Institutionen för kommunikation och information
Examensarbete i informationssystemutveckling 10p
C-nivå
Vårterminen 2007

Sjuksköterskors uppfattningar om informationssäkerhet –
en kvalitativ intervjustudie

Kerstin Karlsson

HS-EA-DVA-2005-001

Sjuksköterskors uppfattningar om informationssäkerhet
– en kvalitativ intervjustudie

Kerstin Karlsson

Sammanfattning

Inom hälso- och sjukvården hanteras känslig patientinformation. I framtiden kommer alltmer information att lagras elektroniskt och därmed bli mer lättillgänglig. Användarna av informationssystemen kan vara en säkerhetsrisk. Metoderna som används vid intrångsförsök inriktas alltmer på att involvera människor istället för att enbart använda sig av teknik.

Syftet med detta arbete är att undersöka användarnas upplevelse och medvetenhet om icke tekniska hot mot informationssäkerheten för digitalt lagrad patientinformation.

Datainsamlingen genomfördes i form av kvalitativa intervjuer med sjuksköterskor anställda på ett sjukhus i västra Sverige. Resultatet visar att det allt överskuggande upplevda hotet var intrång och förlust av sekretess i den elektroniska patientjournalen. Hoten uppfattades som interna främst från personal och till viss del från patienter. Intrång av externa aktörer ansågs osannolikt och av mer teknisk natur. En social engineering attack skulle kunna vara lyckosam, skadan som skulle kunna åstadkommas förstärks av icke fungerande utloggningsrutiner, kombinerat med vissa brister i lösenordshanteringen och användarnas omedvetenhet om hoten.

Nyckelord: Informationssäkerhet, Social engineering, Elektroniska patientjournaler, Sjuksköterskor, Säkerhetsmedvetenhet.

Innehållsförteckning

1. Introduktion

> *Allt jag erfar, ser eller hör, i mitt verk inom läkekonsten och i mitt umgänge med medmänniskorna, som bör hemlighållas, kommer jag att förtiga, som om det aldrig hade sagts.*
>
> Hippokrates ”Läkekonstens fader” 460-370 f. Kr ur Läkareden.

Citatet visar att sekretess inom läkekonsten är av gammalt datum. Anställda inom vårdsektorn är ofta väl förtrogna med begrepp som sekretess, tystnadsplikt och patientsäkerhet. Den frågan som jag har ställt mig är hur stor medvetenheten är om de nya hot och risker som uppstår vid övergång från pappers- till datalagring av informationen.

För det flesta människor känns det som en självklarhet att vårdpersonal är uppdaterade med aktuell hälsoinformation. Att journaler i pappersform fortfarande existerar väcker ofta stor förvåning. De människorna som det berör utgår inte desto mindre från att deras uppgifter är skyddade, oavsett hur informationen är lagrad. Det är för dem en självklarhet att säkerhetsskyddet fungerar. Tyvärr är det ett välkänt faktum att de yttre angriparna till viss del har bytt skepnad från tonåriga datahackers till internationella kriminella ligor. Vi nås allt oftare av rapporter om brister i informationssäkerheten som slår ut datasystem och servrar eller gör att banker förlorar miljonbelopp. Vårdsektorn har hittills, efter vad som är känt, varit skonat från sådana angrepp. För att även i framtiden skydda informationssystemen, informationen och den enskildes integritet krävs inte bara fullödiga tekniska lösningar, utan även att användarna har rätt kunskap och motivation.

Mitt intresse för ämnet har dels sitt ursprung i att journalhandlingar å ena sidan betecknas som känsliga och omfattas av ett flertal lagar, men att de flesta anteckningar ändå berör ganska banala åkommor. Varför skall vi skydda anteckningar om Greta Anderssons höftsmärtor? Vem skulle kunna få tag i uppgifterna och hur skulle det gå till? Under utbildningen i informationssystemutveckling ingick även informationssäkerhet och då förstod jag att virusprogram och brandväggar inte räcker som skydd för informationen. Det finns flera andra villkor som måste uppfyllas. Människan var en av riskfaktorerna. Någon med tillräcklig skicklighet skulle kunna, genom att enbart använda sig av våra allmänmänniskliga egenskaper, tillsammans med lite teknikkunskap, skaffa sig tillgång till information och system. Därmed var problemställningarna i arbetet ganska självklara. Vad trodde andra sjuksköterskor om hot och hur försökte de skydda informationen? Ämnet känns även aktuellt därför att stora IT - satsningar planeras inom vården och användarnas agerande mer och mer lyfts fram som en viktig säkerhetsfaktor.

