspecifikation för informationssäkerhetsarbete till hälso- och sjukvårdssystem. IMIS används i detta arbete som en fallstudie för att illustrera hur en kravspecifikation för informationssäkerhet kan tas fram. Den ska ses som en första del i informationssäkerhetsarbetet omkring IMIS. Under den fortsatta

testen och utvecklingen av IMIS är det meningen att denna kravspecifikation ska följa med och utvecklas jämsides med den tekniska delen av kommunikationsplattformen.

1.3 Hypotes

Genom att följa standarden SS-ISO/IEC 17799 och TIHS (Tillämpningsråd för Informationssäkerhetsarbete inom Hälso- och Sjukvård) under utvecklingsarbetet av hälso- och sjukvårdsystem, ökar sannolikheten för att en kravspecifikation för informationssäkerhetsarbete som innefattar tekniska, sociala och juridiska aspekter kommer att utformas.

1.4 Avgränsning

Undersökning av vad som kan anses vara en tillfredsställande informationssäkerhet utifrån rekommendationer för hälso- och sjukvård (TIHS, SS-ISO/IEC 17799, SITHS (Säker IT inom Hälso- och Sjukvård)), kommer att presenteras i denna rapport. Den kommer också att innehålla förslag på tillvägagångssätt för att uppnå nämnda säkerhet.

Om våra förslag till informationssäkerhetsarbete, som sammanställs som en kravspecifikation i kapitel 10, ska vara relevanta för informationssystem inom hälso- och sjukvård, är det nödvändigt att utvecklingen av informationssäkerhet är en integrerad del i systemutvecklingen.

1.5 Intervjuer och intervjupersoner

Under detta arbete har olika intervjuer genomförts. Resultatet av intervjuerna redovisas i slutet av de kapitel där de är relevanta.

Intervjuundersökning, Typ A, genomfördes med användare (patienter och sköterskor) som ska använda och testa IMIS. Patienter med diabetes valdes ut med hjälp av Barndiabetesförbundet och Blekinge Diabetesförening. Vid urvalet togs hänsyn till att det fanns med representanter från olika åldersgrupper och även föräldrar till barn med diabetes. Vi intervjuade även personer som tillhör olika primärvårdsområden och som tillhör Blekingesjukhuset. Avsikten med intervjuerna Typ A var att ta reda på användares uppfattning om hur hög säkerhet de önskar för att de ska känna sig trygga med att använda IMIS. I samband med intervjuerna beskrevs autentisering enligt SITHS-modellen och eID-kort [kap 6] samt informationsklassificering enligt TIHS-modellen [kap 7]. Frågeformulär redovisas i Appendix 1.

Intervjuundersökning, Typ B, genomfördes med personer som arbetar praktiskt med frågor som är relevanta för arbetet. Val av intervjupersoner till Typ B gjordes utefter vilka arbetsuppgifter de har och i vilka organisationer de arbetar. Syftet med intervjuer Typ B var att komplettera och praktiskt förankra litteraturstudierna. Frågeformulär redovisas i Appendix 2.

1.5.1 Presentation av intervjupersoner i Typ A

Intervjuer genomfördes med tio diabetespatienter och två diabetessköterskor, de presenteras inte vid namn.

1.5.2 Presentation av intervjupersoner i Typ B

Thomas Pehrsson är IT-chef på landstinget Blekinge. Han blev utsedd att svara på några frågor angående landstingets informationssäkerhetsarbete i framtiden. Det finns ingen säkerhetschef på landstinget och dessutom har författarna samarbetat med Pehrsson tidigare, därför föll valet på honom. Eftersom IMIS kommer att användas inom ramen för landstingets verksamhet är det viktigt att veta något om tankarna med landstingets fortsatta säkerhetsarbete.

Intervjun gick till så att tre frågor sändes via mail till Pehrsson. I Appendix 2 finns de frågor han ombads att besvara.

Kjell Allestedt valdes som intervjuperson därför att han är informationssäkerhetsansvarig på Carelink. Vi har till stor del i detta arbete följt rekommendationer från Carelink och tagit del av deras forskning. På de grunderna ansågs att Allestedt kan ge viktiga svar på tankar med Carelinks arbete. Intervjun genomfördes på så sätt att ett formulär skickades via mail, svaren kompletterades och förtydligades därefter i en telefonintervju. I Appendix 2 återges formuläret.

Britt Lagerlund är informationssäkerhetsansvarig för Region Skåne. Under intervjun med Kjell Allestedt framkom att Region Skåne genomför ett pilotprojekt som går ut på att testa en typ av certifikathantering framtagen av Carelink. På rekommendation av Allestedt kontaktade vi därför Britt Lagerlund för ytterligare information angående arbetet med certifikaten.

Johan Förander undervisar i kursen IT-juridik på BTH och kontaktades i egenskap av jurist för att förankra frågeställningar angående lagar och förordningar som berör arbetet.

Lars-Åke Pettersson är informations- och IT-säkerhetschef samt personuppgiftsombud i landstinget Östergötland. Utöver ansvarsområdena inom landstinget är Lars-Åke Pettersson ordförande för ett nätverk som hanterar informationssäkerhet inom vård och omsorg. Han är också inblandad i Carelinks arbete på olika sätt. Lars-Åke Pettersson kontaktades på rekommendation av Kjell Allestedt bland annat för att reda ut begrepp kring lagar och förordningar.

2 IMIS-PROJEKTET

Kapitel två ger information om hur IMIS-projektet startade och tanken med dess utveckling. Informationen i detta kapitel är till för att läsaren ska få grundläggande förståelse för IMIS-projektet och för vad som ligger bakom fallstudien av IMIS.

2.1 Introduktion

Under 2001-2002 utvecklades en prototyp, IMIS (Integrated Mobile Information System), på BTH för att demonstrera hur mobila IT-system kan användas inom hälso- och sjukvård. Prototypen baseras på Engeströms aktivitetsteori [3] som bygger på följande struktur:

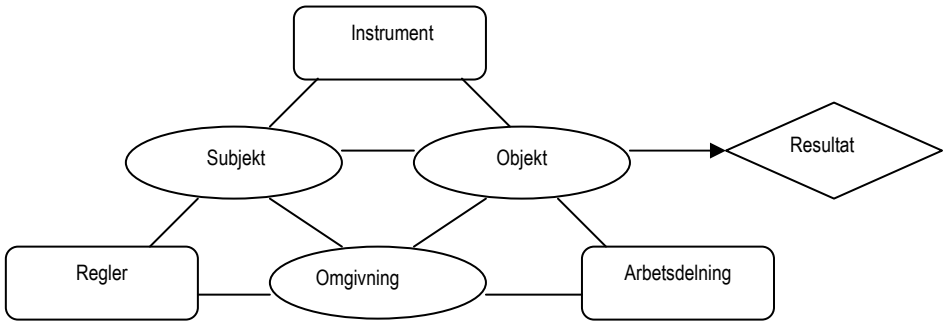

Bild 1: Engeströms aktivitetsteori.

Under våren 2003 ägde ett seminarium rum på BTH. Projektansvarig och företaget Hjort & Partner informerade om tanken med IMIS och diskuterade kring IMIS-projektets framtid. Syftet med seminariet var att diskutera kring en vidareutveckling av IMIS och anpassa denna till diabetesvården och på så sätt uppnå en förbättrad kommunikation mellan vårdtagare och vårdgivare. De som deltog på seminariet var forskare och studenter från BTH, ALMI Företagspartner, Blekinge FoU-enhet, Barndiabetesförbundet Blekinge, Blekinge Diabetesförening och diabetessköterskor från vårdcentralen i Ronneby och Sölvesborg.

Inför vidareutvecklingen av IMIS fanns önskemål om att undersöka faktorer inom informationssäkerhet samt juridiska aspekter aktuella för IMIS. I detta skede skapades idén till detta magisterarbete.

2.2 Syfte

IMIS har två syften, dels att ge diabetespatienter tillgång till en mobil kommunikationsplattform för att underlätta deras nödvändiga kommunikation med sina vårdgivare, dels att ge vårdgivare inom diabetesvården tillgång till samma mobila kommunikationsplattform för att underlätta deras situation och kommunikation med vårdtagare.

Meningen är att både vårdgivare och vårdtagare ska ha tillgång till samma system, access ska tillåtas utefter användare, patient, läkare, sköterska eller annan. Tillgång till systemets funktioner ska regleras efter vilken typ av användare som sökt access. IMIS ska kunna vara både stationär och mobil.

2.3 Mål

Målet med IMIS är att utveckla en internetbaserad kommunikationsplattform för diabetespatienter och diabetessköterskor för att därmed kunna öka livskvaliteten för diabetespatienter och förbättra arbetssituationen för vårdgivare inom diabetesvården.

2.4 Förväntat resultat

Tidigare studier inom IT och diabetesvård visar att en gemensam kommunikationsplattform mellan vårdtagare och vårdgivare skulle öka kvalitet, säkerhet, integritet och tillförlitlighet i en patients liv [30]. En effektiv minskning av kostnader skulle också kunna bli möjlig eftersom kommunikation via IMIS kan ersätta vissa besök. Det är också möjligt att ge instruktioner för behandling via IMIS och därmed minska antalet besök hos vårdgivare.

2.5 Framtida utveckling

Egenvård är betydelsefull för att förbättra diabetespatienters livskvalitet, en enkel och pålitlig kommunikation med vårdgivare förhöjer egenvårdens kvalitet [30]. Diabetesvården är därför ett passande område att påbörja utveckling och testning av idén med en gemensam kommunikationsplattform. Eftersom IMIS bygger på aktivitetsteorin är strukturen, enligt upphovsmannen till IMIS-projektet, anpassad för alla områden inom hälso- och sjukvården men även för organisationer som kommuner och privata sjukvårdsföretag. Tanken med IMIS är att det i framtiden ska leda till en internationell kommunikationsplattform för hälso- och sjukvård [30].

3 GENERELL SÄKERHETSMODELL

Kapitel tre visar hur det går att dela in informationssäkerhetsarbete i olika komponenter. Efter en introduktion följer en kort redovisning för varje komponent. Modellen ska ses som en grund för att läsaren ska inse hur många specialiteter som faktiskt berörs i ett informationssäkerhetsarbete och vilket omfattande arbete det är att dels formulera säkerhetskrav, dels att uppnå dem. Som avslutning på kapitlet redovisas författarnas kommentarer.

3.1 Introduktion

Det är svårt att uppnå tillfredställande informationssäkerhet i nätverk och system. Svårigheten ligger mycket i det faktum att olika människor har olika uppfattning, det som uppfattas helsäkert för en person kan kännas mycket osäkert för en annan [9]. Det är viktigt att var medveten om att full säkerhet aldrig kan uppnås. Det är alltid en kompromiss mellan säkerhetskrav eller önskningar, systemkrav och tillgängliga resurser. Fortfarande saknas det inom informationsteknik den typen av säkerhetsbegrepp som till exempel finns i bilindustrin, där vet den som köper en Volvo vilken säkerhet som medföljer.

Det är många aspekter att ta hänsyn till när det gäller att uppnå säkra system och nätverk. Först och främst måste det finnas en policy som definierar de mål som ska uppnås med säkerhetsarbetet. För att uppnå den säkerhet som policyn föreskriver, finns det sedan olika komponenter att ta hänsyn till. Komponenterna säker arbetsstation, nätverkssäkerhet, organisationssäkerhet och informationssäkerhet måste undersökas och utvärderas enligt gällande säkerhetspolicy.

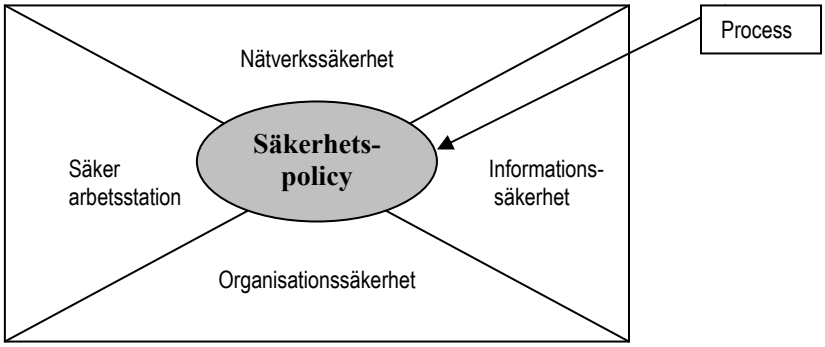

Bild 2: Säkerhetsmodell som bygger på modell i Oppliger 1999 [9].

3.2 Säkerhetspolicy

En säkerhetspolicy ska specificera de mål som ska uppnås angående säkerhet i nätverk och system. Om det inte finns en sådan policy går det inte att bedriva säkerhetsarbete eftersom det måste framgå hur målen ser ut. En säkerhetspolicy ska vara skriven utefter de säkerhetskrav som finns och inte hur de skall uppnås [9].

Arbetet och underhåll kring en säkerhetspolicy ska ses som en itererande process som alltid ska vara aktiv i en verksamhet och se till att policyn följs.

3.2.1 Säker arbetsstation

Identifiering av användaren är en viktig del av arbetsstationens säkerhet. En säker identifiering anses möjlig genom att kombinera någon typ av certifikat med lösenord. Enligt säkerhetsansvarig på Carelink, Kjell Allestedt, är det den enda acceptabla lösningen för svensk hälso- och sjukvård.

Access till ett system kan ges enligt olika modeller, exempel på en modell i olika nivåer är Bell la Padula [1]. Det finns också modeller som är horisontella, till exempel

BMA-modellen som används inom sjukvård i England [1]. Ofta används en kombination av vertikal och horisontell modell.

När det gäller att lagra och bearbeta data kommer design av mjukvara som en viktig del i säkerhetsarbetet [14]. För att uppnå god säkerhet ska säkerhetsexperter vara delaktiga i systemutvecklingen ända från analys till underhåll och vidareutveckling [7].

Rutiner för säkerhetskopiering är en del som inte får glömmas bort, det är enkelt och billigt och det är en mycket god försäkring mot diverse problem som kan uppstå i arbetsstationen.

För att arbetsstationen ska vara säker gäller också att den senaste tekniken vad det gäller antivirusprogram och brandväggar ska finnas installerad.

3.2.2 Nätverkssäkerhet

Med nätverkssäkerhet menas att access till nätverket ska regleras och att data som transporteras ska vara insyns- och integritetsskyddad. Insyns och integritetsskydd innebär att informationen inte kan ses av obehörig och ingen inkräktare kan komma åt att ändra viktiga data, inte heller ska data försvinna under transport över nätet. För att åstadkomma detta finns flera tekniker till hjälp [1], [9]:

- Brandväggar
- Olika typer av protokoll
- Proxy server
- Olika typer av kryptering
- Olika tekniker för transport av data, t ex kretsförmedling och paketfiltrering

3.2.3 Organisationssäkerhet

Mänskligt beteende är den mest betydelsefulla faktorn i allt säkerhetsarbete. Det hjälper inte att ha utmärkta säkerhetsrutiner och bästa tänkbara tekniska säkerhet om inte de som handskas med informationen förstår varför det finns. Om de inte till fullo förstår betydelsen så kommer de att kringgå dem [9], [15]. Beteendet kan påverkas av utbildning, säkerhetskontroller, säkerhetsrutiner och kunskap om vilka lagar som styr aktuell verksamhet. Dessa faktorer medvetandegör vikten av att upprätthålla en god säkerhet. Den informerar också om varför vissa rutiner ska utföras och vilken teknisk hjälp som finns för att upprätthålla säkerhet. Säkerhetskontroller gör att det blir krångligare att utföra otillåtna procedurer, rutiner hjälper till att hålla reda på de rätta arbetsmomenten [9]. Ett exempel som kan belysa detta är att för att få lov att köra bil måste föraren ha körkort, bilen som körs måste vara besiktigad och gällande trafikregler ska följas. Det finns en del att lära av hur säkerhet hanteras i verkliga livet.

3.2.4 Informationssäkerhet

Informationssäkerhet innebär att information som skickas i ett system ska hanteras säkert hela vägen mellan sändare och mottagare [4].

3.3 Författarnas kommentarer

Vi tycker att detta kapitel ger en första uppfattning om de stora komponenter som ingår i säkerhetsarbete. Varje del måste brytas ner i flera delar för att det ska vara möjligt att planera och utföra informationssäkerhetsarbetet i den praktiska verkligheten. Det är viktigt att förstå att den som satsar på säkerhet i endast någon av delarna kommer att misslyckas. Säkerhet är en helhet och måste alltid behandlas som en sådan.

Med exempel från andra tillfällen i livet blir säkerhetstankarna mer förnuftiga och det känns inte alls överdrivet att sträva mot god säkerhet även om det kostar resurser. Det kommer förmodligen att behövas ytterligare mognad hos organisationer för att till fullo inse att informationssäkerhet är lika viktig som säkerhet inom alla andra branscher.

4 JURIDIK OCH LAGAR

Kapitel fyra behandlar generellt vad som gäller för området juridik inom informationssäkerhet samt speciellt vad som gäller för lagar och säkerhetskrav i en vårdprocess. I slutet av kapitlet redovisas författarnas kommentarer.

4.1 Juridik inom informationssäkerhet

Internationellt är lagstiftning inom informationssäkerhet ett högt prioriterat område. Inom G8 och EU pågår för närvarande arbete inom området.

I ett informationssäkerhetsarbete ska juridiska faktorer tas i beaktande. Lagar och förordningar kan styra informationshantering inom olika branscher, vilka är viktiga att känna till. Det juridiska arbetet inom informationssäkerhet bör därför konsulteras med jurister som är kunniga inom det område som är aktuellt för ett projekt eller organisation [7], [18].

4.2 Lagar och säkerhetskrav i en vårdprocess

Hälso- och sjukvård är ett stort och komplext område som innefattar att många lagar och förordningar följs. Lagar som berör informationshantering inom hälso- och sjukvård är; Hälso- och sjukvårdslagen, Patientjournallagen, Lag om hälsodataregister, Lag om vårdregister, Sekretesslagen, Personuppgiftslagen, Lag om yrkesverksamhet inom hälso- och sjukvårdens område och arkivlagen.

Nedanstående sammanställning beskriver de säkerhetskrav som finns på informationssäkerhet i en vårdprocess. Vissa delar av säkerhetskraven återfinns i lagarna som gäller för informationshantering i hälso- och sjukvård och resterande delar är framtagna av Carelink [22].

Säkerhetskrav:

- Patienten ska vara säkert identifierad och tilldelas en unik identitet.
- Hälso- och sjukvårdspersonal ska vara säkert identifierad och tilldelas en unik identitet.
- Patienten ska ha möjlighet till inflytande på hur informationen görs tillgänglig.
- Patientens inflytande ska kunna dokumenteras.
- Tillgång till information/behörighetstilldelning ska baseras på behov, vårdrelation, vårdgivarens roll i verksamheten och patientens samtycke.
- Det ska vara möjligt att vidimera att någon tagit del av en information.
- Informationen ska kunna överföras till arkiv när beslut om detta fattas.
- Läsning av information ska loggas och inkludera loggning av hur informationen har presenterats.

Vid dokumentation ska:

- patienten ha möjlighet till inflytande över hur dokumentationen ska göras tillgänglig.
- information godkännas och signeras av den som ansvarar för innehållet.
- information kunna contrasigneras av den som har övergripande ansvar.
- information kunna versionshanteras.
- alla ändringar ska synas och all tidigare text ska kunna visas i sitt sammanhang.
- alla aktiviteter som gjorts i systemet kunna spåras/loggas.

Vid informationsspridning ska följande beaktas:

- **Tillgänglighet**
  - Information ska kunna spridas med rimliga åtkomsttider och säkerställa att information når mottagaren inom önskad/förväntad tid.

    - Göra mottagaren medveten om att information har anlänt.
    - Göra avsändaren medveten om något skulle gå snett.
    - Säkerställa att information inte förloras.
    - Reservrutiner ska vara väl dokumenterade.
    - Säkerställa att information inte förloras.
    - Reservrutiner ska vara väl dokumenterade.
- **Förändringsskydd**
    - En garanti att information inte har förändrats avsiktligt eller oavsiktligt ska finnas.
    - Garantin ska gälla hela kedjan, d v s från ursprung till slutanvändare och får inte brytas på något ställe.
- **Insynsskydd**
    - Information ska vara skyddad mot obehörig åtkomst/läsning
    - Endast avsedda/behöriga mottagare ska kunna nå/se informationen.
- **Spårbarhet**
    - Informationens ursprung ska kunna garanteras
    - En händelse ska kunna knytas till en person
    - Varken sändande eller mottagande ska kunna förnekas
    - Avsändaren ska få bekräftelse på att mottagaren nåtts av informationen
    - Loggning av all ”skickad” och ”mottagen” information inkl. spridningsinformation ska ske.
- **Strukturerat arbetssätt**
    - Ett strukturerat arbetssätt innebär att spridningsfunktionen är väl dokumenterad och att dokumentationen följs. Bland annat ska det finnas en dokumentation över den tekniska lösningen och överenskommelser mellan parter med kontaktpersoner och klart uttalade ansvarsgränser.

4.3 Intervjuer som berör juridik

Intervjuerna med Lars-Åke Pettersson och Johan Förander har förankrat, att de lagar vi har tagit upp i detta kapitel och i kapitel 10, kravspecifikationen, är relevanta för arbetet.

Resultatet av intervjun med Johan Förander visade att området hälso- och sjukvård är mycket komplext och innefattar många lagar och förordningar. Han arbetar dock inte med hälso- och sjukvårdsjuridik och kan därför inte uttala sig vidare men påpekade omfattningen av området.

Lars-Åke Pettersson föreslog ett utökande av relevanta lagar med Socialtjänstlagen och Tryckfrihetsförordningen.

4.4 Författarnas kommentarer

Eftersom området hälso- och sjukvård är så pass omfattande rekommenderar vi att jurister involveras i IMIS-projektet på ett tidigt stadium. Detta tycker vi krävs för att området är så pass viktigt, både ur vårdtagares och ur vårdgivares synpunkt. Det får inte förekomma några som helst frågetecken gällande de lagar som berör informationssystem inom hälso- och sjukvård. Om några delar av lagar och förordningar åsidosätts, kan systemanvändare bli lagbrytare.

Listan på säkerhetskrav framtagen av Carelink uppfattar vi som en omfattande beskrivning av vilka krav som gäller för en vårdprocess. Vi tycker att listan ska tas i beaktande vid utvecklingen av IMIS likaväl som juridiska fakta.

Synpunkten från Lars-Åke Pettersson om att lägga till Socialtjänstlagen och Tryckfrihetsförordningen har vi i dagsläget inte tagit hänsyn till då vår kunskap inte har räckt till för att undersöka huruvida de berör IMIS-projektet.

Socialtjänstlagens och Tryckfrihetsförordningens inverkan på IMIS-projektet, bör utredas vid vidareutveckling.

5 DET MÄNSKLIGA HOTET INOM INFORMATIONSSÄKERHET

Kapitel fem tar upp hur informationssäkerhet påverkas av det mänskliga ledet och hur risker som utgörs av den mänskliga faktorn kan minskas. Som avslutning redovisas författarnas kommentarer.

5.1 Mänskliga faktorn

Den mänskliga faktorn är många gånger orsaken till att fel uppstår i eller omkring datasystem [2]. Känslig data kan spridas och komma i orätta händer. Påkostade tekniska verktyg används för att skydda känsliga uppgifter i en verksamhet men detta är oftast inte tillräckligt. Det mänskliga ledet är en mycket svag punkt när det gäller informationssäkerhet. För att minska riskerna som den mänskliga faktorn medför krävs strikta rutiner, regler, utbildning och motivation inom området informationssäkerhet [2], [8].

Undersökningar visar att två tredjedelar av de största ekonomiska skadorna i en verksamhet orsakas av anställda eller personal i dess närhet [2]. Resultatet från dessa undersökningar visar även att 50 procent av informationsförluster i företag beror på felaktig hantering av information och utrustning.

Rutiner och riktlinjer för hur anställda och användare ska agera för att skydda information är viktiga för att bygga upp en säker organisation. En viktig punkt i säkerhetsarbete är att man inte kan få en total säkerhet utan målet med säkerhetsarbete, som nämnts tidigare, är att minska säkerhetsrisker till en acceptabel nivå [7], [10].

Den generella användaren inom en organisation har ofta inget dolt syfte att komma åt och sprida otillbörlig information. Om detta trots allt sker beror det ofta på okunskap och oförsiktighet. En organisation kan däremot innehålla användare som utnyttjar sin position inom organisationen för att nå och sprida känslig information. Svårigheten är att kontrollera vilka som är vilka och sätta in rätt åtgärder.

Det finns olika typer av inkräktare till ett datasystem och det är inte förrän man vet vilken typ av inkräktare man har att göra med som man kan skydda sig mot den. Inkräktare kan benämnas antingen som *interna* eller *externa* [11].

Intern inkräktare är en person som har anknytning till eller till och med arbetar inom en organisation. Problemet med interna inkräktare är att de redan är inne i organisationen och känner till rutiner och regler. Dessa åstadkommer därför oftast fler och större skador genom sina attacker [11].

Externa inkräktare är de som inte har någon tidigare relation till en organisation utan har av andra anledningar blivit intresserade av en organisation. En extern inkräktare har inte samma fördelar som en intern men har däremot ofta mer kunskaper och erfarenhet av intrång och attacker.

Inkräktare kan drivas av ekonomiska, sociala, politiska eller personliga motiv och använder olika metoder för att nå dit de vill. Vissa får tillgång till information rent fysiskt genom att besöka målet i fråga, andra använder tekniken som hjälp och sist men inte minst finns det människor som helt enkelt använder sina sociala färdigheter.

5.2 Se upp för sociala manipulatörer

Boken *Bedrägerihandboken* är skriven av en före detta IT-brottsling, Kevin Mitnick. I sin bok tar Mitnick upp mängder med kryphål för att på olika sätt komma åt säkrad information. Han kallar personer, som har en benägenhet att lura och utnyttja människor till att lämna ut obehörig data till främlingar, för sociala manipulatörer. En social manipulatör röjer inga hinder för att komma åt det han/hon vill ha. Dessa människor finns överallt i samhället och bör därför beaktas som en säkerhetsrisk, speciellt i IT-sammanhang [8].

Vanligt förekommande är att intrång görs med hjälp av telefonen som verktyg. Den sociala manipulatören ringer upp aktuellt objekt och uppger sig för att vara någon annan och kommer med hjälp av listiga kommentarer åt information via den person som svarar. Att lämna ut information som kan tyckas vara oskyldig kan resultera i stora skador. Ett anställningsnummer eller kanske något så enkelt som ett efternamn kan vara en del i den sociala manipulatörens plan för att kunna gå vidare till nästa steg att nå otillbörlig information.

En social manipulatör följer ofta ett visst mönster för att nå sitt mål [11]:

- Väljer ut mål att attackera
- Hitta en ursäkt att kontakta och utnyttja valt mål
- Motiverar offret genom att spela på offrets moral, och självkänsla eller genom att tillfredställa behov som lust och hämnd.

5.3 Användarutbildning inom informationssäkerhet

För att skydda sig själv och den verksamhet man arbetar inom mot sociala manipulatörer gäller det att vara medveten om att de finns men även känna till hur de utför sina handlingar. För att öka medvetenheten hos personal när det gäller informationssäkerhet och sociala faktorer behöver information spridas och personal utbildas om hur man ska hantera en social manipulatör. Enligt Mitnick kan angrepp minskas drastiskt om utsatt person alltid har följande steg i åtanke:

- Bekräfta identiteten på den person som framställer en begäran för att försäkra sig om att personen verkligen är den han/hon utger sig för att vara.
- Bekräfta personens behörighet för att försäkra sig om att han/hon verkligen har behörighet för aktuell begäran.

Utbildning inom informationssäkerhet är ett måste för att höja medvetenheten hos den generelle användaren men även för de personer som arbetar med informationssäkerhet för att kunna hålla en hög säkerhetsstandard.

Mitnick tar upp ett antal punkter med inriktning mot mänskligt beteende och social manipulation. Dessa bör beaktas när ett säkerhetsprogram ska utvecklas, vilket bör innehålla följande:

- Beskrivning på hur en angripare använder social manipulation för att lura andra människor
- Metoder som en social manipulatör använder sig av
- Beskrivning på hur en attack som utförs av en social manipulatör upptäcks
- Rutiner för hur en misstänkt förfrågan ska hanteras
- Rutiner för hur försök till attacker och attacker ska rapporteras
- Beskriva det faktum att man inte utan ifrågasättande ska lita på andra människor trots att det oftast känns mest riktigt att göra motsatsen
- Beskriva betydelsen av att verifiera identitet och behörighet för en person som begär information eller liknande
- Rutiner för att skydda känslig information
- Förklaring av säkerhetsföreskrifters betydelse och var dessa kan hittas
- En sammanfattning av viktiga säkerhetsföreskrifter och vad de innebär för den anställde ska få förståelse och anpassa sitt agerande därefter. T ex att den anställde utbildas i hur man skapar och hanterar ett lösenord säkert.
- Beskriva varje anställds skyldighet att hålla sig till säkerhetsföreskrifterna och dess konsekvenser om inte dessa följs

Ett råd som Mitnick ger är att inte låta anställda få tillgång till datorsystemen innan genomgången säkerhetsutbildning. En utbildning för att höja medvetenheten hos anställda/användare är att sätta upp klara och tydliga rutiner för vad som gäller i olika situationer. Följande punkter ska eftersträvas och täckas in i ett säkerhetsprogram för

att uppnå en högre medvetenhet gällande informationssäkerhet bland anställda och användare:

- Säkerhetsföreskrifter som gäller lösenord för datorer och röstbrevlådor
- Procedurer för att lämna ut känsligt informations eller material
- Säkerhetsföreskrifter och rutiner för användning av e-post och röstbrevlådor
- Skyddsåtgärder för att förhindra angrepp som virus, maskar och trojanska hästar
- Fysiska åtgärder som att bära ID-kort och
- Ansvar för att ifrågasätta personer på en arbetsplats som inte bär ID-kort
- Hur man ska avgöra hur information ska klassificeras och vidta försiktighetsåtgärder för att skydda känslig information
- Rätta metoder för att kassera känsliga dokument och datamedia som innehåller, eller vid någon tidpunkt har innehållit, konfidentiellt material

En viktig aspekt i säkerhetsarbete är att utbildning och information angående säkerhetsfaktorer och hanterande hela tiden är pågående. Det krävs kontinuitet för att människor inte ska falla in i gamla vanor utan ständigt påminnas, utmanas och uppmuntras för att upprätthålla en god säkerhetsstandard [8]. Risken för social manipulation ökar med dagens teknik då ständigt fler och mer komplicerade tekniska hjälpmedel utvecklas för att förhindra intrång. Dagens snabba utveckling kräver en större medvetenhet hos människor överlag.

5.4 Författarnas kommentarer

Att informera användare om informationssäkerhet och hot som det mänskliga ledet i informationshantering innebär, tycker vi är en enkel och billig metod för att minska säkerhetsrisker.

För att öka medvetenheten hos användare, krävs det att alla i en organisation eller ett projekt får vara delaktiga i informationssäkerhetsarbetet. På så sätt ökar förståelsen, för det ansvar som åligger var och en, för strävan mot att uppnå en tillfredställande informationssäkerhetsnivå.

Vi tror att, involverandet av användare i informationssäkerhetsarbetet är en förutsättning för att arbetet ska lyckas. Bristande förståelse för regler och rutiner omkring informationssäkerhetsarbetet försämrar säkerheten radikalt.

Betydelsen av att utbilda personal och användare i informationssäkerhet är ständigt återkommande i litteratur om informationssäkerhet. Vi har noterat, att de människor vi har mött under vårt arbete, har relativt lågt säkerhetsmedvetande. Kunskapsnivån inom informationssäkerhet måste höjas för att hotet från det mänskliga ledet ska minska i system som används inom hälso- och sjukvård.

Vi instämmer i Mitnicks förslag om att låta utbilda användare i informationssäkerhet innan tillgång till systemet ges. Vårt förslag är att vårdtagare och vårdgivare som kommer att använda IMIS får genomgå en utbildning i informationssäkerhet som tar upp grunder inom informationssäkerhet och vad som är speciellt viktigt att tänka på vid användandet av IMIS [kap 10.6.2].

6 SITHS-MODELLEN OCH CERTIFIKATHANTERING

Kapitel sex innehåller information om SITHS-modellen som tagits fram av Carelink. I kapitlet sammanställs även information om en certifikatmodell som garantera en säker inloggning och möjligheten till elektronisk signering. Ett underkapitel redovisar intervjusvar samt författarnas kommentarer.

6.1 Grundläggande funktioner inom informationssäkerhet

Carelink är en organisation som bedriver informationssäkerhetsarbete inom vård och omsorg för att säkra informationshantering mellan olika enheter. SITHS, *Säker IT inom Hälso- och Sjukvård,* är ett arbete som Carelink har bedrivit sedan ett par år tillbaka. SITHS är nu till viss del i drift. Målet för SITHS är att utveckla modeller och metoder för hur de grundläggande funktionerna i informationssäkerhet ska kunna realiseras i det IT-stöd för hälso- och sjukvård som finns idag [19].

De grundläggande funktionerna är:

- *Autenticering*; Kontroll av uppgiven identitet.
- *Behörighetstilldelning*; Fastställande av åtkomsträttigheter.
- *Sekretess eller konfidentialitet;* Skydd av information mot otillbörlig insyn.
- *Integritet*; Skydd av information mot oönskad förändring, påverkan eller insyn.
- *Oavvislighet*; Skydd mot att avsändare eller mottagare av information i efterhand kan förneka åtgärd eller kännedom om åtgärd.

Begreppet *autenticering* innebär att en person ska bevisa sin identitet för att få tillgång till ett system som är låst för obehöriga. Autenticering kan ske på tre sätt, genom:

1. Något man HAR (t.ex. säkerhetsdosa)
2. Något man VET (t.ex. PIN-kod)
3. Något man ÄR (t.ex. fingeravtryck, röstigenkänning)

6.2 Certifikathantering enligt SITHS-modellen

SITHS-modellen bygger på att anställda i vård och omsorg har ett personligt elektroniskt ID-kort (eID-kort). Det elektroniska ID-kortet kan förses med ett särskilt anställningscertifikat som anger på vilken arbetsplats en person är anställd på och vilken yrkestitel personen har. Med detta ID-kort kan en säker identifiering ske i olika datasystem. Certifikaten ger möjlighet att signera en handling digitalt vilket motsvarar en vanlig namnteckning [17].

SITHS-modellen kan göra följande punkter möjliga:

- Säker e-post med identifikation av avsändare
- Säker E-handel med digitalt signerade dokument
- SSO (Singel Sign On)
- Digitalt signerade recept, journalhandlingar m.m.
- Säkra överföringar av medicinsk information

När personal inom hälso- och sjukvård ska få elektroniska ID-kort utfärdade ska Carelink fungera som certifikatutgivare.

6.2.1 PKI – Teknisk lösning för elektronisk signering

SITHS-modellen bygger på PKI (Public Key Infrastructure). PKI är den dominerande krypteringsmetod som skapar system för identifiering och kontroll av kryptering och integritet. PKI innebär att data/information krypteras med ett nyckelpar,

en publik och en privat nyckel. Data som man vill ska skickas säkert över en förbindelse krypteras med en privat nyckel som sedan endast kan dekrypteras med motsvarande nyckel. Syftet är att data som skickats krypterat inte ska kunna läsas av någon annan än den som har exakt rätt privata nyckel för att dekryptera data/information.

En privat nyckel används främst för digitala signaturer och för att dekryptera tidigare krypterad information. En publik nyckel används främst för att verifiera digitala signaturer samt för att kryptera data/information. Den publika nyckeln kan ges ut till en grupp personer som ska ha möjlighet att dekryptera och kryptera meddelande inom den specifika gruppen.

PKI möjliggör även elektronisk signering. Syftet med elektronisk signering är att den ska fungera på samma sätt som en vanlig signatur. Endast en person ska kunna utföra den medan andra kan ta del av signerad information. Grundstenarna för elektronisk signering är [5]:

- *Identifiering*; Används för att visa vem som är mottagare respektive sändare
- *Signering*; Används för att ge ett dokument laglig status genom elektronisk signatur
- *Kryptering*; Används för att göra information säker

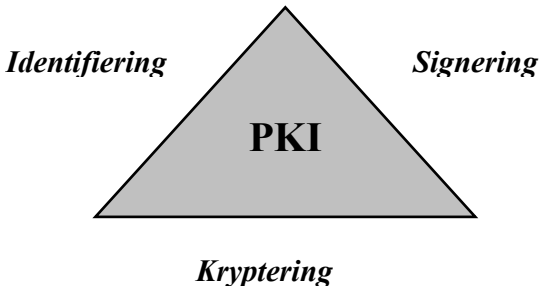

Bild 3: Grundstenarna för PKI

I en PKI ingår funktioner som certifiering, verifiering och revokering (återtagande av certifikat).

SITHS-modellen bygger på utgivning av certifikat via en CA. En certifiering ska utföras av en CA, Certificate Authority, till exempel Posten eller Telia. En CA skall vara en betrodd part som ett stort antal användare litar på [5] Vid en certifikatutgivning ska en tillförlitlig tredje part kunna:

- Garantera att identifiering av den person som certifikatutgivningen gäller stämmer.
- Garantera att uppgifter om identifierad person stämmer.
- Garantera att den privata nyckel som innehas av aktuell personen stämmer överens med den publika nyckel som innehas av CA:n.

När detta är kontrollerat signerar CA:n uppgifterna i certifikatet med sin privata nyckel och går därmed i god för att uppgifterna stämmer [21]. En CA ska sedan ansvara för utfärdandet av publika nycklar och för själva det elektroniska ID-kortet under dess livstid.

SITHS-modellen har enligt följande bild fyra ”ben” som gör att den står stadigt [21]:

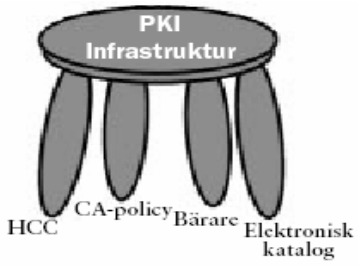

Bild 4: PKI-pallen, hörnpelarna i SITHS-modellen [21]

- HCC – Beskrivning över hur certifikat för hälso- och sjukvård ska se ut.
- CA-Policy – Regelverk över hur certifikat ska utfärdas, framställas, spärras m.m.
- Elektronisk katalog – En katalog som lagrar alla certifikat som är tillgänglig för användare samt där uppgifter om spärrade certifikat kan hämtas.
- Bärare – Ett koncept för hur användare säkert ska förvara och använda sina privata nycklar med hjälp av en kryptografisk modul t ex ett smart kort.

6.2.2 Pilotprojekt inom Region Skåne

Inom Region Skåne har Postens eID-kort och Carelinks certifikat används sedan två år tillbaka. Syftet med detta arbete har varit att få säkerhetstjänster som autenticering, insynsskydd och säker signering. From 1/7 2003 gäller följande praktiska rutiner inom Region Skåne, enligt Britt Lagerlund, informationssäkerhetschef Region Skåne:

En person är RA, Registration Authority för Region Skåne. RA är den person som ansvarar för certifikaten lokalt. En RA:s arbete styrs enligt en RA-policy. I större organisationer finns även en ORA, Organisation Registration Authority, som utser de personer som praktiskt ska ge ut certifikaten, LRA, Local Registration Authority.

För att en person ska få ett certifikat utfärdat måste vederbörande, i detta fall, vara upplagd i Skånekatalogen med tillräckligt djup. Detta innebär att det måste finnas information om var personen arbetar och att han/hon måste vara personligt närvarande vid första certifiaktutfärdandet. LRA:n och den person som ska ha certifikatet utfärdat, kontrollerar att uppgifterna i katalogen stämmer. Uppgifterna ligger sedan som grund för beställning av HC-certifikat som läggs på eID-kortet.

EID-kortet innehåller certifikat som identifierar kortinnehavaren i den elektroniska världen. Med HC-certifikatet blir personen knuten till organisationen Region Skåne och dess specifika arbetsplats. Yrkestitel förs även in i certifikatet, vilka är hämtade från LYHS, Lag om Yrkesverksamhet inom Hälso- och Sjukvård [kap 10.6.9]

Den första juli i år startades ett nytt system för hantering av SITHS hälso- och sjukvårdscertifikat i Region Skåne. Utbildning skedde under junimånad och trots några inkörningsproblem med nya rutiner fungerar hanteringen av certifikat bra, enligt Britt Lagerlund.

Under hösten 2003 kommer certifikat att användas för inloggning till arbetsplaster i ett projekt som kallas ”Klinisk”. Detta omfattar läkemedelslista, vårdöversikt och för säker e-mail.

6.3 Intervjuer som berör SITHS-modellen

Enligt Kjell Allestedt, informationssäkerhetsansvarig på Carelink, behövs elektroniska signaturer för att människor i framtiden kunna umgås tillitsfullt på nätet. Allestedt anser att pappershantering som istället görs elektroniskt kommer att förkorta ledtider. Det kommer att ge högre kvalitet då till exempel inte något papper kan hamna i en låda och bli bortglömt. En pappershantering som med vanlig postgång tar en vecka kan vara klar på några timmar. Elektroniska signaturer sparar, enligt Allestedt, tid och pengar och ger högre kvalitet.

Enligt Thomas Pehrsson, IT-chef på landstinget Blekinge, är de välförtrogna med SITHS-modellen. De kommer att införa certifikat enligt SITHS men de kommer att invänta resultatet från pilotprojektet i Skåne. Landstinget Blekinge, liksom alla Sveriges landsting, har skrivit på en avsiktsförklaring som innebär att när frågan blir aktuell så kommer SITHS att införas, vilket innebär att ingen konkurrerande lösning skall tas fram.

Resultatet av intervjuundersökningar Typ A visade att majoriteten anser att metoden att använda certifikat och lösenord som inloggning är säker. Intervjupersonerna kan därmed mycket väl tänka sig att använda sig av metoden och dessutom känna sig säker i hantering av känslig information. En synpunkt som framkom under intervjuundersökningen var att vissa dock alltid kommer att ta extra känslig information öga mot öga med läkare eller sköterska.

6.4 Författarnas kommentarer

Anledningen att ta upp SITHS-modellen hör ihop med att alla Sveriges landsting har skrivit på en avsiktsförklaring att så småningom införa SITHS. Vi anser att IMIS ska vara förberett för SITHS för att kunna motsvara landstingets kommande krav och därmed kunna ligga steget före i utvecklingen.

SITHS-modellen bygger på PKI, vilket idag ses som den säkraste metoden för autenticering. Med hjälp av SITHS-modellen kan följande uppnås; autenticering, behörighetstilldelning, sekretess, integritet och oavvislighet. Alla komponenter, anser vi, är väsentliga för att IMIS ska bli en seriös produkt för hälso- och sjukvård.

7 TIHS SOM METOD FÖR ATT FÖLJA SS-ISO/IEC 17799

Kapitel sju presenterar tillämpningsråd från ett arbete publicerat av Carelink. Arbetet heter TIHS (Tillämpningsråd för Informationssäkerhetsarbete inom Hälso- och Sjukvård) [18]. Syftet med TIHS är att ge råd hur SS-ISO/IEC 17799 kan tillämpas i informationssäkerhetsarbete. TIHS kommer att användas i kravspecifikationen för IMIS och presenteras i detta kapitel. Som avslutning på kapitlet redovisas intervjuer som berör TIHS samt författarnas kommentarer.

7.1 Bakgrund och syfte med TIHS

SWEDAC (Styrelsen för ackreditering och teknisk kontroll), Stockholms läns landsting, Sahlgrenska Universitetssjukhuset, Norrlands Universitetssjukhus m.fl. har inlett ett samarbete med Carelink för att ta fram en metod att använda för informationssäkerhetsarbete. Avsikten med en arbetsmetod är att den kan användas av laboratorier som vill ha sitt informationssäkerhetsarbete godkänt av Swedac. Metoden som kallas TIHS (Tillämpningsråd för Informationssäkerhetsarbete inom Hälso- och Sjukvården) är också lämplig som stöd för övrigt informationssäkerhetsarbete inom hälso- och sjukvård.

Dokumentet som sammanfattas i detta kapitel [18] riktar sig till alla personer som kan tänkas styra eller medverka i informationssäkerhetsarbete.