Syftet med detta arbete är att undersöka användarnas, i detta fall sjuksköterskornas, upplevelse av och medvetenhet om icke tekniska hot mot informationssäkerheten för digitalt lagrad patientinformation och de informationssystem som de hanterar. Hoten skulle både kunna riktas mot den enskildes integritet, men även innebära att dataintegriteten, det vill säga den lagrade informationens riktighet skadas. Studien vänder sig till dem som administrerar informationssäkerheten, vill fördjupa sina kunskaper i ämnet och även till intresserade användare.

1.1. Översikt över rapporten

Det närmast följande avsnittet kapitel 2 innehåller bakgrundsmaterial. Innehållsmässigt är kapitlet indelat i två stycken. Den första delen innehåller en översikt av informationssystemen inom

vården främst ur ett tidsperspektiv, vad som är aktuellt idag och vilka förändringar som ses inför framtiden, då riktlinjer från den nationella IT-strategin kommer att genomföras. Andra delen behandlar informationssäkerhet. Den inleds med en översikt över grundläggande begrepp och sammanhang inom ämnet informationssäkerhet. Två olika konceptuella modeller för informationssäkerhet introduceras. Därefter följer resonemang om autentisering och lösenordshantering. Till sist presenteras begreppet social engineering, varför det är ett hot och vilka principer från socialpsykologin som möjliggör sådana attacker. Kapitlet avslutas med en översikt över tidigare forskning inom informationssäkerhet och social engineering.

Kapitel 3 innehåller problembeskrivning samt syfte och problemställning för arbetet. I kapitel 4 redovisas val av metod och vilka överväganden som gjordes vid metodvalet. Forskningsstegen som kommer att följas under arbetsprocessen presenteras. Kapitel 5 är en redovisning av intervjumaterialet. Det består av olika teman under vilka resultatet av intervjuerna samlas, avsnittet innehåller även citat från intervjuerna. Kapitel 6 är resultatkapitlet där vad som framkommit i materialavsnittet syntetiseras ytterligare, en kort sammanfattning avslutar kapitlet. I avsnittet illustreras även visuellt hur olika teman från materialet kan sättas in i en av de tidigare presenterade modellerna för informationssäkerhet. Kapitel 7, slutligen, innehåller diskussion över resultatet och om problemställningen kan anses vara besvarad. Avsnittet belyser även styrkor och svagheter i arbetet, både med avseende på resultat och med avseende på arbetsprocessen. Studien kommer även att sättas in i ett större sammanhang i och med att resultatet relateras till andra resultat inom området. Kapitlet avslutas med att slutsatser dras och tänkbara områden för framtida forskning definieras.

2. Bakgrund

I detta avsnitt kommer läsaren att introduceras i ämnet. Stycket inleds med en översikt över informationssystem inom vården, vilka lagar som anknyter till lagring och överföring av information, samt vad som är aktuellt på området IT i vården, idag och i framtiden. Det följande avsnittet innehåller en översikt över ämnet informationssäkerhet. Det behandlar även lösenordshantering, olika autentiseringssätt samt en beskrivning av begreppet social engineering. Avslutningsvis behandlas tidigare forskning inom området informationssäkerhet inom vården samt social engineering.