Syftet med skriften, förutom att vägleda informationssäkerhetsarbetet för verksamheter som önskar bli ackrediterade, är att vara en generell vägledning för informationssäkerhetsarbete inom hälso- och sjukvården. Verksamhet som styrs mot liknande arbetsmetoder ger ett effektivare säkerhetsarbete och en bättre förutsättning för erfarenhetsutbyte. TIHS bygger på att ledning och informationsägare samarbetar i att tillfredsställa behovet av att ta fram säkra rutiner och tekniska lösningar för sin verksamhet. För att få till stånd ett bra informationssäkerhetsarbete krävs det att inblandade parter, som ledning och chefer, är beredda att investera i föreslagna lösningar. TIHS är inte menat att ge normer för informationssäkerhetsarbete, det innehåller inget ställningstagande om vad som kan vara ”rätt” lösning, tanken är istället att ge råd för att möjliggöra utveckling mot ett strukturerat och trovärdigt arbetssätt. Slutligt ansvar för riskhantering och åtgärder ligger hos ledning och informationsägare vid varje enhet och landsting.

7.2 Generella förutsättningar för informationssäkerhetsarbete

Informationssäkerhetsarbete som bedrivs via successiva förbättringar i små steg når ett bättre resultat än plötsliga införande av manuella rutiner eller tekniska lösningar. Med detta sätt att se på arbetet blir det en process som alltid ska vara aktiv inom en verksamhet. I processen ingår också att policys och riktlinjer successivt förbättras. Ett strukturerat och trovärdigt arbetssätt för informationssäkerhet skapas innan eller parallellt med utveckling av tekniska säkerhetslösningar. För att uppnå resultat av arbetet krävs att verksamhet och ledning avsätter resurser. Bild 6 visar hur processen för informationssäkerhetsarbete ser ut.

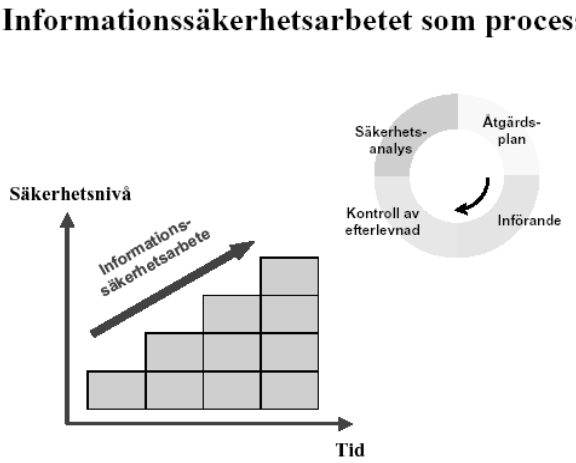

Bild 5: Informationssäkerhetsarbetet som process [18, figur 2]

Säkra helhetslösningar kan som regel uppnås om den totala tjänsten ses som en kedja av manuella och datoriserade rutiner. Manuella fel kan snabbt mångfaldigas via datorprogram utan att det märks för användaren. En riskfaktor är gränssnitten mellan manuella och tekniska rutiner. Ett sätt att hantera denna riskfaktor kan vara att minska de manuella momenten.

Det måste finnas intresse och engagemang från högsta ledningen för att informationssäkerhetsarbetet ska bli framgångsrikt. Mål ska sättas upp för arbetet och ledning och informationsägare ska ansvara för att de nås. Om det bedrivs ett strukturerat arbete och ledningen får adekvat information om hur arbetet bedrivs, kan ledningen få kontroll över det arbete som den ansvarar för.

Enligt TIHS ska de finnas representanter från så väl verksamhet som säkerhet under ett informationssäkerhetsarbete. Stöd kan också behövas från personer med kompetens från juridik, kvalitet och IT. För ett effektivt arbete önskas dessutom en metod- och modelleringsledare.

7.3 TIHS – Huvuddelar

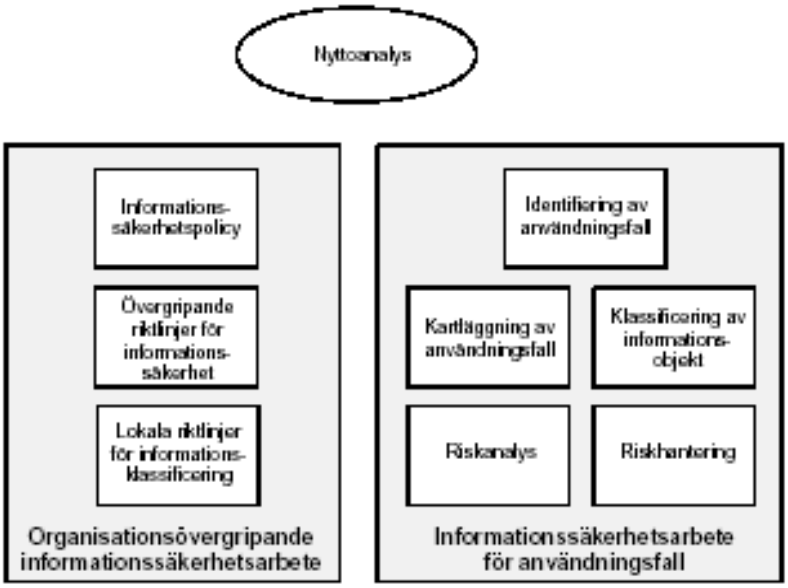

Bild 6: De delar av SS-ISO/IEC 17799 som innefattas i TIHS [18, figur 7]

7.3.1 Nyttoanalys av informationssäkerhetsarbete

Nyttoanalysens syfte

Nyttoanalysen har som mål att skapa en förståelse för att informationssäkerhet runt ett utvecklingsprojekt är nödvändigt. Ledningen för projektet ska uppmärksammas på vilken nytta ett sådant arbete gör. Det innebär konkret att belysa vilka behov det finns för att säkerställa att inte användande av systemet ska drabbas av oförutsedda händelser. Händelser som kan resultera i kvalitetsbrister, lagöverträdelser eller att patienter kommer till skada på något sätt. Genomförande och resultat ska dokumenteras noggrant. Dokumenten ligger till grund för vilka resurser som ska avsättas för informationssäkerhetsarbete.

Faktorer att undersöka i nyttoanalysen

I TIHS rekommenderas att följande faktorer undersöks för att få kontroll på om det finns brister eller osäkerhet omkring dem.

- Överensstämmelse med lagar och förordningar
- Kommersiella villkor, konkurrens
- Felbehandling på grund av felaktigt provsvar
- Röjande av känslig patientinformation
- Risk för dålig publicitet vid fel
- Godkännande

7.3.2 Informationssäkerhetspolicy

Bilden visar i vilket hierarkiskt förhållande policy, riktlinjer, anvisningar och instruktioner står till varandra.

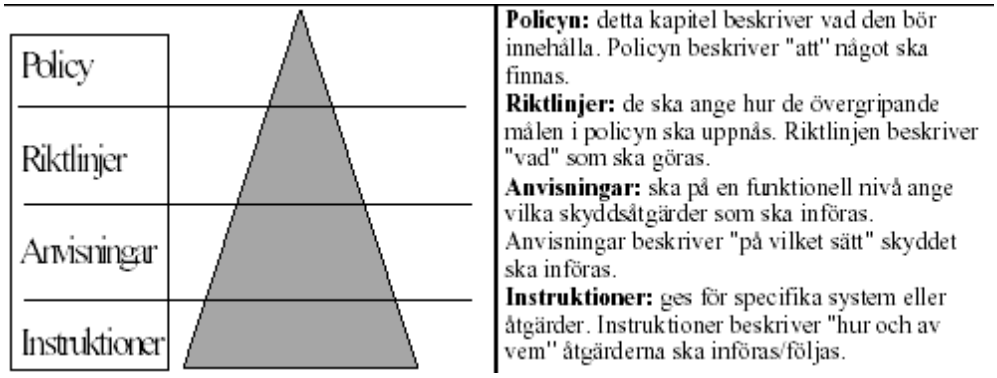

Bild 7: Hierarkiskt förhållande [13, sid 3-3]

Syfte med informationssäkerhetspolicy

Grundläggande innehåll i en informationssäkerhetspolicy visar *vad* organisationen menar med informationssäkerhet vilka *mål* som finns och vilken *omfattning* den har. Det ska klart och tydligt framgå vem som ansvarar för informationssäkerhet och för incidentrapportering. Ledningen ska ha godkänt policyn och det bör finnas en utsedd ägare som ska svara för dess underhåll.

Syftet med en informationssäkerhetspolicy är att ge ledningens viljeinriktning och stöd för informationssäkerhet [13]. Samtidigt visar policyn ledningens engagemang för informationssäkerhet och gör inblandad personal medveten om säkerhetens betydelse.

Vad innehåller en informationssäkerhetspolicy

Det finns ett stort antal frågor som ska besvaras av policyn [13]. Därav kan nämnas:

- Vad är det som ska skyddas?
- På vilken nivå ska skyddet vara?
- Vilka rättigheter och skyldigheter har medarbetarna?
- Hur ska incidenter hanteras?
- Var gäller policyn?

En informationssäkerhetspolicy växer fram stegvis och sker med påverkan från aktuell verksamhet. Det är ofta verksamhetens säkerhetsfunktion som dokumenterar policyn och på så sätt ger underlag för ledningens beslut. Policyn utgör ett centralt dokument som bildar grund för övergripande och detaljerade säkerhetsmål [13].

Underhåll

Fastställd policy ska hållas aktuell och ses över. Vid översyn undersöks bland annat:

- Policyns användbarhet utifrån aktuella incidenter
- Informationssäkerhetsarbetets kostnad och påverkan på verksamhetens effektivitet
- Eventuell inverkan på policyn utifrån tekniska förändringar

Policyns betydelse inom hälso- och sjukvård

Inom hälso- och sjukvård är det angeläget att det finns ett förtroende mellan de parter som utbyter, mestadels sekretessbelagd, information. Ett sätt att skapa detta förtroende är ett fast underlag såsom en policy [23].

7.3.3 Övergripande riktlinjer för informationssäkerhet

En informationssäkerhetspolicy talar om *vilka mål* som ska uppnås. *Hur* det ska gå till att uppnå dessa regleras främst i riktlinjer. Det kan behövas även anvisningar och instruktioner och då följer deras inbördes ordning bild 7 i kapitel 7.3.2.

En övergripande riskanalys [kap 9] bör göras för att undersöka om policyns mål är verksamhetsanpassade. Utefter resultatet av riskanalysen, erfarenheter och incidenter görs riktlinjer upp. På detta sätt erhålls riktlinjer som är anpassade till den specifika verksamheten. Efter att den specifika verksamhetens behov undersökts är det lämpligt att jämföra med exempel på riktlinjer från SS-ISO/IEC 17799 [13]:

- Säkerhetsansvar och säkerhetsorganisation
- Säkerhetsplan
- Incidenthantering
- Risk och sårbarhetsanalys
- Information och utbildning
- Systemförvaltning
- Ändringshantering

7.3.4 Lokala riktlinjer för informationsklassificering

TIHS riktlinjer för informationsklassificering finns beskrivna i tabellen nedan.

Klass	Insynsskydd	Spårbarhet	Tillgänglighet	Riktighet
1	Ej känslig information	Spårbarhet ej viktigt för informationsobjekt	Låga krav på tillgänglighet för informationsobjekt	Låga krav på riktighet för informationsobjekt
2	Känsligt informationsobjekt	Spårbarhet skall finnas på informationsobjekt	Höga krav på tillgänglighet för informationsobjekt	Höga krav på riktighet för informationsobjekt
3	Hög känslighet på informationsobjekt	Spårbarhet med mycket hög tillförlitlighet	Mycket höga krav på tillgänglighet för informationsobjekt	Mycket höga krav på riktighet för informationsobjekt
4	Mycket hög känslighet på informationsobjekt			

Bild 8: Tabell över möjliga riktlinjer för informationsklassificering [18, figur 9]

Insynsskydd (definition enligt SS-ISO/IEC 17799)
– Säkerställande av att information är tillgänglig endast för dem som har behörighet för åtkomst.

Spårbarhet (definition enligt STG/TK 99 N110)
– Möjligheten att i efterhand identifiera genomförda händelser.

Tillgänglighet (definition enligt SS-ISO/IEC 17799)
– Säkerställande av att behöriga användare vid behov har tillgång till information och tillhörande tillgångar.

Riktighet (definition enligt SS-ISO/IEC 17799)
– Skydd av information och behandlingsmetoder så att de förblir korrekta och fullständiga.

Lokala riktlinjer ska utarbetas för att definiera den speciella verksamhetens prioritetsbehov. Det går inte att direkt överföra en viss verksamhets klassificering till en annan då samma klass kan definieras på olika sätt i olika verksamheter.

Anledning till att göra informationsklassificering

Information som skapas, hanteras eller lagras är en av verksamhetens mest betydelsefulla tillgångar. Det är avgörande för verksamhetens effektivitet och trovärdighet, att hålla hög nivå på informationens tillgänglighet, sekretess och riktighet [13].

För att kunna bedriva ett effektivt informationssäkerhetsarbete måste kunskapen om informationstillgångar vara uppdaterad och korrekt. Informationen ska klassificeras för att det ska vara möjligt att ange prioritet och skyddsnivå. Klassificering utgör nödvändigt underlag för informationssäkerhetsarbete, riskhantering och övriga beslut som rör informationstillgångarna [13].

Målet för klassificeringen är ”Att säkerställa att informationstillgångar får en lämplig skyddsnivå” [13, sid 5-1].

Utformning av klassificeringssystem

Ett klassificeringssystem är mer effektivt om det är enkelt och antalet klasser bör vara fastställt från början. Riktlinjer för klassificeringen bör vara utformade så att klassificeringen omprövas med jämna mellanrum för att undvika kostsam överklassificering [13].

Klassificeringsprocessen

När de lokala riktlinjerna tas fram så startar det med definition av de olika klasserna som ska användas vid klassificeringen. Vid det arbetet bedöms de olika faktorerna sekretess, riktighet, tillgänglighet och spårbarhet. För varje faktor ska definieras vilka säkerhetskrav som gäller för varje klass. Dessa övergripande riktlinjer ska godkännas av ledningen. I pilotprojektet från Akademiska Sjukhuset finns tydligt angivet hur framgång nås i det arbetet.

> ”Det är också en tydlig framgångsfaktor att de personer som är ansvariga för informationen diskuterar skyddsbehov utifrån det område där man har sin profession, t.ex. den kliniska verksamheten. Att få verksamhetsföreträdare att med utgångspunkt i diskussioner om tekniska resurser (t.ex. nätverksprodukter eller programvara) diskutera skyddsbehov är en mindre framkomlig väg enligt pilotprojektet. Detta kan kanske anses som en självklarhet, men det är troligen ganska vanligt att riskanalyser och liknande moment görs av säkerhetsavdelningar eller IT-avdelningar av och för tekniker.” [23, sid 16].

De övergripande riktlinjerna som fastställts används sedan för att klassificera varje informationsobjekt i de användningsfall som kommer att analyseras.

7.3.5 Identifiering av användningsfall

Anledning till att utgå från användningsfall är att det sätter fokus mot information och inte enbart mot IT [18], [23], [kap 10.5]. Det säkrar att hela kedjan av handlingar ska få tillräcklig säkerhet. Möjlighet ges till att prioritera det mest angelägna

användningsfallen så att det viktigaste säkras först. I användningsfallen kan också göras en prioritering om det är tekniska eller manuella rutiner som ska åtgärdas först.

7.3.6 Kartläggning av användningsfall

Syftet med följande steg i informationssäkerhetsarbetet är att kartlägga nuläget. Alla steg i kartläggningen ska göras för varje användningsfall och ska dokumenteras. Kartläggningen kräver deltagare med kunskap från både verksamhet och teknik.

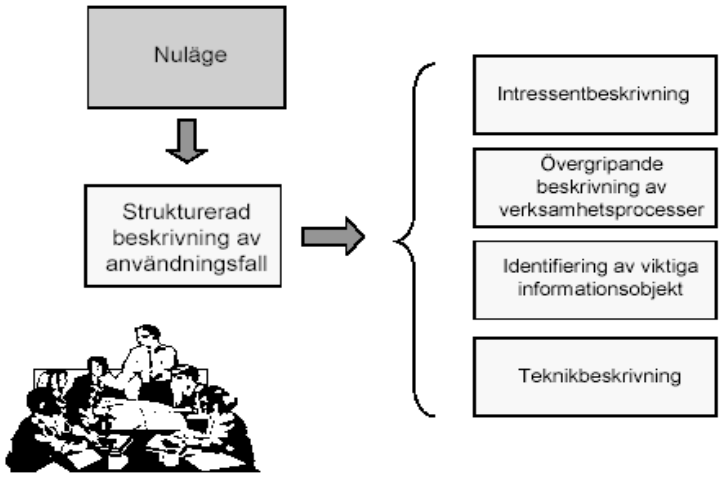

Bild 9: Kartläggning av användningsfall [18, figur 12]

Intressentbeskrivning

Syftet är att identifiera och dokumentera de intressenter som involveras i användningsfallet.

Övergripande beskrivning av verksamhetsprocessen

Syftet är att identifiera och beskriva på övergripande nivå såväl manuella rutiner som teknik ur ett verksamhetsperspektiv. Denna dokumentation utgör underlag för riskanalys och riskhantering.

Identifiering av viktiga informationsobjekt

Två viktiga delar i informationssäkerhetsarbete är själva informationen samt dess känslighet. Identifiering och dokumentering av informationsobjekt är därför grundläggande moment i säkerhetsarbetet.

Teknikbeskrivning

Beskrivning ur ett tekniskt perspektiv ska göras för varje användningsfall. Beskrivningen ska innehålla information om system, nät, utrustning o.s.v. som berör informationsutbytet. Tekniken ska bedömas utifrån delarna i klassificeringstabellen; insynsskydd, riktighet, tillgänglighet och spårbarhet.

7.3.7 Klassificering av informationsobjekt

Klassificering av informationsobjekt ska genomföras utifrån lokala riktlinjer för informationsklassificering. Ansvarig för arbetet med att klassificera objekt är den person som är utsedd till ägare av aktuell informationen eller ställföreträdande ägare. Personuppgiftsansvarig i en organisation är ytterst ansvarig för informationssäkerhet. Medverkan i informationssäkerhetsarbetet av informationsägaren eller representant för ägaren är viktig. Om den sker från för hög verksamhetsnivå kan det innebära brist på tid att engagera sig i arbetet. Medverkan på för låg nivå kan i sin tur innebära att klassificeringen ändras av person på högre nivå. Användaren/kunden ska också deltaga i klassificeringsarbetet.

Att klassificera skydd innebär att tekniska komponenter i ett användningsfall ska klassificeras enligt insynsskydd, spårbarhet, tillgänglighet och riktighet. Nivån på

skyddet ska bedömas utifrån de lokala riktlinjerna för informationsklassificering. Underlaget som tas fram under klassificering av skydd ska användas för att stämma av mot den information som ingår i användningsfallet och dess klass. Detta i sin tur blir sedan underlag till riskanalyssteget.

7.3.8 Riskanalys

Syfte, mål och genomförande av en riskanalys, tas upp i arbetet kapitel 9 därför tas här endast upp det som är speciellt för TIHS och IMIS.

Följs tillämpningsråden i THIS ges ett enkelt och effektivt underlag för genomförande av steget riskanalys. När stegen kartläggning och klassificering av användningsfall är genomförda ska en riskanalys utföras. Riskanalysprocessen ska resultera i en riskanalysrapport.

7.3.9 Riskhantering

Riskhantering ska göras i de användningsfall där det är hög sannolikhet att risken inträffar och konsekvensen av den ger ett högt utslag i riskanalysen [23]. Riskanalysrapporten ska ligga till grund för den handlingsplan som ska tas fram under riskhanteringen.

Stöd via policy och riktlinjer

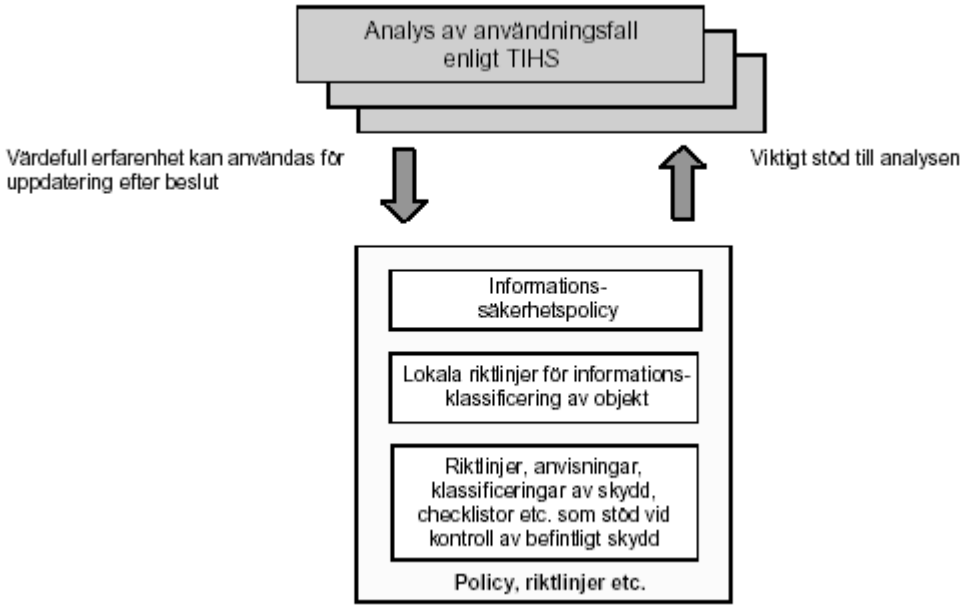

Bild 10: Stöd via policy, riktlinjer e t c [18, figur 20]

Bedömning av risker

För ett användningsfall sker en kontroll mot existerande underlag som kan vara informationssäkerhetspolicy, riktlinjer, anvisningar eller checklistor. Om de finns tillräckligt med underlag av bra kvalitet och på en detaljerad nivå så är det möjligt att bedöma om befintligt skydd är tillräckligt. Om skyddet inte är tillräcklig så krävs det riskhanteringsåtgärder.

7.3.10 Riskhantering

Riskhantering innebär att ifrån resultatet av riskanalysen eliminera, reducera, överföra eller acceptera de risker som behandlats i analyssteget. Med ledningens medverkan och med tillgängliga resurser i beaktande, ska beslut tas till hur riskerna ska hanteras. Resultatet sammanställs i en handlingsplan som ska följas för att realisera resultatet av riskanalysarbetet. Åtgärdsförslag formuleras med hänsyn till befintlig policys och riktlinjer, dokumenterade tekniklösningar och tidigare förslag på riskhantering. Arbetet med riskanalys och riskhantering bör ske iterativt.

Den handlingsplan som tas fram ska innehålla aktiviteter, tidsplan och finansieringsplan. Planen kan delas in i tre delar (Citat TIHS sid. 29).

- Åtgärder som organisationen själv kan vidta, såsom förändringar av manuella rutiner, utbildning eller lokala tekniska lösningar.
- Åtgärder som avser övergripande säkerhetsinfrastruktur som organisationen inte själv kan eller bör besluta om.
- Systemleverantörernas tillämpningar som kan behöva förändras.

7.3.11 Förvaltning av informationssäkerheten

Policy, riktlinjer, klassificerade objekt, kartlagt nuläge mm måste hållas aktuella om säkerhetsarbetet ska vara av god kvalitet. Det kan ske via löpande översyn i gång om året. Det bör också göras vid speciella händelser såsom nya användningsfall, förändringar i organisationen eller införande av nytt IT-system.

7.4 Intervjuer som berör TIHS

Enligt Kjell Allestedt, informationssäkerhetsansvarig på Carelink, är TIHS baserad på standarden SS-ISO/IEC 17799, vilken i de flesta sammanhang anses vara att rekommendera. Eftersom TIHS förespråkar att så många som möjligt ska följa liknande modell, för att befrämja vidareutveckling och förbättring av modellen, ställdes frågan om TIHS kommer att bli en standard inom hälso- och sjukvård. Svaret på det är att varje landsting är självstyrande så är det de själva som bestämmer om de vill implementera standarden. Hittills är de inte många organisationer som certifierat sig enligt SS-ISO/IEC 17799. Allestedt känner inte till om det finns rekommendationer från socialstyrelsen att vårdgivare ska följa vissa modeller och metoder vid informationssäkerhetsarbete.

IT-chefen inom landstinget Blekinge, Thomas Pehrsson, uppger att han inte har någon kännedom om vad THIS är för något. I och med det så finns i nuläget inga planer på att implementera TIHS.

Resultatet av intervjuundersökning Typ A, som är relevant för detta kapitel, visar att sköterskor och patienter överlag efterfrågade hög eller högsta klassificeringsnivå på insynsskydd, tillgänglighet, spårbarhet och riktighet.

7.5 Författarnas kommentarer

Vi instämmer med idén i TIHS om att använda gemensamma arbetsmetoder i informationssäkerhetsarbete. På det sättet ökar kunskaper och erfarenheter och gör det möjligt att samarbeta för att förbättra säkerhetsarbetet. TIHS är en metod för hur det är lämpligt att tillämpa standarden SS-ISO/IEC 17799 inom hälso- och sjukvård.

Vi kommer att förespråka att TIHS används vid säkerhetsarbetet för IMIS även om inte landstinget Blekinge ännu har planer på att använda TIHS. Om metoden kommer att användas vid vidareutvecklingen av IMIS kommer vi att rekommendera metoden för Thomas Pehrsson IT-chef för landstinget Blekinge.

Vi rekommenderar att en nyttoanalys för IMIS ska genomföras eftersom det ställs stora krav på ett system som ska användas i hälso- och sjukvård. Enligt vår åsikt går det inte att utveckla ett system för hälso- och sjukvård utan att informationssäkerhetsarbetet finns med från start. Resultat från nyttoanalysen visar att ledningen står bakom ett sådant arbete.

IMIS kommer att kommunicera med olika parter inom hälso- och sjukvård som hanterar sekretessbelagd information. En informationssäkerhetspolicy skapar ett förtroende mellan inblandade parter. En policy är också den viktigaste delen för att kunna bedriva ett informationssäkerhetsarbete, utan policy finns inga mål att arbeta efter. På dessa grunder anser vi att IMIS-projektet måste ta fram en egen informationssäkerhetspolicy.

Vi anser att metoden med användningsfall är ett utmärkt sätt att bryta ner informationssäkerhetsarbetet och ta ner det till rättvisande nivå. Vi tror att det kan vara

lätt att göra riskanalyser och informationsklassificering på en hög nivå och sedan tro att hela verksamheten täcks in, användningsfall försvårar en sådan felbedömning. Enligt vår mening ska informationssäkerhetsarbete fokusera lika mycket på människa och teknik, metoden med att arbeta med användningsfall är ett utmärk sätt att realisera detta.

8 RIKTLINJER FÖR LEDNING AV INFORMATIONSSÄKERHET, SS-ISO/IEC 17799

Kapitel åtta ger en sammanfattning av den internationella standarden SS-ISO/IEC 17799. Den anses vara det för närvarande bästa instrumentet för hur ett informationssäkerhetsarbete ska bedrivas. Den metod, TIHS, som vi presenterar i kapitel sju, är ett sätt att tillämpa vissa delar av standarden, riskanalys, säkerhetspolicy, organisatorisk säkerhet och klassificering och kontroll av tillgångar. De delar som inte innefattas i TIHS presenteras här. Som avslutning redovisas författarnas kommentarer.

8.1 Introduktion

SS-ISO/IEC 17799 är en svensk och internationell standard vars syfte är att skapa struktur i informationssäkerhetsarbete. Standarden specificerar hur alla verksamheter kan bygga upp ett Ledningssystem för Informationssäkerhet, LIS,. Den heter Riktlinjer för ledning av informationssäkerhet och består av två delar. Del 1, ISO-standard SS-ISO/IEC 17799, innehåller råd för hur ett ledningssystem för en säker informationshantering inom en organisation byggs upp och underhålls. Del 2, svensk standard SS 62 77 99-2, består av en kravlista baserad på Del 1. Kravlistan används som underlag vid certifiering av en organisations ledningssystem för informationssäkerhet [13]

Med informationssäkerhet menas i LIS följande tre egenskaper:

- *Sekretess* – säkerställande av att informationen är tillgänglig endast för dem som är behöriga att ta del av och använda den,
- *Riktighet* – skydd av informationen så att den är och förblir korrekt och fullständig,
- *Tillgänglighet* – säkerställande av att användarna har till gång till informationen när den behövs.

Ytterligare en viktig egenskap är spårbarhet som innebär möjligheten att i efterhand identifiera genomförda händelser [13].

Standarden är väldigt komplex och detaljrik därför har SIS gett ut boken ”Handbok i Informationssäkerhetsarbete” som bygger på SS-ISO/IEC 17799. Varje delområde i standarden behandlas i handboken och i slutet på varje område finns en checklista med frågor som när de besvaras ger en bild av hur dagsläget ser ut. I varje kapitel finns också scenarier från ett exempelföretag som används i boken. Exemplen ger en tydlig bild över olika säkerhetsincidenter som kan inträffa och på vilka sätt de kunde förebyggas genom att använda standardens rekommendationer.

8.2 Klassificering och kontroll av tillgångar

Detta kapitel innehåller en punkt under avsnittet ”Klassificering av information” som inte tas upp i TIHS. Författarna bedömer att den är viktig och den redovisas här.

Märkning av information

För känsliga eller kritiska klasser av information måste vissa moment beaktas särskilt noga då de utgör en kritisk del av informationshanteringen. Momenten är följande:

- kopiering
- lagring
- överföring via post, fax, eller e-post
- överföring via tal (även mobiltelefon, röstbrevlåda, telefonsvarare)
- förstöring
- arkivering

I varje informationsklass bör det definieras speciella rutiner för hur de kritiska momenten ska hanteras [13].

8.3 Personal och säkerhet

I en organisation betraktas människor som den viktigaste resursen samtidigt som de utgör ett hot för en organisation. Att uppnå en hög nivå av informationssäkerhet innebär att människor i en organisation är lojala mot varandra och att organisationen har en god arbetsmiljö. Att täcka in hela säkerhetsbegreppet personal och säkerhet kan göras av en organisation som prioriterar informationssäkerhet lika högt som en god arbetsmiljö.

8.3.1 Säkerhet i beskrivning av befattningar och vid rekrytering och omplacering

Mål enligt SS-ISO/IEC 17799: Att minska riskerna för mänskliga misstag, stöld, bedrägeri eller felaktigt utnyttjande av tillgångar.

En riskprofil bör tas fram för varje befattning inom en organisation som hanterar känsligt material. Denna profil gäller för all personal och ska stämmas vid all typ av nyanställning och omplacering.

Inkluderande av säkerhet i beskrivning av ansvar i arbetet

En befattningsbeskrivning bör innehålla vilka informationstillgångar som hör till en tjänst och att ansvaret gäller för både skydd och underhåll. När en befattningsbeskrivning upprättas ska befintlig riskprofil tas i beaktande.

Val av personal och policy

Följande områden bör tas i beaktande vi all rekrytering och anlitande av personal (t ex konsultverksamhet).

- *Identitet* bör kontrolleras via accepterade id-handlingar
- *Referenser* bör kontrolleras
- *Meritförteckningar* bör kontrolleras utifrån riktighet och rimlighet. Bör bekräftas med betyg eller intyg.
- *Kreditupplysning* bör kontrolleras för befattningar som innebär ett ekonomiskt ansvar.
- *Utdrag ur polisregister* kan vara befogat på vissa befattningar, bör dock inte tillmätas för stort värde eftersom utdraget kan vara ofullständighet på grund av sekretessregler.

Sekretessavtal

Avtal som berör sekretess bör upprättas vid anställning och anlitande av personal som tydligt definierar vad sekretessen avser, vilket ansvar och vilka befogenheter som gäller för sekretessbelagd information. Inom den offentliga sektorn regleras sekretess enligt lagstiftning.

Anställningsvillkor och anställningsförhållanden

Villkor för anställning och anställningsförhållande bör tydligt definiera ansvar, rättigheter och skyldigheter som en anställning. Frågor som bör tas upp ur informationssäkerhetsperspektiv kan t ex vara upphovsrätt, nyttjande och spridande av information. Vad som gäller för upphörande eller ändring av befattning bör definieras i anställningsförhållande.

8.3.2 Användarutbildning

Mål enligt SS-ISO/IEC 17799: Att säkerställa att användare är medvetna om hot och risker rörande informationssäkerhet och är rustande så att de i sitt dagliga arbete kan stödja organisationens informationssäkerhetspolicy.

För att minimera säkerhetsrisker bör användare utbildas i säkerhetsrutiner och korrekt hantering av informationshanteringsresurser. Detta gäller all personal som på något sätt är involverade i en organisation.

Utbildning och övning i informationssäkerhet

Information om gällande informationssäkerhetspolicy och tillhörande regelverk bör delges alla anställda vid introduktion på arbetsplatsen med tillhörande kontinuerlig uppföljning.

8.3.3 Reaktion på säkerhetsincidenter och funktionsfel

Mål enligt SS-ISO/IEC 17799: Att minska skador på grund av säkerhetsincidenter och fel och att övervaka och dra lärdom av dessa.

Rapportering av säkerhetsincidenter

Rutiner gällande rapportering och hantering av incidenter bör finnas och kännas till av alla i organisationen.

Rapportering av svagheter avseende säkerhet

Rutiner gällande rapportering och hantering av säkerhetsmässiga svagheter bör finnas och kännas till av alla i organisationen.

Rapportering av funktionsfel i program

Rutiner gällande rapportering av funktionsfel i program som används av medarbetare bör finnas och analyseras för att sätta in rätt hjälpfunktion.

Att lära av incidenter

Att utvärdera rapporterade svagheter och incidenter är väsentligt för att utveckla ledningssystem och skyddet för informationstillgångar. Resultatet av utvärderingar bör användas vid riskanalyser och uppdatering av informationssäkerhetspolicy.

Disciplinär process

I samband med utbildning om informationssäkerhet bör information om att t ex en varning, omplacering, uppsägning eller polisanmälan är en disciplinär åtgärd. En disciplinär åtgärd måste ha stöd av ett regelverk och dess användning är konsekvensen av att en avsiktligt illojal handling mot organisationen har gjorts.

8.4 Fysisk och miljörelaterad säkerhet

Fysisk och miljörelaterad säkerhet har till syfte att skydda till exempel lokaler och utrustning. Det gäller inte enbart skydd mot kriminella handlingar som stöld eller skadegörelse utan det gäller också att skydda mot slarv eller naturkatastrofer. Många orsaker finns som ställer till fel i den tekniska miljön och mänskliga misstag och slarv utgör stora säkerhetshot.

8.4.1 Säkrade utrymmen

Mål enligt SS-ISO/IEC 17799: Att förhindra obehörigt tillträde, skador och störningar I organisationens lokaler och information.

Skalskydd

Med skalskydd menas fysiska hinder runt verksamheter eller större och mindre delar av lokaler. De kan bestå av olika byggtekniska konstruktioner som exempelvis ståldörr, galler eller förstärkt betongväggvägg. Det finns alltid sätt att ta sig förbi skalskydd så de ska kompletteras med lämpliga typer av larm för att fylla sin funktion.

Tillträdeskontroll

Någon form av tillträdeskontroll bör finnas till säkrade utrymmen. Kontrollen kan ske med bemannad reception eller med hjälp av teknik. Både in och utpassering bör registreras för att kontrollen ska vara användbar. Det bör finnas en central funktion för behörighetstilldelning.

Skydd av kontor, rum och utrustning

Vid denna typ av skydd rekommenderas larm och TV-övervakning. Utrustning som bedöms speciellt värdefull kan skyddas med separat skydd. Vid utformning av dessa skydd är det av vikt att väga in hot både i den externa och interna miljön.

Arbete i säkrade utrymmen

Då personal som inte är behöriga, utför arbetsuppgifter i säkrade utrymmen bör de övervakas på något sätt

Avgränsade utrymmen för godsmottagning och lastning

Obehörigt tillträde till känsliga områden kan undvikas om godsmottagning och lastning sker i avgränsade utrymmen. Allt som passerar in och ut vid godsmottagningen ska registreras och inkommande gods bör kontrolleras.

8.4.2 Skydd av utrustning

Mål enligt SS-ISO/IEC 17799: Att förhindra förlust, skada eller påverkan på tillgångar och avbrott i verksamheten.

Placering och skydd av utrustning

Utrustning bör placeras så att risk genom obehörig insyn, åtkomst, avlyssning och hot från intern och extern miljö beaktas. Speciellt känslig utrustning bör placeras så att utformning av punktskydd underlättas. Brand är alltid ett stort hot och brandrisk minimeras med hjälp av byggnadstekniska åtgärder.

Elförsörjning

Interna och externa faktorer kan störa elförsörjningen. Ett effektivt tillgänglighetsskydd ska innefatta skydd mot elavbrott och andra störningar i elförsörjningen. För särskilt avbrottskänsliga system rekommenderas dubblerade och av varandra oberoende vägar för elförsörjning.

Kablageskydd

Kablageskydd bör omfatta skydd mot avlyssning, åverkan och elektromagnetisk störning.

Underhåll av utrustning

Allt underhåll av utrustning är känsliga moment där hemlig information måste skyddas. Det bör finans en plan för hur underhåll ska utföras.

Säkerhet för utrustning utanför egna lokaler

Planering bör finnas för hur utrustning ska skyddas utanför egna lokaler. Skyddet omfattar bland annat handdatorer, persondatorer, mobiltelefoner och pappersdokument. Risker kan variera mellan olika platser och tidpunkter och det är viktigt att kalkylera med risker i samband med att utrustning lämnas ut för service.

Säker avveckling eller återanvändning av utrustning

Lagringsmedia ska avmagnetiseras och licensierade program förstöras vid avveckling eller återanvändning av utrustning. Det kan också finnas speciella regler för förstöring av IT-utrustning.

8.4.3 Allmänna åtgärder

Mål enligt SS-ISO/IEC 17799: Att hindra att informationsbehandlingsutrustning äventyras eller stjäls.

Policy för städat skrivbord och tom skärm

Policyn innebär att känslig information inte lämnas oskyddad när den inte används. Rutiner för hur informationen förvaras när den inte används minimerar risk för sekretessbrott, brand och vattenskador.

Avlägsnande av egendom

Fastställda rutiner bör finnas för avlägsnande av egendom. Det bör också finnas riktlinjer för hur säkerhetsklassad utrustning ska hanteras.

8.5 Styrning av kommunikation och drift

8.5.1 Driftrutiner och driftansvar

Mål enligt SS-ISO/IEC 17799: Att säkerställa korrekt och säker drift av informationsbehandlingsutrustning.

Dokumenterade driftrutiner

Dokumenterade driftrutiner bör betraktas som styrande dokument och ska uppdateras vid förändringar. Dokumentationen bör omfatta hela den integrerade systemmiljön, kommunikation, säkerhetskopiering, underhåll, ledning, personsäkerhet

i datahallar och posthantering. Alla identifierade rutiner bör ha klara instruktioner om tillvägagångssätt.

Styrningar av ändringar i drift

Förändringar i drift kan påverka säkerheten i olika delar av ett system. För att kunna hålla en bra säkerhetsnivå bör de finnas formella rutiner att följa i samband med förändringar i informationsbehandlingsutrustning och system.

Rutiner för incidenthantering

Rutinerna bör innefatta rutiner för driftavbrott och fel på informationssystem (även avsiktligt framkallade), störningar och felaktigheter på grund av inkorrekt data och sekretessbrott. Det ska även finnas rutiner för hur incidenter rapporteras och vilka instanser som ska informeras. Vid ett intrång ska snabbt och korrekt agerande kunna ske.

Uppdelning av arbetsuppgifter

Uppdelning av arbetsuppgifter kan vara en lämplig metod att minska risk för missbruk av system. Samma person bör exempelvis inte ha kontroll över både driftsättning och utveckling av ett system.

Uppdelning av utvecklings- och driftresurser

En uppdelning som innebär att resurser för drift, utveckling och test ska hållas åtskilda är en huvudregel. Åtskillnaden kan ske på olika sätt det kan vara genom att använda olika domäner, kataloger eller processorer.

Hantering av externa resurser

En möjlig riskfaktor är hantering av externa resurser därför bör analys av hanteringen genomföras. Det kan vara nödvändigt att undersöka externa leverantörers hantering av exempelvis incidenthantering och säkerhetsorganisation

8.5.2 Systemplanering och systemgodkännande

Mål enligt SS-ISO/IEC 17799: Att minimera risken för systemfel.

Kapacitetsplanering

En adekvat kapacitetsplanering bör innefatta både nuvarande och eventuella kommande behov. En sådan planering gör att det går att täcka viss framtida utveckling av informationsbehandlingen.

Systemgodkännande

När av ledningen fastställda krav är definierade, överenskomna, dokumenterade och testade, kan systemgodkännande ske.

8.5.3 Skydd mot skadliga program

Mål enligt SS-ISO/IEC 17799: Att skydda riktighet i program och data.

Åtgärder mot skadliga program innebär att organisationen har riktlinjer som rekommenderas omfatta följande punkter:

- Ett formellt förbud i policy mot användning av icke godkända program samt mot att hämta hem datafiler eller program från externa källor som Internet.
- Program för detektering av skadliga program samt stödprogram för återställande.
- Regelbunden granskning av program och data i samband med kritiska verksamhetsprocesser.
- Antivirusprogram, som också inbegriper kontroll av bifogade filer i e-post.
- Fastställande av ledningsrutiner och ansvar för virusskydd.
- Avbrottsplan
- Verifiering av – och tillgång till – information som rör skadliga program.

8.5.4 Ordning och reda

Mål enligt SS-ISO/IEC 17799: Att bevara informationsbehandlings- och kommunikationstjänsternas riktighet och tillgänglighet.

Säkerhetskopiering

All säkerhetskopiering bör ske enligt fasta rutiner för såväl tidpunkt för kopiering och permanent lagring av dessa. För kritiska tillämpningar bör det finnas tre generationer säkerhetskopior lagrade utanför det normala driftstället.

Operatörsloggar

Allt arbete som utförs av operatörer bör loggas. De bör kontrolleras regelbundet av oberoende person så att medvetna eller omedvetna misstag upptäcks tidigt.

Felloggar

Felloggar bör föras över rapporterade fel för att möjliggöra spårning av fel och incidenter. Granskning bör ske av både felloggar och korrigerande åtgärder.

8.5.5 Styrning av nätverk

Mål enligt SS-ISO/IEC 17799: Att säkerställa skyddet av information i nätverk och tillhörande infrastruktur.

Styrmedel för nätverk

Hänsyn bör tas till behovet av skydd av data i nätverksmiljön. Rutiner för säkerhet i nätverksmiljöer bör innefatta lokal utrustning som t ex arbetsstationer och skrivare. Ansvar för att rutinerna följs bör vara skilt från ansvar för datordrift. Med hjälp av brandväggar och annan teknisk uppdelning av miljön kan säkerhetskrav som gäller åtkomst regleras.

8.5.6 Mediahantering och mediasäkerhet samt kontroll över flyttbara medier

Mål enligt SS-ISO/IEC 17799: Att förhindra skador på tillgångar och avbrott i verksamheten

Avveckling av media

All avveckling bör ske enligt dokumenterade riktlinjer som omfattar alla typer av lagringsmedia.

Rutiner för informationshantering

Alla rutiner för informationshantering bör vara tydliga för att minimera risk för missbruk eller obehörig åtkomst.

Säkerhet för systemdokumentation

Säkerhet för systemdokumentation innebär att lagringsmedia för dokumentation är säkert och åtkomligt.

8.5.7 Utbyte av information och program

Mål enligt SS-ISO/IEC 17799: Att hindra förlust, förändring och missbruk av information som utbyts mellan organisationer.

Avtal om utbyte av information och program

Sådana avtal bör utformas så att den egna organisationens bedömning av informationstillgångarnas känslighet ligger till grund för avtalsutformning.

Säkerhet för media under transport

Säkerhetsrutiner för transport av media bör återspegla transportens värde för organisationen.

Säkerhet i elektronisk handel

Genom väl genomförda risk/sårbarhetsanalyser kan tillfredsställande säkerhet uppnås. Analyserna ligger till grund för tekniklösningar, säkerhetsorganisation och rutiner som organisationen beslutar.

Säkerhet för elektronisk post

En tydlig policy för elektronisk post bör finnas. Riktlinjer utformas dels för att förhindra virusspridning, dels för att förhindra att post och adresser förekommer i olämpliga sammanhang.

Säkerhet för elektroniska kontorssystem och annat informationsutbyte

Integrerade kontorssystem bör utvärderas på samma sätt som övriga delar i IT-miljön vid utarbetande av policy och riktlinjer. Policy och riktlinjer bör också omfatta sådana typer av informationsutbyte som t ex fax och video.

8.6 Styrning av åtkomst

Åtkomstskydd för information är lika viktigt som att ha skydd för fysiska tillgångar därför har informationssäkerhet och fysisk säkerhet en väsentlig och given plats i verksamheter som nått framgång.