2.1. Informationssystem i vården

Informationssystemen inom vården ersätts mer och mer av elektroniska system. Införandet av elektroniska informationssystem har gått långsamt och implementeringen har ofta saknat helhetssyn. I Vård-IT-kartan UsersAwards (2004) undersökning om användarnas erfarenheter av vårdens IT-stöd, undersöks 50 olika IT-system. Dock fanns ytterligare 350 system som inte hade tillräckligt många användare. Med det förstås att många system är specifika för små nischer inom vården. Ett system har hanterat patientadministration, ett annat laboratoriesvar. Lösningarna har bara täckt ett administrativt problem på ett ställe och få har insett att vinster skulle kunna göras genom att hämta data från olika system. Detta beskrivs närmare av Raghupathi (2002) och Stuewe (2002). Haux (2006) beskriver även behovet för framtidens system. Forskningsdata och statistik skall kunna hämtas från systemen. Data skall kunna användas för epidemiologiska studier. Nya system skall även kunna hantera datatyper som gör det möjligt att exempelvis inkludera mätdata från portabla övervakningsapparater som patienten har i hemmet.

Under de senaste åren har den nationella ledningsgruppen för IT i vård och omsorg utarbetat ett förslag till en nationell IT - strategi för vård och omsorg, vilken trädde i kraft i mars 2006 Även internationellt pågår inom EU arbete för e-hälsa. Samtliga medlemsländer uppmanas att ta fram nationella strategier för arbetet på e-hälsoområdet (Regeringskansliet, 2006). Den nationella visionen för IT i framtidens vård och omsorg innehåller bland annat följande:

> *Med hjälp av ändamålsenliga IT-stöd får alla patienter god och säker vård och bra service. Vårdpersonalen kan ägna mer tid åt patienterna och anpassa vården till varje patients behov. IT används som ett strategiskt verktyg i alla delar av vården och de samlade vårdresurserna utnyttjas på ett mer effektivt sätt.*
> Regeringskansliet (2006) sid. 6.

I visionen framhålls även att patienter måste kunna få del av information om vård och hälsa, samt sin egen hälsosituation. Personal måste få tillgång till IT-stöd som garanterar patientsäkerheten och underlättar deras dagliga arbete. Ansvariga inom vården skall kunna följa upp patientsäkerheten och kvalitén på vården och använda IT för styrning av verksamhet samt tilldelning av resurser. Arbetet är uppdelat i sex insatsområden.

- Harmonisera lagar och regelverk med en ökad IT-användning.
- Skapa en gemensam informationsstruktur.
- Skapa en gemensam teknisk infrastruktur.
- Skapa förutsättningar för samverkande och verksamhetsstödjande IT-system.

- Möjliggöra åtkomst till information över organisationsgränser.
- Göra information och tjänster lättillgängliga för medborgarna.

Begreppet **patientsäkerhet** definieras enligt följande; *”Säkerheten för patienten mot skada och risk för skada till följd av åtgärd inom hälso- och sjukvården eller brist på sådan åtgärd*” Socialstyrelsen (2004). En senare och kortare definition av patientsäkerhet är *”Skydd mot vårdskada”*. Där vårdskada definieras som *”lidande, obehag, kroppslig eller psykisk skada, sjukdom eller död som orsakas av hälso- och sjukvården och som inte är en oundviklig konsekvens av patientens tillstånd”* (SOFS, 2005:12). Det kan vara svårt att inrymma den komplexitet som patientsäkerhetsbegreppet innebär i en kort definition, men den senare versionen verkar vara den för tillfället allmänt vedertagna. Det här arbetet kommer inte fortsättningsvis att närmare beröra säkerhet ur patientsäkerhetsperspektivet. När termen säkerhet används syftas istället på informationssäkerhet det vill säga säkerhet för den information som lagras. Det begreppet ges en närmare definition senare i avsnitt 2.2.

Den nationella IT strategin innefattar planering för en landsövergripande nationell patientöversikt, där alla vårdgivare skall kunna ta del av den vård som patienten erhållit oavsett vårdform och geografiska och organisatoriska gränser. Ett annat av målen i den nationella IT strategin är att harmonisera lagar och regelverk, idag regleras lagring, överföring och dokumentation huvudsakligen av följande lagar:

Patientjournallagen (SFS 1985:562) anger vad vårdgivare är skyldiga att dokumentera. I denna anges även att journalhandling skall hanteras och förvaras så att inte obehöriga får tillgång till den.