8.6.1 Verksamhetskrav på styrning av åtkomst

Mål enligt SS-ISO/IEC 17799: Att styra åtkomst till information

Policy för styrning av åtkomst

En informationssäkerhetspolicy ska tydligt definiera riktlinjer som gäller tilldelning/frântagning av åtkomsträttigheter och operativ användning av rättigheterna. Operativ styrning kan ske genom obligatorisk eller frivillig åtkomststyrning. Obligatorisk styrning, vilket är mest säkerhet, innebär att åtkomsträttigheter för samtliga användare till varje informationsresurs måste definieras vilket sker centralt medan frivillig styrning innebär att ägaren till respektive informationsresurs sköter åtkomststyrningen.

8.6.2 Styrning av användares åtkomst

Mål enligt SS-ISO/IEC 17799: Att förhindra obehörig åtkomst till informationssystem

Användarregistrering

Systemet för användarregistrering bör innefatta steget nyregistrering och samtliga steg fram till slutlig avregistrering. En användaridentitet som är unik tillsammans med loggning för användaraktiviteter är en väsentlighet för att kunna spåra en användares handling. Syftet med spårbarhet är att kunna ställa användare till svars för sina handlingar och samtidigt frita andra användares ansvar.

Styrning av särskilda rättigheter

Åtkomsträtten som överträder normal åtkomstkontroll, privilegierad behörighet, bör användas ytterst försiktigt och så att spårbarheten upprätthålls.

Styrning av lösenord för användare

En formell och sekretessbelagd rutin bör följas vid utdelning av lösenord. Innan rutinen genomförs ska användaren identifieras, regler för hantering av lösenord ska vara fastställda och att användaren har förstått dessa regler. Temporära lösenord ska användas ytterst sparsamt och följa vissa regler.

Granskning av användares åtkomsträttigheter

Behörigheter som delats ut bör granskas vid jämna mellanrum.

8.6.3 Användares ansvar

Mål enligt SS-ISO/IEC 17799: Att förhindra obehörig användaråtkomst

Användning av lösenord

Lösenord ska:

- bestå av minst sex tecken, varav minst två numeriska eller specialtecken
- inte ska kunna associeras till användaren.
- hållas hemliga
- sparas på säkert sätt på pappers eller datamedia
- aldrig lagras oskyddat

Obemannad användarutrustning

Utrustning som datorer eller terminaler som lämnas utan tillsyn bör skyddas på ett tillfredställande sätt t ex genom skärmsläckare eller att inloggning krävs efter en viss tid utan användande. Arbetsstationer och terminaler ska normalt aldrig slås av utan utloggning.

8.6.4 Styrning av åtkomst till nätverk

Mål enligt SS-ISO/IEC 17799: Skydd av nätverkstjänster

Policy för utnyttjande av nätverkstjänster

Tillgång och behörighet till nätverk och nätverkstjänster bör styras via en policy.

Tvingande vägval

För att förhindra obehörig användning av nätet bör fördefinierade vägval finnas i nätverket.

Autentisering av användare för externanslutning

Vid externa anslutningar ska rätt säkerhetsåtgärder vidtas eftersom det innebär oerhört stora risker.

Autentisering av nod

Vid externa anslutningar ska rätt säkerhetsåtgärder vidtas eftersom det innebär oerhört stora risker.

Skydd av extern diagnosport

Diagnosportar för distansunderhåll bör vara avstängda och fysiskt skydde när de inte används.

Uppdelning i nätverk

Dagens utökande teknik medför nya problem vilket också kräver nya lösningar ur informationssäkerhetsperspektiv. Logiskt sektionerade nätverk med säkrad kommunikation mellan sektionerna är ett sätt att försöka besvara problemen.

Kontroll över nätverksanslutning

Hjälpmedel för nätverkskontroll är växlar, filtrerande routrar och brandväggar vilka bör användas i någon form beroende på vad som krävs.

Styrning av vägval

För att vara säker på att informationsflödet följer policyn och regler för åtkomst kan styrning av vägval i delade nätverk vara aktuell.

Säkerhet i nätverkstjänster

För att kunna garantera säkerhet krävs ett samarbete med leverantören av nätverkstjänsten samt att eventuellt begränsa tillgången till nätverkstjänsterna till en viss tid på dygnet.

8.6.5 Styrning av åtkomst till operativsystem

Mål enligt SS-ISO/IEC 17799: Att förhindra obehörig åtkomst till datorer

Automatisk terminalidentifikation

Automatisk terminalidentifikation innebär att identifiering sker med hjälp av en fysisk enhet för identifiering vid en viss plats eller terminal.

Påloggningsrutin för terminal

Rutiner för påloggning ska:

- tillåta en enkel och effektiv påloggning för legitima användare
- minimera möjligheten för obehöriga att komma åt system

Först efter fullständig påloggning ska systeminformation o s v visas och antalet inloggningsförsök bör begränsas och loggas.

Identifiering och autenticering av användare

Användare ska tilldelas en unik användaridentitet (undantag för administratörer som lämpligen tilldelas flera identiteter). Användares identitet ska kunna styrkas genom något användaren:

- vet (lösenord)
- har (kort)
- är (fingeravtryck)

Lösenordsrutin

Rutiner för lösenord bör innebära att:

- kvaliteten på lösenord kontrolleras
- lösenordbyte sker med jämna mellanrum
- återanvändning av lösenords hindras
- lösenord visas och sparas på ett säkert sätt

Användning av systemhjälpmedel

Användning och tillgång till systemhjälpmedel som kan forcera åtkomstspärrar ska begränsas och användning ska auktoriseras och loggas.

Överfallslarm för att skydda användare

Användare som anses vara i riskzonen för fara och tvång ska förses med överfallslarm.

Tidsfördröjd nedkoppling av terminal

Automatisk utloggning och nedkoppling av terminalen kan vara lämplig för att förhindra obehörig åtkomst.

Begränsad uppkopplingstid

Restriktioner för uppkopplingstid kan öka säkerheten vilket dock kräver verksamhetens tillåtelse.

8.6.6 Styrning av åtkomst till tillämpningar

Mål enligt SS-ISO/IEC 17799: Att förhindra obehörig åtkomst av information i informationssystem

Begränsning av åtkomst till information

Utformning av tillämpningssystem bör utformas så att differentierad åtkomst till systemdata och -funktioner kan tillämpas och att åtkomst följs enligt policy och regler.

Isolering av känsliga system

Är ett system speciellt känsligt eller kritiskt kan helt eller delvis dedikerade tekniska plattformar krävas.

8.6.7 Övervakning av systemåtkomst och systemanvändning

Mål enligt SS-ISO/IEC 17799: Att upptäcka obehöriga aktiviteter

Loggning av händelser

Väsentligt för spårbarhet är att kunna logga användaraktiviteter. Revisionsloggar bör föras och förvaras säkert skyddade om de registrerar följande:

- avvikelser
- oregelbundenheter
- andra säkerhetsrelaterade händelser

Övervakning av systemanvändning

Områden att bevaka ur säkerhetsperspektiv är:

- behörig åtkomst
- försök till obehörig åtkomst
- avvikande användarbeteende
- privilegierade bearbetningar
- system och intrångslarm

System att övervaka detta är system för nätövervakning och intrångsdetektering och det bör ske både i realtid och genom granskning av loggar.

Klocksynkronisering

Datorklockor som används inom ett nätverk bör ställas enligt överenskommen standardtid för att kunna säkerställa giltigheten på loggar som görs.

8.6.8 Mobil datoranvändning och distansarbete

Mål enligt SS-ISO/IEC 17799: Att trygga informationssäkerheten vid användning av mobil utrustning och vid distansarbete.

Mobil användning

Det viktigaste skyddet vid mobil användning är användare själv, vilket kräver säkerhetsutbildning och klara säkerhetsprocedurer inom informationssäkerhet.

Speciella skyddsåtgärder mot stöld, obehörig insyn eller avlyssning kan krävas på utrustning som används på oskyddade platser. Speciell maskin- och programvara för säkerhetskopiering, kryptering och virusskydd kan även vara väsentlig. Nämnda rutiner gäller t ex pc, handdator och mobiltelefon.

Distansarbete

Säkerhetsaspekter som bör beaktas vid distansarbete är:

- fysiskt skydd och förvaring
- kommunikationsskydd
- skydd mot obehörig insyn
- skydd mot obehörig användning
- säkerhetskopiering och kontinuitetsplanering
- revision och övervakning av säkerhet

Legala, försäkrings- och arbetsmiljöaspekter ska utredas och beaktas noga vid regelbundet distansarbete.

8.7 Systemutveckling och systemunderhåll

Vid utveckling av ett system är det viktigt att väga in säkerhetskrav redan vid början av själva utvecklingen annars kan utvecklingen blir mycket kostsam och resultera i ett system som inte kommer att användas.

8.7.1 Säkerhetskrav på system

Mål enligt SS-ISO/IEC 17799: Att säkerställa att säkerhet byggs in i informationssystem.

Systemutvecklingens olika delar måste vara klart definierade och dokumenterade innan utvecklingsarbetet börjar. Grunden för utvecklingen är kravspecifikationen för projektet som även ska ta upp säkerhetskrav. Vilken nivå säkerhetskraven hamnar på beror på vilket värde informationen som ska hanteras har för aktuellt projekt. Även risker och riskhantering bör tas i beaktande och den skada som skulle kunna uppstå om inte säkerheten är tillräcklig. Den gång som säkerhetsarbetet bör följa är:

- Strategi
- Analys
- Genomförande
- Test/Överlämnande
- Drift/Underhåll
- Avveckling

8.7.2 Säkerhet i tillämpningssystem

Mål enligt SS-ISO/IEC 17799: Att förhindra förlust, felaktig förändring och missbruk av data i tillämpningssystem.

Att kontrollera in- och utdata i ett system är viktigt för att kunna garantera kvaliteten av den information som hanteras. Lämpliga kontrollera kan vara följande:

- dubbelinmatning av data
- rimlighetstester
- gränsvärden

Inmatningsfel kan i vissa fall ställa till förödande konsekvenser därför är det viktigt att metod av kontroll anpassas efter den information som ska hanteras. Inmatad data som är rätt kan även den förvanskas genom bearbetningsfel, felhantering eller sabotage. Därför behövs även här kontroller vilket gäller likadant för utmatad data kontrolleras med t ex rimlighetskontroller.

8.7.3 Kryptering

Mål enligt SS-ISO/IEC 17799: Att skydda informations sekretess, autenticitet och riktighet

Med hjälp av olika krypteringstekniker skyddas informationens sekretess och riktighet och kan även garantera dess äkthet. För en organisation som använder kryptering är ansvarsfördelning, generering och distribution av nycklar en väsentlig fråga. I frågan om kryptering, val av algoritm och andra krypteringsmetoder är det lämpligt att ta hjälp av experter.

8.7.4 Säkerhet i databaser och filer

Mål enligt SS-ISO/IEC 17799: Att säkerställa att IT-projekt och deras stödrutiner genomförs på ett säkert sätt.

Yttersta försiktighet bör tas vid system- och programändringar, alla ändringar bör dokumenteras för att kunna spåras i efterhand. Tester på databaser ska göras på särskilda kopior av databasen som sedan kan raderas. Testning av program bör följa strikta regler och rutiner.

8.7.5 Säkerhet vid utveckling och underhåll

Mål enligt SS-ISO/IEC 17799: Att uppnå och bibehålla säkerhet i tillämpningssystem och information.

Vid systemförändringar bör formell rutin följas för godkännande och beslut. Följande frågor bör ingå:

- Behörighet och behörighetskontroll
- Rätten att fatta beslut om ändring
- Kontroll av att andra program inte påverkas av ändringen
- Uppdatering av styrdokument
- Ändring och anpassning av drift- och användardokumentation
- Arkivering av gamla versioner

Upphandling av ny programvara bör ske med välrenommerade leverantörer av program och vid extern utveckling bör avtal upprättas angående t ex upphovsrätt, kvalitet och tester.

8.8 Kontinuitetsplanering

8.8.1 Aspekter på kontinuitetsplanering

Mål enligt SS-ISO/IEC 17799: Att motverka avbrott i organisationens verksamhet och skydda kritiska rutiner från effekter av oförutsedda allvarligare avbrott eller katastrofer.

Avbrotts och konsekvensanalys

Avbrotts och konsekvensanalys genomförs i samband med riskanalys. I denna inkluderas en katastrofsituations påverkan både på affärsverksamhet och på infrastruktur.

Att utarbeta och införa kontinuitetsplaner

Att utarbeta, införa och underhålla en kontinuitetsplan är ett omfattande arbete som kräver ledningens sponsring. I en större organisation kan det utses en förvaltningsorganisation som ansvarar införande och underhåll av planen.

Ramverk för verksamhetens kontinuitetsplanering

Ett ramverk för verksamhetens kontinuitetsplanering kan med fördel utarbetas i projektform. I arbetet ingår moment som t ex att bygga upp riskmedvetenhet i verksamheten, ta fram reservrutiner, dokumentera rutinerna samt föreslå åtgärder och beslut som ska tas på ledningsnivå.

Test, underhåll och ändring av avbrottsplaner

Det ligger på förvaltningsorganisationens ansvar att testa, underhålla och ändra avbrottsplaner. Deras ansvar omfattar också att anpassa planen till förändringar i organisationen. Förvaltningsorganisationen ska definiera hur och när behov finns för

granskning, den ska också försäkra sig om att det finns kapacitet att sätta planen i verket.

8.9 Efterlevnad

8.9.1 Efterlevnad av rättsliga krav

Mål enligt SS-ISO/IEC 17799: Att undvika handlande i strid mot lagar och andra författningar, avtal och eventuella andra yttre säkerhetskrav.

Identifiering av lämpliga bestämmelser

Identifiering av lämpliga bestämmelser bör ske för varje informationssystem. Det ska klart framgå vilka rätts- och avtalsregler som gäller. Ansvariga för efterlevnad bör utses och få tillgång till de styrmedel som behövs för att efterlevnaden ska kunna följas upp.

Immaterialrätt

Immaterialrätt reglerar t ex upphovsrätt, patent och varumärkesskydd. För produkter så regleras i licensavtal vilka restriktioner som gäller.

Skydd av organisationens register och handlingar

För att undvika förstörelse och förvanskning av uppgifter eller att de avslöjas otillåtet, bör organisationens register och handlingar skyddas. Ett system för lagring och hantering bör upprättas. Lagringsmedia väljs i förhållande till hur och hur länge registret ska lagras.

Skydd av persondata

Hantering av persondata regleras i lag, PUL. I PUL anges vilka personuppgifter som får behandlas och vilka krav som ställs på hanteringen. Individuellt ansvar krävs för register med personuppgifter.

Förhindrande av missbruk av informationsbehandlingsresurser

Instruktioner bör upprättas om hur organisationens utrustning får användas. Användare i organisationen bör informeras om vilken användning som är tillåten och om de påföljder som finns vid överträdelser. Rutiner för uppföljning bör finnas för att kunna upptäcka missbruk.

Reglering av kryptering

I vissa länder regleras i lag hur kryptering får ske. Det kan var restriktioner för import/export eller det kan var krav på statlig tillgång av krypteringsnycklar. Expertis bör anlitas innan information eller utrustning flyttas till annat land.

8.9.2 Granskning av säkerhetspolicy och teknisk efterlevnad

Mål enligt SS-ISO/IEC 17799: Att säkerställa att system följer organisationens säkerhetspolicy och säkerhetsnorm.

Efterlevnad av säkerhetspolicy

Efterlevnad av säkerhetspolicy följs upp genom regelbunden granskning av informationssystem, systemleverantörer, ägare av information och informationstillgångar, användare och ledningspersonal. Arbete bör aktivt stödjas av informationsägarna.

Kontroll av teknisk efterlevnad

Kontroll av teknisk efterlevnad genomförs lämpligen av specialister. Säkerhetslösningar ska kontrolleras så att de är korrekt implementerade. Genom tester ska effektivitet mot systemintrång kontrolleras.

8.9.3 Hänsynstagande vid revision av system

Mål enligt SS-ISO/IEC 17799: Att maximera systemrevisionens effektivitet och samtidigt minimera driftstörningar orsakade av revisioner.

Styrning av revision av system

Styrning sker i samråd med ledningen, överenskommelser träffas angående de kontroller som ska göras. Revisorer och revisionsprogram bör endast ha läsrättighet.

Loggning rekommenderas för att möjliggöra spårbarhet. Revisionsrutiner och ansvarsförhållanden ska dokumenteras.

Skydd av hjälpmedel för revision av system

Åtkomst till revisionshjälpmedel bör begränsas. Hjälpmedlen bör lagras åtskilda från utvecklings och produktionssystem.

8.10 Lagrum, efterlevnad av rättsliga krav

8.10.1 Rättsregler som bör beaktas vid informationsbehandling.

Regler om sekretess och tystnadsplikt

- *Sekretesslagen* avgör (exklusivt) vilken information hos myndigheter och andra offentliga organ som är offentlig respektive sekretessbelagd.
- Regler om sekretess- och tystnadsplikt i särskilda verksamheter finns bland annat för sjukvårdsverksamhet, tele- och postverksamhet och advokatverksamhet.

Regler om förvaring och arkivering

- *Arkivlagen* tar upp arkivregler för myndigheter och andra offentliga organ.
- *Bokföringslagen* uppställer krav på betryggande arkivering av allt räkenskapsmaterial i minst tio år.
- *Aktiebolagslagen* uppställer bland annat krav på att aktiebok och protokoll från styrelsemöten förvaras på betryggande sätt.

Regler om skydd för personlig integritet

- *Personuppgiftslagen* innehåller detaljerade bestämmelser om behandling av personuppgifter. Lagen gäller både manuell och automatisk (data) behandling av personuppgifter

Immaterialrättsliga regler

- *Upphovsrättslagen* innebär att upphovsmannen till exempelvis bilder, texter och datorprogram har ensamrätt att sprida och mångfaldiga dessa. Även databaser skyddas av lagen.
- *Varumärkeslagen* (VML) och firmalagen (FL) innebär att den som inregistrerat eller inarbetat ett varumärke eller en firma har ensamrätten till detta och att andra är förbjudna att utan tillstånd använda samma eller förväxlingsbart varumärke respektive firma i näringsverksamhet.
- *Patentlagen* (PL) innebär att den som fått patent på en uppfinning har ensamrätt att yrkesmässigt utnyttja uppfinningen.

Arbetsrättsliga regler

- *Medbestämmandelagen* (MBL): Förhandlings- och informationsskyldigheten enligt MBL måste iakttas vid införande av riktlinjer för verksamheten i organisationen, exempelvis vid införande av riktlinjer för övervakning av anställdas e-post- och Internetanvändning, och vid införandet av sanktioner för överträdelse av riktlinjerna.

Regler om krypteringsprodukter

- Rådsförordning (EG) nr. 3381/94 och lag (1998:397) om strategiska produkter: *Krypteringsprogramvara* omfattas generellt av exportkontrollagstiftning – såväl inom EU som Sverige – varför utgångspunkten är att tillstånd krävs från Inspektionen för Strategiska Produkter för export och i vissa fall utförsel av sådan programvara. Det finns dock generella undantag för vissa typer av krypteringsprogramvara. Tillgängliggörande via Internet anses normalt innebära export. Sverige har däremot inga importrestriktioner avseende krypteringsprodukter.

8.10.2 Riktlinjer/föreskrifter med juridisk anknytning som bör utarbetas

- Behörighetsregler
- Sekretessregler
- E-post och Internetanvändning
- Användning och inköp av programvara
- Hantering av överträdelser

8.11 Författarnas kommentarer

När vi har gått igenom standarden och jämfört med vad vi läst i övrig litteratur kan vi konstatera att den täcker in de delar som anses innefattas i begreppet informationssäkerhet. Vi tycker att standarden ska följas vid en vidareutveckling av IMIS och vi kommer att följa den i detta arbete.

Standarden kan verka oerhört komplex och det är lätt att tänka: Vem ska ha tid att gå igenom och utföra allt detta? Hur ska man kunna bekosta ett arbete att säkra ett projekt enligt ISO-standarden? Vi tror, att de pengar som inte satsas på detta arbete nu, kommer man att få lägga i senare skede på de problem som kommer att uppstå. Tiden kommer också att gå åt till att reda ut problem istället för till proaktivt arbete.

Det är viktigt att komma ihåg, att i ett litet projekt blir inte informationssäkerhetsarbetet så tidskrävande och kostsamt, det är dock ändå viktigt att alla punkter i standarden kontrolleras så att ingen viktig del glöms bort.

Vi är av den uppfattningen att det är bra om många verksamheter använder samma modell för sitt informationssäkerhetsarbete. Om det är så, får man en gedigen kunskapsbas att använda vid vidareutveckling och förbättring. Det bör vara ett krav tycker vi att alla som hanterar skyddsvärd information ska använda denna standard.

SS-ISO/IEC 177 99 förespråkar användarutbildning och vi instämmer. Att genomföra användarutbildningar är en relativt enkel och effektiv men framförallt billig metod som därför passar utmärkt till IMIS.

9 GENERELL BESKRIVNING OM RISKANALYSARBETE

Kapitel nio är till för de läsare som inte sedan tidigare har kunskap om vad riskanalysarbete innebär. Kapitlet beskriver grundläggande vad en riskanalys är och varför det är viktigt för en organisation att genomföra den. Här tas även upp olika metoder för riskanalysarbete. Som avslutning redovisas intervjuer som berör riskanalys samt författarnas kommentarer.

9.1 Grundläggande om riskanalys

Definition av en risk är ”någon eller något som skapar eller utgör en fara” [10]. En riskanalys ger en organisation/projekt möjligheten att ta kontroll över dess framtida resultat. En analys bör genomföras så fort nya uppgifter, projekt eller idéer ska utformas eller utvecklas.

För att en riskanalys ska vara effektiv måste processen accepteras som en del i en organisations/projekts utveckling.

Riskanalysarbete innebär att fastställa följande [8], [10]:

- Vilka informationstillgångar har verksamheten?
- Vilka informationstillgångar behöver skyddas?
- Vilka specifika hot finns till respektive tillgång?
- Vilken skada skulle respektive tillgång kunna innebära om respektive hot skulle inträffa?
- Vilken prioritet har respektive tillgång med tanke på risk, skada och kostnad?

Syftet med att utföra en riskanalys är att utvärdera aktiviteter och bestämma relevanta åtgärder för genomförandet av dessa.

Målet med en riskanalys är inte att eliminera alla risker utan att minska riskerna till en acceptabel nivå [10]. Vad som är en acceptabel nivå bestäms av legala krav, ekonomiska övervägande, rättspolitiska faktorer och tidigare erfarenheter inom en organisation [12].