Sekretesslagen (SFS 1980:100) anger förbud att röja uppgifter och lämna ut enskilda handlingar. Förbudet gäller även mellan myndigheter och mellan olika verksamhetsgrenar inom samma myndighet. För att uppgifter skall få föras vidare krävs patientens samtycke. Här ingår även tystnadsplikt för personal samt den inre sekretessen, vilken innebär att uppgifter inom en myndighet inte får lämnas ut utan att ett behov finns.

Personuppgiftslagen (PUL) (SFS 1998:204) syftar till att hindra intrång i den personliga integriteten.

Lag om vårdregister (SFS 1998:544) preciserar hur personuppgifter skall behandlas mer specifikt inom hälso- och sjukvården. Lagen markerar även tydligt att endast den som har behöver personuppgifter för sitt arbete, det vill säga vårdar patienten, har rätt till uppgifterna.

Under oktober 2006 har ett betänkande lämnats från Patientdatautredningen, Statens offentliga utredningar (SOU); Patientdatalagen (SOU, 2006:82). Sammanhållen journalföring - personuppgiftsbehandling inom hälso- och sjukvården. I betänkandet föreslås en ny sammanhängande reglering av personuppgiftsbehandlingen inom hälso- och sjukvården i en särskild lag, *patientdatalagen*. I lagen regleras bl.a. frågor om journalföring, sekretess, elektronisk tillgång till patientuppgifter och användningen av patientuppgifter i verksamhetsuppföljning. Denna nya lag skall göra det möjligt att lagligt föra över uppgifter mellan myndigheter och kunna möjliggöra en landsövergripande journal, journaluppgifter skall även kunna användas administrativt/strategiskt för uppföljningar av verksamheten. Enligt betänkandet skall lagen ge den enskilde patienten rätt att spärra sina uppgifter för överföring (SOU, 2006:82).

Jag anser att vårdsektorn har ett stort behov att öka IT-användningen av de orsaker som angivits

ovan. Anledningen till att det har gått så långsamt tror jag går att finna dels i de lagar som beskrivs, det kan säkert även bero på det har funnits ett visst motstånd och brist på kompetens inom dataområdet hos personal – på alla nivåer, en annan faktor kan vara strukturen inom vårdsektorn, med olika huvudmän och ett ibland kortsiktigt politiskt styre. Det som gör att läget ser ljusare ut idag är tillkomsten av den nämnda IT-strategin, som även har en bred politisk förankring på regeringsnivå. Förekomsten av strategin innebär att det idag finns en nationell samordning och ekonomiska medel avsatta till satsningen.

I praktiskt hänseende behöver allt fler system integreras för att kunna skapa en gemensam infrastruktur. I detta avseende är inte vårdsektorn unik. Boddy et al. (2005) beskriver det branschövergripande behovet av interoperabilitet, integrering och sammanställning av data, beroende på sammanslagningar av företag, krav på förkortade ledtider eller företagslednings behov av system för bättre uppföljning och planering. Utvecklingen historiskt sett har gått från informationssystem som enbart gav vinster i produktionsledet till system som även fungerar som ett strategiskt instrument för företagsledningen (Boddy et al, 2005). Chen och Doumeingts (2003) beskriver komplexiteten när interoperabilitet eftersträvas. Angreppssättet måste vara holistiskt, inte enbart tekniskt utan även utgå från förändringar i organisation, ekonomi och sociala trender och behov. Problemen kan härstamma det tekniska lagret; vilka system som används, hur uppgifter finns lagrade, hur överföringen skall ske. Det finns även administrativa, kunskaps- och affärsmässiga problem. Det kan till exempel vara hur standarder för termer och begrepp skall utformas. Hur processerna ser ut i de olika delarna som skall integreras, lagar och förordningar, samt olika mognad gällande säkerhetsmedvetenhet (Chen & Doumeingts, 2003).

2.2. Informationssäkerhet

Organisatoriska förändringar påverkar säkerheten för informationen som lagras. I det följande avsnittet finns en översikt över informationssäkerhetsbegreppet och de fyra grundkomponenterna. Det avsnittet vänder sig i första hand till läsare som saknar grundläggande kunskaper i informationssäkerhet. Olika konceptuella modeller för informationssäkerhet presenteras. Begreppet autentisering, olika autentiseringssätt, hot och risker i samband med lösenordhantering och begreppet social engineering kommer att behandlas mer ingående.

Det kan förekomma en viss begreppsförvirring när säkerhet för information skall beskrivas. Pfleeger och Pfleeger (2003, sid. 10) använder begreppet *computer security*” *When we talk about computer security we mean that we are addressing three very important aspects of any computer-related system: Confidentiality, integrity, and availability.* Termen **Informationssäkerhet** kan definieras som; *”the process of protecting data from unauthorized access, use, disclosure, modification, or disruption”* (Wikipedia, 2007) eller *”Förmågan att upprätthålla önskad sekretess (konfidentialitet), riktighet och tillgänglighet avseende information och informationstillgångar*” *(*Krisberedskapsmyndigheten, 2006, sid. 8). Swedish standards institute (SIS, 2003 sid. 8), har en liknande definition; *”säkerhet beträffande informationstillgångar rörande förmågan att upprätthålla önskad konfidentialitet (sekretess), riktighet (integritet) och tillgänglighet (även spåbarhet och oavvislighet)”* dessutom kan även auktorisation och autentisering ingå (SIS, 2003). I Sverige används idag begreppet informationssäkerhet som en samlande term som skall täcka in alla aspekter på hur information skall skyddas, oavsett lagringssättet. I detta arbete kommer informationssäkerhet definieras enligt SIS:s definition och ur följande fyra aspekter; tillgänglighet, sekretess, integritet och spårbarhet. Här följer en definition av alla fyra aspekterna.

> *Tillgänglighet: Möjligheten att utnyttja informationstillgångar efter behov i förväntad utsträckning och inom önskad* tid (SIS, 2003, sid. 12).

Information skall vara tillgänglig på rätt plats och vid rätt tidpunkt.

> *Konfidentialitet /Sekretess: Avsikten att innehållet i ett informationsobjekt inte får göras tillgängligt eller avslöjas för obehöriga* (SIS, 2003, sid. 9).

Endast den som har rättighet att ta del av informationen, skall kunna se den.

> *Riktighet/Integritet: Egenskap att information inte obehörigen, av misstag eller på grund av funktionsstörning har förändrats* (SIS, 2003, sid. 10).

Inget får vara felaktigt tillagt, borttaget eller förvanskat.

> *Spårbarhet Möjlighet att entydigt kunna härleda utförda aktiviteter i systemet till en identifierad användare* (SIS, 2003, sid. 11).

Det skall kunna utläsas vem som har bearbetat informationen, dvs. skrivet, läst, tagit bort ändrat eller kopierat.

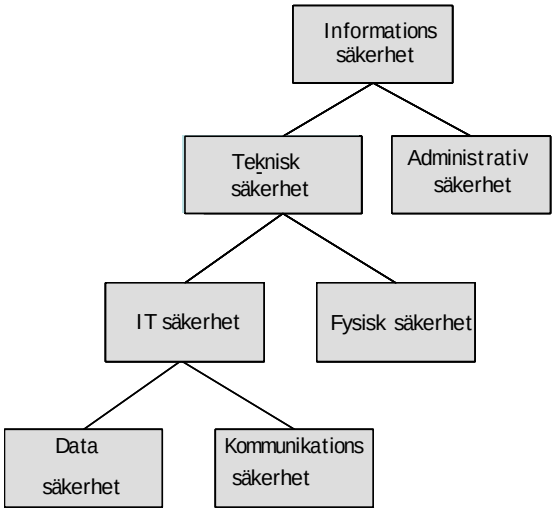
För att en god informationssäkerhet skall upprätthållas bör enligt Pfleeger och Pfleeger (2003) en organisation ha en god administrativ säkerhet. Den innefattar regler för hur säkerhetsarbetet skall utformas, inkluderande ansvarfördelning och utbildning av användarna. Dessutom måste det finnas en god teknisk säkerhet, innefattande dels den fysiska säkerheten, men även hur överföring och lagring av data skall skyddas.

Pfleeger och Pfleeger (2003) beskriver hur den administrativa säkerheten måste uppgraderas så att den möter kraven från nya utmaningar. Hot och risker måste värderas och sårbarheter identifieras. Utifrån detta skall säkerhetspolicys utarbetas.