9.2 Riskanalysmetoder

Det finns många metoder att använda vid genomförandet av en riskanalys. De metoder som är mest populära är de som är relativt enkla, de som fungerar i olika typer av organisationer oavsett storlek och de som involverar personer som har kunskaper inom alla område som berör aktuellt objekt [10].

Kvalitativ och kvantitativ är de två kategorier som riskanalysmetoder ofta delas in i. Den metod som har mest fördelar är den kvalitativa.

9.2.1 Kvalitativ riskanalysmetod

Genom att genomföra en kvalitativ riskanalys bestäms vilken nivå av skydd som behövs för program, system, inrättningar o s v inom en organisation. Metoden innebär att en noggrann undersökning av tillgångar, hot och sårbarhet genomförs. Syftet med undersökningen är att ta reda på hur stor risken är att hot verkligen inträffar, eventuella kostnader som hot skulle medföra och vilka säkerhetsåtgärder som behövs för att minska hot till en acceptabel nivå. Nackdelen med den kvalitativa metoden är att den är subjektiv, trots detta är det denna metod som rankas högst [10]. Nedan följer en 10-stegsmodell av en kvalitativ riskanalysmetod [10]. Denna ligger som grund för många andra kvalitativa riskanalysmetoder.

Steg 1: Utveckla en arbetsbeskrivning

För att kunna genomföra en lyckad analys krävs det att det tas fram en definition över målet med arbetet. Vad som ska undersökas och hur? Vem är ansvarig för den del

som ska undersökas och vilka avgränsningar som ska hållas på det som ska undersökas?

Steg 2: Ta ut kompetent arbetsteam

I den kvalitativa processen är det viktigt att ett kompetent team tas fram som ska utföra analysen. För att analysen ska bli mest effektiv rekommenderas att personer från följande områden är inblandade:

- ägare/ansvarig
- användare
- systemanalys
- applikationsprogrammering
- databasadministration
- fysisk säkerhet
- nätverk
- juridik
- operationssystem
- informationssäkerhet
- underhåll

Steg 3: Identifiera hot

Den huvudsakliga uppgiften i processen är att identifiera vilka hot som kan göra skada inom det område som undersöks. Det finns många metoder för att genomföra detta steg men den som anses mest effektivt är om medlemmarna i teamet brainstormar fram idéer som sedan kategoriseras. Alla steg i analysen förs efter varje steg in i en tabell över de beslut som fattas angående riskfaktorerna.

Steg 4: Prioritera hot

När hoten är identifierade gäller det att prioritera dem. Hoten ordnas efter hur ofta det är troligt att de inträffar. Varje hot får ett nummer (oftast på en skala mellan 1 och 5) som visar om risken är stor eller liten som sedan förs in i tabellen.

Steg 5: Kartlägg konsekvenser

Steg fem går ut på att undersöka och klartlägga vilka konsekvenser inträffade hot skulle innebära. Även i detta steg ges varje hot ett nummer som förs in i tabellen.

Steg 6: Beräkna riskfaktor

I steg sex används de nummer som förts in i tabellen under varje steg till att beräkna varje hots riskfaktor. Varje hots resultat ordnas sedan från det högsta värdet till det lägsta. Värdena hamnar mellan 2 och 10 och desto högre riskfaktor ett hot får ju desto högre säkerhetsåtgärder krävs.

Steg 7: Identifiera säkerhetsåtgärder

De hot som fått högre värde än 6 i steg sex tas vidare till steg sju för att identifiera säkerhetsåtgärder för respektive hot. Åtgärden som tas fram ska innehålla tekniska, administrativa och fysiskt möjliga delar till en ekonomiskt acceptabel nivå i förhållande till det som undersöks.

Steg 8: Kostnadsanalys

Det viktigaste steget i riskanalysen är att göra en kostnadsanalys. Varje skyddsåtgärd kostar pengar och i steg åtta beräknas denna summa och förs in i åtgärdstabellen till respektive hot. Målet är att identifiera de åtgärder som erbjuder de bästa skyddet till minst summa pengar.

Steg 9: Prioritera säkerhetsåtgärder

När åtgärderna är framtagna och beräknade måste de prioriteras eftersom resurser ofta är begränsade. Denna prioritering ligger till grund för vad som kommer att åtgärdas och i vilken ordning.

Steg 10: Riskanalysrapport

Syftet med att skriva en riskanalysrapport är att rapportera resultatet och att organisationen kan arkivera den för framtida behov. När riskanalysen är genomförd är det upp till organisationen att ta beslut om vad som verkligen ska åtgärdas.

9.3 Intervjuer som berör riskanalys

Resultatet av intervjuundersökning med Typ A visar att riskanalysarbete inom landstinget Blekinge inte involverat vårdcentraler och sköterskor. Kunskapen om riskanalyser är mycket begränsad.

9.4 Författarnas kommentarer

En kvalitativ riskanalysmetod som finns beskriven, förespråkas i litteratur och i TIHS.

Vi ifrågasätter hur landstinget genomför riskanalysarbete, eftersom de sköterskor vi intervjuat inte varit involverade eller ens kände till vad riskanalysarbete innebär. Ett övergripande riskanalysarbete tycker vi bör vara känt inom alla verksamheter och avdelningar inom landstinget.

10 KRAVSPECIFIKATION FÖR INFORMATIONSSÄKERHETSARBETE FÖR HÄLSO- OCH SJUKVÅRDSSYSTEM – IMIS EN FALLSTUDIE

Här utformas och anpassas en kravspecifikationen lämplig för informationssäkerhetsarbete för hälso- och sjukvårdssystem. Kravspecifikationen tas fram genom en fallstudie av IMIS enligt de teoretiska delar som tidigare beskrivits i arbetet samt rekommendationer från författarna.

Vissa delar i informationssäkerhetsarbete ska genomföras i grupper där berörda parter samarbetar, ledning, tekniker, säkerhetsansvariga, jurister och slutanvändare [7], [13], [18]. Detta bör beaktas vid vidareutveckling av IMIS.

Kravspecifikationen för informationssäkerhet till IMIS kan användas som underlag vid vidareutveckling av IMIS.

10.1 Arkitektur för IMIS

IMIS är ett internetbaserat system som består av en webserver och en databas, enligt bild 11. Förslaget över systemarkitekturen innefattar komponenterna säker arbetsstation, nätverkssäkerhet, organisationssäkerhet och informationssäkerhet [kap 3].

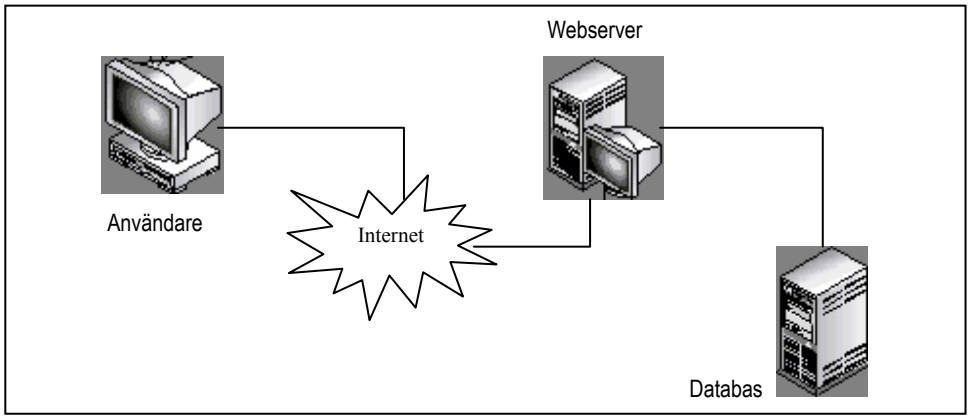

Bild 11: Systemarkitektur för IMIS

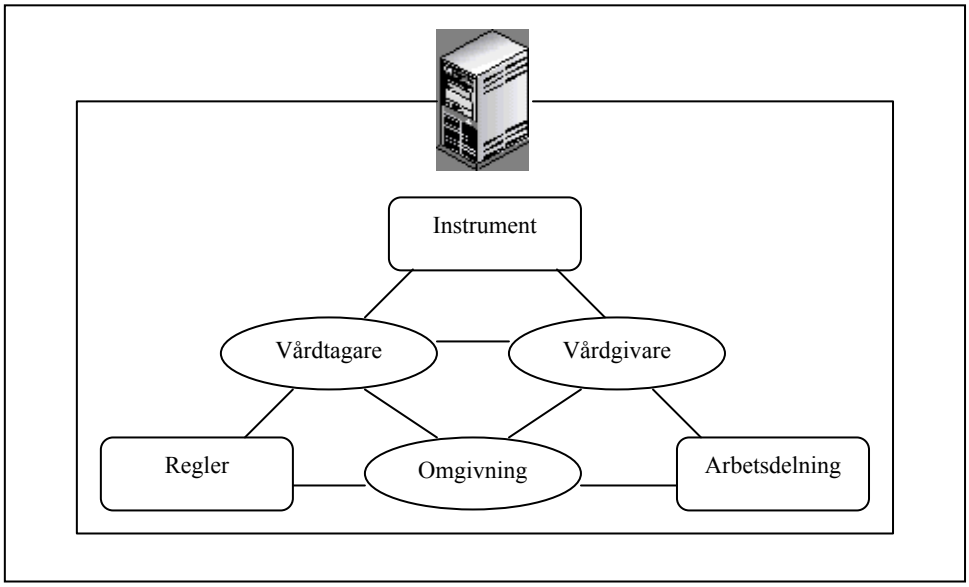

Bild 12: Analysstruktur i IMIS enligt Engeströms aktivitetsteori

10.2 Framtida förvaltning av IMIS

Vid en fortsättning och vidareutveckling av IMIS [kap 2], rekommenderas att IMIS databas ska förvaltas av en utomstående specialist. Som exempel kan nämnas att Sigma förvaltar databaser åt landstinget Blekinge.

Fördelen med en sådan lösning är att kunskap gällande hantering och lagring av information kan delegeras till specialister.

10.3 Nyttoanalysen för IMIS

Nyttoanalys bör göras för IMIS. Ledning och säkerhetsansvariga bör genomföra analysen för att skapa förståelse för informationssäkerhetsarbetets betydelse och för IMIS specifika behov. I nyttoanalysen ska osäkerheter och brister undersökas enligt faktorer i kapitel 7.3.1.

Resultatet ska sammanställas och dokumenteras. Dokumentet blir underlag för beslut att initiera ett säkerhetsarbete.

När ledningen uttalat sitt stöd för informationssäkerhetsarbete, blir nästa steg att ta fram en informationssäkerhetspolicy.

10.4 Organisationsövergripande informationssäkerhetsarbete för IMIS

10.4.1 Informationssäkerhetspolicy

Informationssäkerhetsarbetet är en viktig del för IMIS och för att veta vilka mål som finns för arbetet måste det finnas en policy. Den bör utarbetas av projektets säkerhetsansvariga och beslutas av ledningen. När policyn är godkänd ska alla inblandade i projektet delges innehållet. En ägare ska utses som ansvarar för underhåll och vidareutveckling av policyn. Det bör också ske en periodisk översyn.

Som stöd för utarbetandet av en informationssäkerhetspolicy rekommenderas kapitel 3 i Handbok i Informationssäkerhetsarbete som har tydliga instruktioner om hur en policy bör utformas.

10.4.2 Övergripande riktlinjer för informationssäkerhet

En övergripande riskanalys [kap 7 och 9] bör utföras för IMIS-projektet. Resultatet av den pekar på vilka specifika behov som finns och visar om informationssäkerhetspolicyn är verksamhetsanpassad.

Riskanalysen bör genomföras av representanter för projektets ledning och personer med kompetens inom säkerhet, teknik och kvalitet. Utifrån resultatet kan riktlinjer som hanterar befintliga hotbilder utformas.

10.4.3 Lokala riktlinjer för informationsklassificering

Representanter för den kliniska verksamheten (sköterskor och läkare) bör diskutera vilket skyddsbehov som finns för den information som ska hanteras i IMIS. Därefter fattas beslut av den medicinska ledningen. Som medicinsk ledning bör IMIS ha en ansvarig läkare som har yttersta ansvar för information som hanteras i IMIS. Ansvarig läkare avgör rimligt skyddsbehov för verksamheten. De riktlinjer som beslutas gälla, används senare av informationsägarna för att klassificera informationsobjekten i varje kartlagt användningsfall.

För att få ett rimligt antal klasser i de olika bedömningarna bör TIHS rekommendationer för informationsklassificering följas [kap 7]

Klass	Insynsskydd	Spårbarhet	Tillgänglighet	Riktighet
1	Ej känslig information	Spårbarhet ej viktigt för informationsobjekt	Låga krav på tillgänglighet för informationsobjekt	Låga krav på riktighet för informationsobjekt
2	Känsligt informationsobjekt	Spårbarhet skall finnas på informationsobjekt	Höga krav på tillgänglighet för informationsobjekt	Höga krav på riktighet för informationsobjekt
3	Hög känslighet på informationsobjekt	Spårbarhet med mycket hög tillförlitlighet	Mycket höga krav på tillgänglighet för informationsobjekt	Mycket höga krav på riktighet för informationsobjekt
4	Mycket hög känslighet på informationsobjekt			

Bild 13: Tabell över riktlinjer för informationsklassificering [18, figur 9]

Bedömningsgrunder för lokala riktlinjer

För att definiera vilken konkret information som ska tillhöra respektive klass bör diskussionen föras enligt nedanstående bedömningsgrunder [23].

Vid bedömning av *insynsskydd* rekommenderas att diskutera efter följande bedömningsgrunder:

- Olika hög grad av insynsskydd kan behövas beroende på var informationen uppkommit
- Grad av skydd varierar med vad informationen innehåller. Är det diagnos, klinisk bedömning eller annan detaljerad information påverkas klassificeringen
- Vissa typer av uppgifter kan ses som rutinmässiga och vissa kan vara extremt känsliga

Även sekretessbelagd information kan ha olika grader av skyddsbehov.

Vid bedömning av *spårbarhet* rekommenderas att diskutera efter följande bedömningsgrunder:

- Gäller spårbarheten kvalitetsfrågor
- Gäller spårbarheten möjlighet att ta fram statistikuppgifter
- Är det viktigt att spåra personalaktiviteter kring vissa data
- Är det viktigt att styrka personalen aktiviteter
- Har tidsfaktorn betydelse

Vid bedömning av *tillgänglighet* rekommenderas att diskutera efter följande bedömningsgrunder:

- Gäller det akut vård. I de fall informationsobjektet används i flera fall ska det klassa efter det som är mest akut
- Har tillgängligheten betydelse för andra kliniska verksamheter
- Är den viktig för patientens vård/omhändertagande

Vid bedömning av *riktighet* rekommenderas att diskutera efter följande bedömningsgrunder:

- Behövs indikation på att information förvanskats
- Hur viktig är informationen för patientens vård
- Har informationen betydelse för andra kliniska verksamheter
- Gäller höga kvalitetskrav

10.5 Informationssäkerhetsarbete för användningsfall i IMIS

I detta avsnitt visas exempel för att förtydliga tillvägagångssätt vid identifiering, kartläggning och klassificering av informationsobjekt och tekniskt skydd. Ett rätt förfarande enligt TIHS-metoden kräver att informationsägare, tekniker, säkerhetsansvariga och användare samarbetar i hela processen med användningsfall [kap 7].

10.5.1 Identifiering av användningsfall

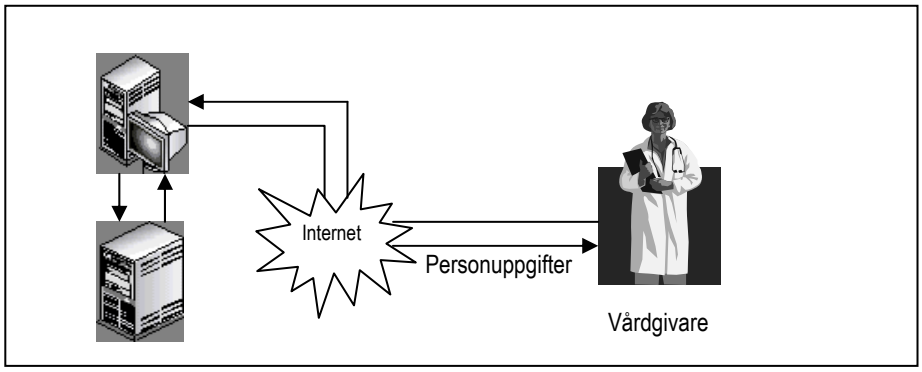

Bild 14: Användningsfall - Läsa personuppgifter

För att exemplifiera identifiering av ett användningsfall i IMIS har vi valt ut funktionen att vårdgivare läser personuppgifter från databasen – Vårdtagare. Funktionen att läsa personuppgifter finns i IMIS första kravspecifikation för funktioner i IMIS-prototypen.

10.5.2 Kartläggning av användningsfall

Kartläggning av användningsfall bör genomföras vid vidareutveckling av IMIS, en kartläggning för varje användningsfall. Personer som ska ingå vid kartläggningen av användningsfallet *läsa personuppgifter* är informationsägare, vårdgivare, tekniker och säkerhetsansvariga.

Intressenter i aktuellt användningsfall:
Vårdgivare

Beskrivning av verksamhetsprocess i aktuellt användningsfall:
Informationsägaren, vårdgivare, tekniker och säkerhetsansvariga ska diskutera processen som rör autenticering av vårdgivare enligt SITHS-modellen, inloggning i IMIS samt funktionen att läsa personuppgifter. Resultatet ska dokumenteras och fungera som underlag vid eventuell riskanalys.

Identifiering av informationsobjekt i aktuellt användningsfall:
Vårdtagares personuppgifter

Teknisk beskrivning av aktuellt användningsfall:

- Teknisk utrustning kring certifikathantering, enligt SITHS-modellen
- IMIS
- Webserver
- Databas (vårdtagare) med inbyggd säkerhetsfunktion för att hantera användarvyer
- Kryptering ska tillämpas vid transport av information
- Brandväggar
- Antivirusskydd för vårdgivares arbetsstation och webserver

10.5.3 Klassificering av informationsobjekt och tekniskt skydd

Informationsobjekt ska klassificeras av informationsägare och användare, enligt de lokala riktlinjer som tagits fram för IMIS.

Lokala riktlinjer gällande tekniskt skydd för IMIS ska tas fram av informationsägare och tekniker, enligt exempel i tabellen nedan [23]. Riktlinjer för tekniskt skydd ska tas fram för insynsskydd, tillgänglighet, spårbarhet och riktighet.

Insynsskydd

Klass	*Bedömning*	*Tekniskt Skydd*
Klass 1	• Innefattar information som inte är sekretessbelagd och ej går att härleda till någon person.	• Inget tekniskt stöd
Klass 2	• Innefattar sekretessbelagd information som kräver relativt lågt behov av skydd t ex blodsockervärde.	• Teknikiskt stöd för insynsskydd
Klass 3	• Innefattar sekretessbelagd information som kräver högt behov av skydd som är känsligt för aktuell patient t ex personuppgifter eller hälsotillstånd.	• Tekniskt stöd och rutiner som tillsammans ger ett högt insynsskydd
Klass 4	• Innefattar sekretessbelagd information som inte överhuvudtaget ska hanteras digital som är ytterst känsligt för aktuell patient.	• Ej aktuellt för bedömning av tekniskt skydd

Bild 15: Författarexempel på riktlinjer för insynsskydd

Tekniskt skydd ska klassificeras av tekniker som har kunskap om IMIS programvara och tekniska resurser, enligt de lokala riktlinjer som tagits fram.

I de fall bedömningen för informationsobjekt inte stämmer överens med bedömningen för tekniskt skydd ska efterföljande steg riskanalys och riskhantering genomföras. Exempelvis kräver informationsobjektet P*ersonuppgifter* klass 3 för insynsskydd, vilket enligt tekniker kan visas vara omöjligt att uppnå med den tekniska utrustning som finns tillhanda. I detta fall ska en riskanalys genomföras. Resultatet av riskanalysen kan då visa att ett inköp av säkrare utrustning är nödvändig och därmed gör det möjligt att kunna garantera att klass 3 efterföljs för personuppgifter när det gäller insynsskydd.

10.5.4 Riskanalys

Riskanalys inom IMIS ska göras för de delar som tagits fram efter klassificeringen av informationsobjekt och tekniskt skydd. Riskanalysen bör i sin tur eventuellt resultera i område som kräver riskhantering. För att risker inom alla områden ska tas upp för diskussion och behandlas enligt riskanalysen olika steg ska en riskanalys i IMIS. I aktuellt användningsfall involveras följande personer:

- informationsägare
- metodledare
- tekniker
- säkerhetsansvariga
- vårdgivare

10.5.5 Riskhantering

Om en genomförd riskanalys för IMIS resulterar i en riskhantering för några områden, ska en handlingsplan för dessa områden skrivas och följas. Ledningen för IMIS ska ta beslut om vilka punkter i handlingsplanen som ska genomföras.

10.6 Punkter i SS-ISO/IEC 17799 som berör IMIS

Följande avsnitt tar upp de punkter i SS-ISO/IEC 17799 som inte ingår i TIHS men berör IMIS-projektet. Här ges rekommendationer för hur arbetet med IMIS ska anpassas enligt standarden. Rekommendationerna gäller för de delar av IMIS-projektet som inte berör landstingets personal och utrustning. I de punkter som gäller personal och utrustning förutsätts att landstinget följer standardens rekommendationer.

10.6.1 Klassificering och kontroll av tillgångar

Kapitel fem i ”Handbok för Informationssäkerhet” behandlar klassificering och kontroll av tillgångar. Här nämns endast punkten *märkning av information* från avsnittet ”Klassificering av information” eftersom den inte tas upp i TIHS.

Klassificering av information

Punkten *märkning och hantering av information* bör följas i IMIS då stora delar av informationen i systemet är känslig och hanteringen av den i många fall är reglerad i lag.

10.6.2 Personal och säkerhet

Kapitel sex i ”Handbok för Informationssäkerhet” behandlar personal och säkerhet.

Säkerhet i beskrivning av befattningar och vid rekrytering och omplacering

Standarden rekommenderar att en riskprofil ska tas fram för varje befattning som hanterar känsligt material. I IMIS rekommenderas att personer på befattningarna personuppgiftsansvarig och databasadministratör kontrolleras noggrant. Personer med dessa befattningar kommer att ha ansvar för, och tillgång till mycket känslig information.

För varje tjänst som ingår i IMIS-projektet bör befattningsbeskrivning skrivas.

Vid rekrytering av personal eller vid nyanställningar till IMIS-projektet, bör rekommendationer i standarden följas. Vid rekrytering och nyanställningar för befattningarna personuppgiftsansvarig och databasadministratör är detta speciellt viktigt. Eftersom IMIS är ett system som hanterar sekretessbelagd information krävs att en allmän kontroll görs av all personal.

Ett tydligt sekretessavtal, med tydliga disciplinära åtgärder, ska definieras enligt standarden. Avtalet ska gälla för samtlig personal som berörs av eller arbetar med IMIS-projektet. Information om IMIS, arkitektur, teknik mm, får inte komma till obehörigs kännedom.

Punkterna *anställningsvillkor och anställningsförhållande* bedöms inte beröra IMIS-projektet.

Användarutbildning

Utbildningar som rekommenderas i detta avsnitt ska påbörjas så tidigt som möjligt i IMIS-projektet. Utbildningen garanterar att alla känner till vad informationssäkerhet innebär, och det ansvar som åligger varje användare för att upprätthålla god säkerhet.

Nivå	Deltagare	Innehåll	Syfte
1.	Ledning, personal och användare	Generell kunskap om informationssäkerhet • Vad är informationssäkerhet? [kap 3] • Vilka hot och risker finns? [kap 3, 5] • Juridisk informationssäkerhet, generellt samt speciellt för hälso- och sjukvård [kap 4, 10.6.9]	Öka medvetenhet inom området informationssäkerhet och för att ledning, personal och användare ska känna delaktighet i säkerhetsarbetet.
2.	Ledning och personal inom IMIS-projektet	Informationssäkerhet i praktiken • Genomgång av informationssäkerhetspolicy och rutiner • Hot och risker ur användarsynpunkt [kap 5] • Ansvar och skyldigheter för användare [kap 5]	Ledning och personal ska ta ansvar för att följa informationssäkerhetspolicyn. Ledning och personal får kunskap om vilka risker och hot som finns för kategorin användare och hur riskerna kan förebyggas.
3.	Patient, sköterskor och läkare	Informationssäkerhet i praktiken för användare • Informera om delar i informationssäkerhetspolicyn som berör användare • Hot och risker ur användarsynpunkt [kap 5] • Ansvar och skyldigheter för användare [kap 5] • Information och användande av eID-kort och certifikat [kap 6]	Användare ska ta ansvar för att följa de delar i informationssäkerhetspolicyn som berör användare. Användare får kunskap om vilka risker och hot som finns för kategorin användare och hur riskerna kan förebyggas.
4.	Patient, sköterskor, läkare och ev. andra berörda personer	Användarutbildning i systemet IMIS • Information om systemet • Praktisk hantering av funktioner t ex inloggning	Användare ska få information och systemet och hur dess olika funktioner fungerar.

Bild 16: Schema över lämplig utbildning för involverade i IMIS-projektet

Säkerhetsincidenter och funktionsfel

Punkterna *rapportering av säkerhetsincidenter*, *rapportering av svagheter avseende säkerhet, rapportering av funktionsfel, att lära av incidenter* och *disciplinär process* bör följas enligt standarden.

Information om disciplinära åtgärder vid brott mot säkerhetsbestämmelser bör finnas med i utbildning nivå 2 och 3.

10.6.3 Fysisk och miljörelaterad säkerhet

Kapitel sju i ”Handbok för Informationssäkerhet” behandlar fysisk och miljörelaterad säkerhet. Det som rekommenderas för IMIS i detta avsnitt, gäller endast för den del av arkitekturen som finns till höger om den grå linjen i bilden.

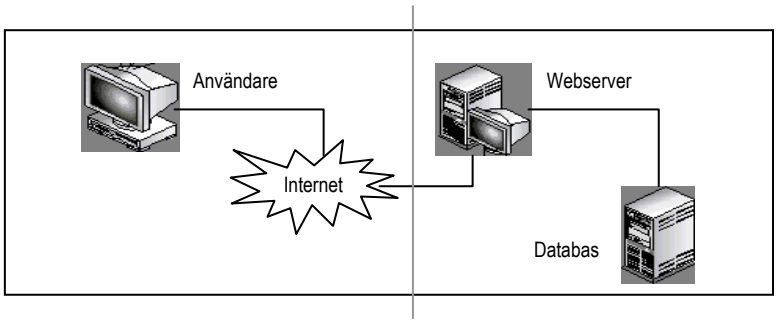

Bild 17: Bild över delar i IMIS arkitektur som berörs i kapitel 10.6.3.

Säkrade utrymmen

Här är det lämpligt att följa vad standarden beskriver angående *skalskydd, tillträdeskontroll, skydd av kontor* och *arbete i säkrade utrymmen*. En punkt som inte bedöms gälla alls för IMIS är *avgränsade utrymmen för godsmottagning och lastning*, det bedöms inte heller nödvändigt med tv-övervakning i säkrade utrymmen.

Patienters arbetsstationer kan var mobila eller fasta och det förutsätts att de skyddads av patienterna.

Skydd av utrustning

Stora delar av den information som hanteras i IMIS är sekretessbelagd. Det får till följd att vad det gäller *placering och skydd av utrustning, elförsörjning, kablageskydd, underhåll av utrustning, säkerhet för utrustning utanför egna lokaler* och *säker avveckling eller återanvändning av utrustning*, ska standarden följas för IMIS-projektet.

I utbildning nivå 2 och 3, bör det ingå information om hur utrustning bör placeras, skyddas och underhållas.

Allmänna åtgärder

Standardens punkter, *policy för städat skrivbord och tom bildskärm* och *avlägsnande av egendom* gäller för IMIS.

I utbildning nivå 2 och 3 bör det diskuteras hur skyddad information ska hanteras när den inte används.

10.6.4 Styrning av kommunikation och drift

Kapitel åtta i ”Handbok för Informationssäkerhet” behandlar styrning av kommunikation och drift.

Driftrutiner och driftansvar

Standardens punkter *dokumenterade driftrutiner, styrning av ändringar i drift, rutiner för incidenthantering, uppdelning av arbetsuppgifter, uppdelning av utvecklings- och driftresurser* är aktuellt för IMIS. Den del som gäller hantering av *externa resurser* är inte aktuell för IMIS-projektet men kan möjligen bli det i ett senare skede.

Systemplanering och systemgodkännande

För IMIS finns behov av såväl *kapacitetsplanering* som *systemgodkännande* enligt standardens rekommendationer. Hur lång framtida utveckling som ska tas hänsyn till i kapacitetsplaneringen, bör diskuteras av tekniker och ledning.

Skydd mot skadliga program

Förebyggande åtgärder mot skadliga program som beskrivs i standarden, rekommenderas för att ge IMIS-användande optimal säkerhet.

Policyn med förbud att använda icke godkända program, kan lämpligen presenteras i samband med utbildning nivå 2 och 3. Diskussion kring lämpligt skydd av antivirusprogram bör tas upp i utbildning nivå 2 och 3.

Ordning och reda

Punkten s*äkerhetskopiering* är endast aktuellt för hanteringen av IMIS databas, standardens rekommendationer bör följas.

Felloggar bör finnas. *Operatörsloggar* måste finnas på grund av att hantering av information i IMIS till stora delar är reglerad i lag. Loggarnas funktion styrs enligt lagar och informationsklassificeringen [23], [kap 10.5.3]

Styrning av nätverk

För IMIS gäller högsta möjliga säkerhetskrav för att reglera åtkomst på grund av det höga skyddsvärdet i den information som hanteras. Styrmedel för nätverk som beskrivs i standarden gäller för IMIS.

Speciellt för IMIS gäller att webservern inte ska ingå i något nätverk, den ska endast vara ansluten till databasen. Databasen ska vara av den typ som har en inbyggd säkerhetsfunktion, vilket innebär att det går att skapa olika vyer för olika typ av användare.

Brandvägg bör installeras enligt bild och åtkomst regleras enligt rutiner för åtkomst [kap 10.6.5]. För att öka säkerheten i IMIS är det önskvärt att brandväggen är en router eftersom det skulle minska risken för externa inkräktare.

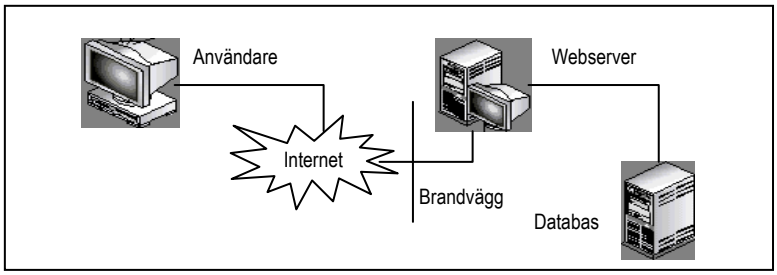

Bild 18: IMIS arkitektur med brandvägg

Mediahantering och mediasäkerhet samt kontroll över flyttbara medier

Standardens punkter, *avveckling av media, rutiner för informationshantering och säkerhet för systemdokumentation* gäller för IMIS. Rutiner för informationshantering och avveckling av media, är av yttersta vikt på grund av den höga skyddsnivån på information som hanteras och lagras i IMIS.

Utbyte av information och program

Här gäller endast punkten *säkerhet för elektronisk post*. I övrigt bedöms standarden inte beröra IMIS.

För patientanvändare kan det ingå information om risker med e-post och riktlinjer för säker e-posthantering i utbildning nivå 2 och 3.

10.6.5 Styrning av åtkomst

Kapitel nio i ”Handbok för Informationssäkerhet” behandlar styrning av åtkomst.

Verksamhetskrav på styrning av åtkomst

I informationssäkerhetspolicyn för IMIS ska riktlinjer för tilldelning och fråntagning av åtkomsträttigheter tas upp. Rekommendationen för IMIS är obligatorisk styrning.

Lagen om yrkesverksamhet inom hälso- och sjukvård och sekretesslagen reglerar åtkomst. Lagarnas påverkan på denna punkt bör utredas av jurist.

Styrning av användares åtkomst

Punkten *användarregistrering* ska följa standarden. Vid identifiering av användare i IMIS rekommenderas att detta utförs med hjälp av kryptografisk modell t ex ett eID-kort [kap 6]. EID-kortet ska innehålla uppgifter om användaren för identifiering i systemet. Ett förslag är att använda Secure Office från Steria i inledningsfasen i IMIS [28]. Secure Office är en heltäckande IT-säkerhetsplattform som är anpassad för användning av olika PKI-lösningar. Detta är upp till ledningen att besluta eftersom det medför en kostandsfråga.

Åtkomststyrningen för sköterskor och läkare kommer, enligt den avsiktsförklaring som landstinget skrivit på, så småningom styras enligt SITHS-modellen och certifikat för hälso- och sjukvård [kap 6].

Punkterna *styrning av lösenord för användare* och g*ranskning av användares åtkomsträttigheter* ska följas enligt standarden.

Användares ansvar

Punkten *användning av lösenord* ska följa standarden och tas upp i utbildning nivå 2 och 3.

Vid användning av IMIS ska systemet aldrig lämnas obemannat utan tillsyn. Inloggning och skärmsläckare ska därför anpassas för att skydda IMIS.

Styrning av åtkomst till nätverk

Detta avsnitt bedöms inte beröra IMIS.

Styrning av åtkomst till operativsystem

Punkten *automatisk terminalidentifikation* kommer inom landstinget till viss del att hanteras enligt SITHS-modellen via certifikat och eID-kort. I inloggningsproceduren till IMIS bör en säkerhetsfunktion byggas in som tillåter max tre inloggningsförsök. Vid fler försök bör en logg skickas automatiskt enligt ordinarie loggrutiner för IMIS.

Punkten *påloggningsrutin för personal* regleras enligt SITHS-modellen. För övrigt ska standarden följas.

Punkterna *identifiering och autenticering av användare, lösenordsrutin* och *användning av systemhjälpmedel* ska följas enligt standarden [kap 6].

Automatisk utloggning och nedkoppling bör vara implementerad i IMIS för att förhindra obehörig åtkomst.

Punkten *begränsad uppkopplingstid* är inte applicerbar på IMIS.

Styrning av åtkomst till tillämpningar

Punkten *begränsning av åtkomst till information* ska följas enligt standarden.

Punkten *isolering av känsliga system* ska följas och anpassas för IMIS i enlighet med arkitekturen i bild x.

Övervakning av systemåtkomst och systemanvändning

Punkterna *loggning av händelser, övervakning av systemanvändning* och *klocksynkronisering* ska följas enligt standarden.

Åtkomst vid distansarbete och mobilanvändning

Om IMIS ska användas i handdatorer ska information om mobilt användande ingå i utbildning nivå 2, 3 och 4.

Hälso- och sjukvård ställer stora krav på mobil utrustning och användande, därför bör denna punkt få stor uppmärksamhet när och om användandet av mobila enheter ska tillämpas i IMIS. Tekniker och ledning bör undersöka vad mobil användning innebär och tillämpa lösningar som uppfyller gällande säkerhetskrav.

Punkten *distansarbete* i standarden kan jämföras med patienters användning av IMIS och ska följas enligt standarden. Punkten ska tas upp i utbildning nivå 3.

10.6.6 Systemutveckling och systemunderhåll

Kapitel tio i ”Handbok för Informationssäkerhet” behandlar systemutveckling och systemunderhåll.

Säkerhetskrav på system

Enligt standarden är informationssäkerhet oerhört viktigt redan vid utvecklingen av system. Rekommendationer enligt denna kravspecifikation för informationssäkerhet i IMIS bör därför följas vid utvecklingen av IMIS. Under hela utvecklingen av IMIS ska tekniker och säkerhetsansvariga samarbeta enligt bild x., oavsett vilken utvecklingsmodell som används.

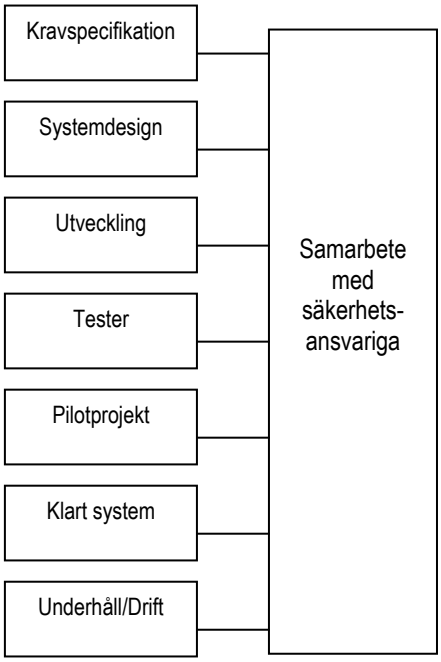

Bild 19: Rekommenderad designmetod [7], anpassad för IMIS.

Säkerhet i tillämpningssystem

Rimlighetskontroll av in- och utdata data bör implementeras i IMIS.

Kryptering

För att öka säkerheten i IMIS bör olika typer av kryptering tillämpas. Sekretessbelagd information som hanteras i IMIS ska krypteras vid transport. Informationsklassificering och klassificering av tekniskt skydd ska beaktas vid val av krypteringsmetod och teknisk utrustning.

Säkerhet i databaser och filer

Databasen ska vara av den typ som har en inbyggd säkerhetsfunktion, vilket innebär att det går att skapa olika vyer för olika typ av användare.

Tester och underhåll av vald databas ska genomföras och dokumenteras. Tester bör, enligt standarden utföras på kopior av databasen som sedan kan raderas. System och programändringar ska dokumenteras för att kunna spåras.

Säkerhet vid utveckling och underhåll

Vid utveckling och underhåll av IMIS ska rutiner finnas för vem som har befogenhet att göra ändringar, kontroll av hur systemets olika delar påverkas ska genomföras, uppdatering av styrdokument ska genomföras, eventuell uppdatering av drift- och användardokumentation samt arkivering av äldre version av IMIS ska genomföras.

10.6.7 Kontinuitetsplanering

Kapitel elva i ”Handbok för Informationssäkerhet” behandlar kontinuitetsplanering.

Standarden verkar på denna punkt vara skriven för en stor organisation, därför ges följande förslag till kontinuitetsplanering för IMIS.

En avbrotts och konsekvensanalys bör genomföras i samband med riskanalys. Resultatet kan användas som underlag för en handlingsplan för avbrott där också reservrutiner dokumenteras. Handlingsplanen ska godkännas av IMIS ledning.

Test av handlingsplanen bör genomföras och den ska också uppdateras i samband med återkommande riskanalyser, då är det också lämpligt att kontrollera att det finns resurser att genomföra planen.

10.6.8 Efterlevnad

Kapitel tolv i ”Handbok för Informationssäkerhet” behandlar efterlevnad.

Efterlevnad av rättsliga krav

För IMIS rekommenderas att ledning och säkerhetsansvariga går igenom följande punkter i standarden, *identifiering av lämpliga bestämmelser, skydd av organisationens register och handlingar, skydd av persondata* och *missbruk av informationsbehandlingsresurser*. Detta bör göras på ett tidigt stadium i IMIS-projektet för att säkerställa att juridiska krav uppfylls igenom hela projektet.

Instruktioner bör upprättas om hur organisationens utrustning får användas likaså rutiner för att upptäcka missbruk av desamma.

Punkterna i*mmaterialrätt* och *reglering av kryptering* aktualiseras efter hand som behov uppkommer.

Granskning av säkerhetspolicy och teknisk efterlevnad

Den som ansvarar för informationssäkerhetspolicy för IMIS, bör ta ansvar för punkten *efterlevnad av säkerhetspolicy* och anpassa den till IMIS-projektet. Den teknikansvariga bör ansvara för punkten *kontroll av teknisk efterlevnad* och anpassa den till IMIS-projektet.

Hänsynstagande vid revision av system

I dagsläget kan avsnittet inte relateras till IMIS-projektet. Bör undersökas vid vidareutveckling av denna kravspecifikation.

10.6.9 Lagrum

Kapitel tretton i ”Handbok för Informationssäkerhet” behandlar lagrum, efterlevnad av rättsliga krav.

Lagrum tar upp de lagar som berör IMIS-projektet. De beskrivs kortfattat. Vid vidareutveckling av IMIS ska jurister med specialkunskap inom hälso- och sjukvård konsulteras.

Alla lagar som berör IMIS-projektet ska lagras i fulltext i databasen - Regler.

Hälso- och sjukvårdslagen (1982:763)

Hälso- och sjukvårdslagen tar upp målet med hälso- och sjukvård som innebär en god hälsa och vård på lika villkor. I lagen tas även krav upp över hur en god vård ska utföras. Landstingens och kommuners ansvar i hälso- och sjukvård definieras samt att ledning inom hälso- och sjukvård ska kunna tillgodose en hög patientsäkerhet och att kvalitetssäkringar ska göras fortlöpande.

Patientjournallagen (1985:562)

En patientjournal skall innehålla de uppgifter som behövs för en god och säker vård av patienten. Uppgifterna skall föras in i journalen så snart som möjligt och en journal gäller endast för en patient. I journalen skall information finnas om vem som har gjort en anteckning och när. Patientens integritet ska respekteras och journalen ska hanteras och förvaras så att obehöriga ej kan komma åt den. Patienten själv skall dock kunna ta del av sin journal så snart som möjligt efter hans/hennes begäran. En journalhandling ska om inget annat anges bevaras i tre år efter det att senaste anteckning förts in.

Lag (1998:543) om hälsodataregister

Automatiserad behandling av personuppgifter i hälsodataregister får utföras av *central förvaltningsmyndighet* som då även fungerar som personuppgiftsansvarig. Ett hälsodataregister får behandla personuppgifter vid framställning av statistik, utvärdering, uppföljning, och kvalitetssäkring av hälso- och sjukvård samt vid forskning och epidemiologiska undersökningar. Ett hälsodataregister får innehålla endast de uppgifter som behövs för de ändamål för vilka personuppgifter får behandlas enligt lagen.

Lag (1998:544) om vårdregister

Den som bedriver vård får utföra automatiserad behandling av personuppgifter i vårdregister. För syftet att bereda vård i enskilda fall får personuppgifter i ett vårdregister behandlas för dokumentation av vården av patienter eller för sådan

administration som rör patienter. Ett vårdregister får endast innehålla de uppgifter som enligt lag eller annan författning skall antecknas i en patientjournal. Kontroll av ett vårdregister ska skötas av en personuppgiftsansvarig som ska se till att lagen följs i hanteringen av personuppgifter.

Sekretesslagen (1980:100, t o m 1998:486)

Denna lag innehåller bestämmelser om tystnadsplikt i det allmännas verksamhet och om förbud att lämna ut allmänna handlingar. I sistnämnda hänseende innefattar bestämmelserna begränsning i den i tryckfrihetsförordningen stadgade rätten att ta del av allmänna handlingar.

Bestämmelserna avser förbud att röja uppgift, vare sig det sker muntligen eller genom att allmän handling lämnas ut eller det sker på annat sätt.

Vid datoriserad informationsbehandling måste sekretess bedömas under konstruktion av databaser och söksystem eftersom IT ger stora möjligheter att söka fram information som sedan kan sättas samman med ett olagligt syfte.

Personuppgiftslagen (1998:204)

1998 ersatte Personuppgiftslagen Datalagen och det är den tekniska utvecklingen inom informationshantering och EG-direktiv som lett till lagens tillkomst. Syftet med lagen är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Som personuppgift räknas all slags information som direkt eller indirekt kan härledas till en fysisk person som är i livet. PUL gäller alla former av behandling. Det finns vissa lagar som har företräde gentemot PUL bland andra Lagen om vårdregister och Lagen om hälsodataregister. Detta innebär att om det i andra lagar eller förordningar finns bestämmelser som avviker från PUL ska de bestämmelserna gälla.

Personuppgifter får endast behandlas om den registrerade har lämnat samtycke till behandling om inte behandlingen rör situationer där inte samtycke krävs (§ 10). Utgångsläget är även att personuppgifter som anses känsliga (§ 13) är förbjudna att behandla då det inte gäller speciella fall (§ 15).

Behandling av personuppgifter ska kontrolleras av en personuppgiftsansvarig som ser till att lagen följs vid hantering av personuppgifter. Enligt lagen räknas den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandling av personuppgifter som personuppgiftsansvarig. Ett personuppgiftsbiträde, till exempel ett konsultföretag, kan behandla personuppgifter för den personuppgiftsansvariges räkning. I dessa fall ska avtal skrivas gällande personuppgiftsbiträdes behandling av personuppgifter.

Personuppgiftsansvarige ska kontrollera:

- att personuppgifter behandlas lagligt, korrekt och i överensstämmelse med god sed.
- att personuppgifter endast samlas in för särskilda, utryckligt angivna och berättigande ändamål.
- att personuppgifterna är adekvata och relevanta för ändamålet.
- att inte fler personuppgifter behandlas än vad som är nödvändigt för ändamålet.
- att personuppgifter inte bevaras under en längre tid än nödvändigt.

Personuppgiftsansvarige är *skyldig* att anmäla behandling av personuppgifter som är helt eller delvis automatiserad till Datainspektionen, vissa undantag finns dock (§ 37 PUL, 3-5 §§ personuppgiftsförodningen 1998:1191 och 4-5 §§ Datainspektionens föreskrifter DIFS 1999:3) [6].

Lag (1998:531) om yrkesverksamhet inom hälso- och sjukvårdens område

Lagen ger bestämmelser som berör:

- skyldigheter för hälso- och sjukvårdspersonal.
- behörighets- och legitimationsregler.
- begränsningar i rätten att vidta vissa hälso- och sjukvårdande åtgärder.
- disciplinpåföljd och återkallelse av legitimation m.m.

- Socialstyrelsens tillsyn.
- Ansvarsnämnds verksamhet inom Hälso- och sjukvård.
- ansvarsbestämmelser, överklagande m.m.

Lagen tar även upp hur den som tillhör hälso- och sjukvårdspersonal ska utföra sitt arbete. En patient ska ges sakkunnig och omsorgsfull hälso- och sjukvård som ska utformas tillsammans med patienten under tiden ska alltid patienten visas omtanke och respekt. Patient eller närstående ska ges anpassad information om hälsotillstånd och metoder för vård och behandling. Lagen tar även upp vilka regler som gäller för legitimering och utövande av yrkestitel samt hur och när tystnadsplikten gäller.

Arkivlagen

I arkivlagen ges bestämmelser om myndigheters och organs arkiv samt att myndigheter och organ ska kontrolleras av arkivmyndigheter som t ex kommunstyrelse eller landstingsstyrelse.

11 DISKUSSION

11.1 Test av hypotes

Vår hypotes lyder:

Genom att följa standarden SS-ISO/IEC 17799 och TIHS (Tillämpningsråd för Informationssäkerhetsarbete inom Hälso- och Sjukvård) under utvecklingsarbetet av hälso- och sjukvårdsystem, ökar sannolikheten för att en kravspecifikation för informationssäkerhetsarbete som innefattar tekniska, sociala och juridiska aspekter kommer att utformas.

Vi tycker att vårt resultat tydligt visar att hypotesen stämmer. Kapitel 10 som är den första kravspecifikationen för informationssäkerhetsarbete till IMIS-projektet innefattar tekniska, sociala och juridiska aspekter.

11.2 Intervjuernas betydelse för arbetet

Vi genomförde två olika typer av intervjuer Typ A (sköterskor, patienter) och Typ B (personer som kontaktas p.g.a. deras yrkesroll).

Tanken med många frågor i intervjuformulär till Typ A var att få förståelse för diabetessköterskors arbetssituation och diabetespatienters sjukdomssituation. Intervjuundersökning Typ A resulterade därför mest i information som var användbar för teknikerna i IMIS. Genomförandet av intervjuer Typ A gav oss en inblick i sköterskors och patienters vardag och på så sätt fick vi en övergripande förståelse för den betydelsen IMIS kan få för dem. Intervjusvar gällande autentisering och informationsklassificering visade sig inte ha något specifikt värde för framtagandet av kravspecifikationen, vilket var vår förhoppning. Vid intervjuerna beskrevs SITHS och TIHS. Eftersom intervjupersonerna inte hade någon kunskap inom området sedan tidigare fick de genom upplägget av intervjuerna inga valmöjligheter och frågorna blev därför ledande.

Vi har nu mer kunskap både om informationssäkerhet och om IMIS, därför hade vi idag formulerat intervjufrågor till sköterskor och patienter på ett sätt som hade varit mer användbart för informationssäkerhetsarbetet.

Intervjuer Typ B har varit oerhört värdefulla för hela arbetet. I kapitel 4-8 har vi med hjälp av intervjusvar kunnat bekräfta hur teorier om informationssäkerhet används i praktiskt arbete inom hälso- och sjukvårdens verksamhetsområde. Genom intervjupersonernas kunskaper har vi fått underlag för hur framtidens krav på informationssäkerhet inom hälso- och sjukvården kan komma att se ut. Tack vare intervjuerna Typ B har vi kunnat utforma kravspecifikationen så, att IMIS-projektet kan komma att matcha framtida krav för informationssäkerhet i hälso- och sjukvård. Intervjusvar som berör juridik fick oss att få förstå hur stort och komplext område juridik inom hälso- och sjukvård verkligen är.

11.3 Författarkommentarernas placering

Vi anser att vårt upplägg, med författarnas kommentarer i slutet av varje kapitel istället för i diskussionen, ökar läsbarheten. Upplägget har underlättat arbetsgången och den erfarenheten kommer vi att ta med oss till liknande arbete i framtiden.

11.4 Utvärdering av resultat

11.4.1 Kravspecifikation

Vi tycker att den första kravspecifikationen för IMIS är ett gediget arbete med förankring både i teori och i praktik. Vi har gett användbara förslag för t ex autenticering av användare, användarutbildning och förvaltning av databas.

I all litteratur vi har läst, inklusive TIHS och SS-ISO/IEC 17799, poängteras att informationssäkerhetsarbete är grupparbete med olika konstellationer för olika arbetsuppgifter. Vårt arbete att ta en kravspecifikation för informationssäkerhetsarbete har i många delar varit komplicerat på grund av detta faktum.

11.4.2 Juridikens betydelse

Under arbetets gång har vi till fullo insett vilken oerhört komplicerad juridisk struktur som styr arbete inom digital informationshantering och hälso- och sjukvård. Vi vill poängtera än en gång att juridisk expertkonsultation är ett krav för att säkerställa att informationshanteringen i IMIS ska följa lagar och förordningar.

11.5 Framtida utveckling för IMIS

Eftersom det finns en tanke att IMIS ska kunna anpassas till att täcka stora delar av hälso- och sjukvårdens behov, måste informationssäkerheten från början införlivas i utvecklingen av IMIS. Standarden SS-ISO/IEC 17799 är internationell och gäller således även vid internationell anpassning av IMIS. Lagar och regelverk måste dock anpassas olika för olika länder.

Kravspecifikationen för informationssäkerhetsarbete ska utvecklas och uppdateras jämsides med vidareutvecklingen av IMIS.

Vi rekommenderar att ett internetbaserat informationssystem avsett för hälso- och sjukvård inte ska hantera sekretessbelagd information. Vi anser inte att dagens teknik kan garantera den absoluta säkerhet som krävs för sådan information.

11.6 Kommande steg för informationssäkerhetsarbete

Nästa viktiga steg för att komma vidare med informationssäkerhetsarbete, är att satsa på utbildning. Det är nödvändigt att höja säkerhetsmedvetandet hos användare och organisationer. Tekniken finns idag för att nå en hög säkerhetsnivå men vi anser att brister finns på grund av att det individuella säkerhetsmedvetandet är förhållandevis på för låg nivå. Genom utbildning är det möjligt att höja den nivån och därmed öka informationssäkerheten.

En viktig fråga för utvecklare av informationssystem, är att hålla sig ajour med, och bevaka både internationell och nationell utveckling angående kommande förändringar av lagar och förordningar.

Vi tycker det är av stor betydelse att kommande forskning fokuserar på att hitta former och metoder för att väcka intresset för informationssäkerhetsarbete inom företag och organisationer. I dag heter det ofta att det inte finns tid och pengar för arbetet. Faktum är att det *måste* finnas tid och pengar, annars finns det ingen framtid för informationssystem. För att kunna utnyttja de möjligheter som finns med informationssystem och ta vara på den teknik som finns, måste informationssäkerhetsarbete tas på allvar.

BEGREPPSDEFINITION

- **Ackreditering -** Ackreditering är en kompetensprövning som sker enligt europeiska och internationella standarder. Ackreditering innebär att Swedac fortlöpande prövar att företaget i fråga är kompetent att utföra de provningar, analyser, kalibreringar, certifieringar och kontroller som det ackrediterats för.
- **ALMI Företagspartner** – Erbjuder affärsutveckling i kombination med finansiering.
- **Blekinge FoU-enhet** – Forsknings- och utvecklingsenhet för socialtjänst, primärvård och psykiatri i Blekinge.
- **Certifikat** – Ett elektroniskt signerat intyg av en publik nyckels tillhörighet till en specifik nyckelinnehavare.
- **eID-kort** – Elektroniska ID-kort i form av ett aktivt kort innehållande certifikat och nycklar samtidigt som kortets framsida utgör en visuell ID-handling.
- **CA –** Certificate Authority, Organisation/myndighet som utfärdar certifikat genom att signera certifikat med sin privata CA-nyckel. CA-nyckel är i sin tur ett nyckelpar där nyckelparets privata del används av CA:n för att signera certifikat och dess publika del används för att verifiera samma certifikat.
- **G8 -** (Grupp av åtta), är en samling av världens rikaste länder för politisk och ekonomisk samordning. Medlemmarna är Frankrike, Italien, Japan, Kanada, Ryssland, Storbritannien, Tyskland och USA.
- **HC certifikat** – Hälso- och sjukvårdscertifikat för svensk vård och omsorg.
- **HSS** – Hälso- och sjukvårdsstandardiseringen
- **IMIS** – Integrated Mobile Information System, mobil plattform för att underlätta kommunikation mellan diabetespatienter och diabetessköterskor.
- **IMIS-projektet –** Innefattar de personer som arbetar med IMIS som samt personer som på olika sätt berörs av arbetet.
- **LRA –** Local Registration Authority, en part som av en RA tilldelats uppgiften att hantera olika decentraliserade procedurer relaterad till certifikatbeställning, spärrning m.m.
- **RA** – Registration Authority, en part som av en CA tilldelats uppgiften att identifiera och registrera nyckelinnehavare samt hantera olika decentraliserade procedurer relaterat till certifikatbeställning, spärrning mm.
- **SSO** – Single Sign On, en användare ges tillgång till flera system samtidigt med en inloggning.
- **SIS –** Swedish Standards Institute
- **Swedac –** SWEDAC, Styrelsen för ackreditering och teknisk kontroll, är en central myndighet under Utrikesdepartementet med uppgifterna att verka som nationellt ackrediteringsorgan samt att ansvara för kontrollfrågor enligt lagen om teknisk kontroll.

REFERENS

Böcker

[1] Anderson R. J. (2001), *Security Engineering*, Jon Wiley & Sons

[2] Dataföreningen Sverige (2000), *Helsäkert – En bok för dig om säker information*, Lund: Studentlitteratur

[3] Engeström Yrjö (1987), *Learning by Expanding*, Orienta Konsultit: Helsinki

[4] Gollman Dieter (2000), *Computer Security*, John Wiley & Sons

[5] Halvarsson Andreas (2002), *Elektroniska Signaturer*, Studentlitteratur: Lund

[6] Lindberg Agne & Westman Daniel (2001), *Praktiskt IT-rätt*, Norstedts Juridik AB: Stockholm

[7] Maiwald Eric & Sieglein William (2002), *Datasäkerhet i praktiken*, Pagina Förlag AB: Sundbyberg

[8] Mitnick Kevin (2002), *Bedrägerihandboken – Hantera den mänskliga faktorn*, Sundbyberg: Pagina Förlags AB

[9] Oppliger Rolf (1999), *Security Technologies for the World Wide Web,* Artech House INC: Norwood

[10] Peltier Thomas R. (2001), *Information Security Risk Analysis*, Florida: CRC Press LLC

[11] Pipkin Donald L. (2000), *Information Security*, New Jersey: Prentice Hall PTR

[12] Seipel Peter (2001), *Juridik och IT*, Norstedts Juridik AB: Stockholm

[13] SIS HB 360 (2002), *Handbok I Informationssäkerhetsarbete,* Docusys: Stockholm.

[14] Viega John & McGraw Gary (2002), *Building Secure Software*, Addison-Wesley

Tidskrifter

[15] Andersson Jugås Sven-Erik, *Helheten viktigt för Syscoms It-arbete*, Säkerhet & Sekretess (2003:6), IDG-gruppen: Stockholm

Webbadresser

[16] Carelink, *Informationssäkerhet*, Tillgänglig: http://www.carelink.se/pages/newsbill.asp?VersionID=1&Pages=1,16

[17] Carelink, *Vad är SITHS?*, Tillgänglig: http://www.carelink.se/files/doc_200312111629.doc

[18] Carelink, *TIHS –Tillämpningsråd för informationssäkerhetsarbete inom Hälso- och Sjukvården*, Tillgänglig: http://www.carelink.se/files/doc_2002115115639.pdf

[19] Carelink*, SITHS - Certifikatpolicy för utgivande av certifikat inom vård och omsorg*, Tillgänglig: http://www.carelink.se/files/doc_2003225100947.pdf

[20] Carelink, *Implementering av hälso- och sjukvårdscertifikat*, Tillgänglig: http://www.carelink.se/files/104658_Implementering_v000531.pdf

[21] Carelink, *Infrastruktur för informationssäkerhet i hälso- och sjukvården*, Tillgänglig: http://www.carelink.se/files/104757_Infrastruktur_v000515.pdf

[22] Carelink, *Informationssäkerhet i vårdprocessen*, Tillgänglig: http://www.carelink.se/files/doc_2002126110411.pdf

[23] Carelink, *Pilotprojekt TIHS Akademiska laboratoriet*, Tillgänglig: http://www.carelink.se/files/doc_2002116132620.pdf

[24] Cordis, *Information Society Technologies*, Tillgänglig: http://www.cordis.lu/ist/home.html

[25] Dataföreningen i Sverige AB, *SBA – IT säkerhet och riskanalys,* Tillgänglig: http://www.dfs.se/products/sba/

[26] OAT, *Hemsida,* Tillgänglig: http://telehealth.hrsa.gov/index.htm

[27] Rixlex, *Författningar och förordningar*, Tillgänglig: www.riksdagen.se/debatt/lagar_forordningar.asp

[28] Steria, *Ny PKI-klient från Steria,* Tillgänglig: http://www.steria.se/index.db2?id=737

Forskningsrapporter

[29] Blekinge FoU-enhet, *Clinical Audit om den diabetessjukes eller vårdnadshavares eget kunnande och kontaktbehov med sjukvården*.

Övrigt

[30] Ansökan till Vinnova angående IMIS-projektet (030422), *Integrated Mobile Information System For Diabetic Healthcare (IMIS)*.

APPENDIX 1 - INTERVJUFRÅGOR TYP A

Frågeformulär – Sköterskor

Namn: .....
Adress: .....
Tele: .....

Fråga 1:
I vilken utsträckning har Du kontakt med Dina patienter?

Svar: Varje vecka □ Varje månad □ Några gånger per år □

Fråga 2:
Hur kommunicerar Ni idag?
Svar: .....
.....

Fråga 3:
Tror Du att IMIS kommer att underlätta kontakten med Dina patienter?
Svar: .....
.....

Fråga 4:
Hur går det till att ta emot blodsockervärde från Dina patienter idag?
Svar: .....
.....

Fråga 5:
Hur pass viktig är den labdata som skickas, enligt TIHS klassificeringstabell? (Klassificera enligt klassificeringstabell i TIHS)

Klass	Insynsskydd	Spårbarhet	Tillgänglighet	Riktighet
1	Ej känslig information	Spårbarhet ej viktigt för informationsobjekt	Låga krav på tillgänglighet för informationsobjekt	Låga krav på riktighet för informationsobjekt
2	Känsligt informationsobjekt	Spårbarhet skall finnas på informationsobjekt	Höga krav på tillgänglighet för informationsobjekt	Höga krav på riktighet för informationsobjekt
3	Hög känslighet på informationsobjekt	Spårbarhet med mycket hög tillförlitlighet	Mycket höga krav på tillgänglighet för informationsobjekt	Mycket höga krav på riktighet för informationsobjekt
4	Mycket hög känslighet på informationsobjekt			

Svar: .....
.....

Fråga 6:
Hur vill Du att patientens blodsockervärde ska presenteras?
Svar: .....
.....

Fråga 7:
Tycker Du att metoden med certifikat verkar vara en säker inloggningsmetod jämfört med idag?
Svar: .....
.....

Fråga 8:

Nu när Du vet lite om IMIS, skulle Du kunna tänka Dig att kommunicera med Dina patienter via IMIS, även sekretessbelagda uppgifter?
Svar: .....
.....

Fråga 9:
Har Du några idéer om vad Du skulle vilja kunna använda IMIS till i framtiden?
Svar: .....
.....

Fråga 10:
Vet Du några lokala föreskrifter som gäller informationssäkerhet, förutom Landstingets policy?
Svar: .....
.....

Fråga 11:
Har Du varit involverad i något riskanalysarbete, i så fall hur ofta?
Svar: .....
.....

Frågeformulär - Patient

Namn: .....
Adress: .....
Tele: .....
Födelseår: .....
Kön: .....

Fråga 1:
I vilken utsträckning har Du kontakt med Din diabetessköterska?

Svar: Varje vecka □ Varje månad □ Några gånger per år □

Fråga 2:
Hur kommunicerar Ni idag?
Svar: .....
.....

Fråga 3:
Tror Du att IMIS kommer att underlätta kontakten med Din diabetessköterska?
Svar: .....
.....

Fråga 4:
Hur går det till att skicka blodsockervärde idag?
Svar: .....
.....

Fråga 5:
Hur pass viktig är den labdata som skickas, enligt TIHS klassificeringstabell? (Klassificera enligt klassificeringstabell i TIHS)

Klass	Insynsskydd	Spårbarhet	Tillgänglighet	Riktighet
1	Ej känslig information	Spårbarhet ej viktigt för informationsobjekt	Låga krav på tillgänglighet för informationsobjekt	Låga krav på riktighet för informationsobjekt
2	Känsligt informationsobjekt	Spårbarhet skall finnas på informationsobjekt	Höga krav på tillgänglighet för informationsobjekt	Höga krav på riktighet för informationsobjekt
3	Hög känslighet på informationsobjekt	Spårbarhet med mycket hög tillförlitlighet	Mycket höga krav på tillgänglighet för informationsobjekt	Mycket höga krav på riktighet för informationsobjekt
4	Mycket hög känslighet på informationsobjekt			

Svar: .....
.....

Fråga 6:
Sparas värdena t ex en dag eller längre innan de skickas till Din diabetessköterska?
Svar: .....
.....

Fråga 7:
Tycker Du att metoden med certifikat verkar vara en lämplig inloggningsmetod för Dig som patient?
Svar: .....
.....

Fråga 8:
Nu när Du vet lite om IMIS, skulle Du kunna tänka Dig att kommunicera med Din diabetessköterska via IMIS, även känsliga, personliga uppgifter?
Svar: .....
.....

Fråga 9:
Har Du några idéer om vad Du skulle vilja kunna använda IMIS till i framtiden?
Svar: .....
.....

APPENDIX 2 - INTERVJUFRÅGOR TYP B

Intervjufrågor till:

Kjell Allestedt, Informationssäkerhetsansvarig på Carelink

1. Forskning och rekommendationer angående riskanalys – hur har man kommit fram till TIHS rekommendationer angående hela modellen från början med policy till slutet med själva riskanalysen?
2. Är detta något som kommer att bli standard inom hälso- och sjukvård? I så fall när?
3. Ska de modeller och metoder användas i hälso- och sjukvård? I så fall när?
4. Hur ska de implementeras i vårdprocessen?
   Framtagning av certifikat – hur kom det sig att man valde den typen av autenticering?
5. De rekommendationer om certifikat som autenticering, kommer de att gälla i framtiden avseende system som ska köpas in till hälso- och sjukvård?
   Finns det rekommendationer nu från socialstyrelsen att vårdgivare ska följa vissa metoder och modeller vid riskanalys och informationssäkerhetsarbete?
6. Har Carelink någon speciell person som arbetar med lagar och sekretessfrågor inom informationssäkerhet i vården? Finns det i så fall möjlighet att kontakta den personen?
7. Steria, är enligt ett dokument från Carelink det It-företag som ska ha hand om utvecklingen av en nationell CA. Vet Du hur det arbetet fortlöper?
   Har Du någon ytterligare information att ge som kan vara lämplig i vårt arbete?

Thomas Pehrsson, IT-chef på landstinget Blekinge

1. Känner Du till TIHS (Tillämpningsråd för Informationssäkerhet inom Hälso- och Sjukvård)?
2. Har Ni i Landstinget tänkt använda dessa tillämpningsråd?
3. Har Ni i Landstinget tänkt använda de certifikat och PKI som Carelink tagit fram?

Britt Lagerlund, informationssäkerhetschef för Region Skåne

1. Hur fortlöper arbetet med certifikathanteringen?
2. Hur fungerar certifikathanteringen rent praktiskt?

Johan Förander, jurist och lärare i IT-juridik på BTH

1. Har Du någon möjlighet att hjälpa oss att hitta rätt bland lagar och förordningar angående vårt arbete?
2. Vi behöver förankra de lagar vi har tagit fram med en jurist, kan Du tipsa oss om något vi kanske har glömt?
3. Kan Du rekommendera någon bra sida på Internet gällande lagar och förordningar?

Lars-Åke Petterson, informations- och IT-säkerhetschef samt personuppgiftsombud för landstinget Östergötland

1. Vilket är Ditt ansvarsområde och vilken typ av uppgifter arbetar Du med?
2. Styrs allting inom, den numera, digitala sjukvården av lagar eller finns det ytterligare riktlinjer att följa för att garantera patientens säkerhet med tanke på digitala journalsystem o s v?
3. I vårt projekt har det diskuterats kring att patienten själv ska äga rätten till det som står i patientens journal, för att underlätta den digitala hanteringen. Detta var enligt Allestedt även en fråga som diskuterades inom Carelink och att det arbetet är mycket omfattande juridiskt. Vad vet Du om detta arbete? Är det möjligt? Vem ansvarar för arbetet för eventuell vidare kontakt?
4. Allestedt nämnde en patientportal som ska testas i Östergötland. Vet Du något om detta arbete? Hur ser portalen ut och hur ska den komma att användas? Vem ansvarar för arbetet för eventuell vidare kontakt?
5. Har Du någon möjlighet att hjälpa oss att kontrollera de lagar vi har tagit fram som berör vårt arbete?