Tekniskt sett skyddas tillgångarna fysiskt med hjälp av stöldskydd, larm, brandskydd och skydd för strömavbrott. Mjukvara, hårdvara och lagrad information skyddas bland annat av virusprogram och brandväggar. Det släpps ständigt nya och säkrare versioner av virusprogram och operativsystem. När information lagras eller transporteras kan den skyddas genom kryptering. Krypteringsalgoritmer blir lättare att knäcka i och med att datorerna får bättre prestanda. Men samtidigt kommer nya algoritmer som har starkare skydd. Nya sårbarheter gör att skydden stärks (Pfleeger & Pfleeger, 2003).

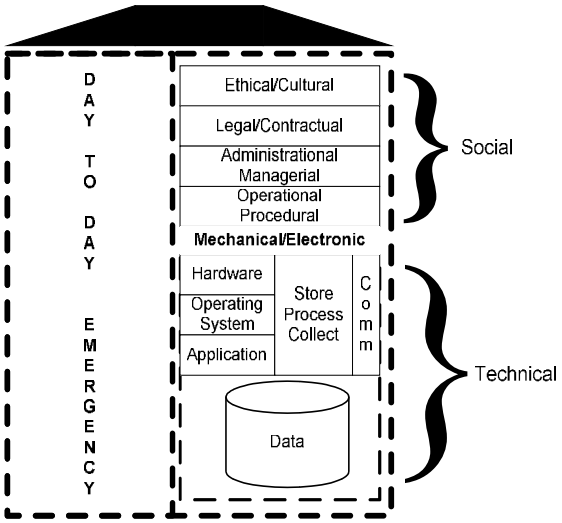
Pfleeger och Pfleeger (2003) redogör för olika hot mot informationstillgångar. Hoten kan vara interna eller externa. Hoten kan vara omedvetna eller planerade. Hotkällan kan vara både människan, tekniken och naturen. Hot mot *tillgängligheten* till informationen kan orsakas av fysiska skador som brand, stöld, strömavbrott med mera. Tillgängligheten kan även skadas av skadlig kod. Även belastningsattacker *Denial of Service* (DoS)- attacker som innebär överbelastning av server eller annan kritisk funktion är ett hot mot tillgängligheten. Hot mot *sekretess* kan ske genom avlyssning av trafik eller genom att på annat sätt obehörigen få tillgång till information. *Integriteten* kan hotas genom att system eller applikationer inte håller tillräckligt hög klass, så transaktioner inte ger riktiga värden, men även av illasinnad kod. Obehöriga som har tillgång till system kan även skada integriteten avsiktligt eller oavsiktligt. *Spårbarhet* kan skadas av skadlig kod, då viss kod även kan ändra och radera loggar (Pfleeger & Pfleeger, 2003). Spårbarheten kan även skadas om inloggningar används slarvigt internt eller om inloggningsuppgifter läcker ut och används av fel personer.

Det finns olika modeller för informationssäkerhet. SIS modellen illustreras i figur 1. Denna modell visar på ett åskådligt och tydligt sätt de olika beståndsdelarna i modellen och utgår från olika miljöer som skyddsåtgärderna sätts in i. Speciellt på den tekniska sidan finns en detaljrikedom som väl täcker området, även om datasäkerhet och kommunikationssäkerhet till viss del överlappar varandra. På den administrativa sidan finns däremot stora luckor. Administrativ säkerhet kan innebära många olika saker och säkerhet ur exempelvis användarperspektiv finns inte explicit uttryckt.



Figur 1, SIS:s modell för informationssäkerhet efter SIS (2003)

Ett annat sätt att belysa begreppet är *Security By Consensus*, SBC- modellen (Kowalski, 1994) som visas i figur 2. Vid första anblicken kan tyckas att modellen inte ger en lika klar och överskådlig bild av begreppet, men modellen täcker förutom de tekniska även in de sociala aspekterna av informationssäkerhet, något som SIS-modellen saknade, och kan därför användas för att utvärdera och definiera säkerhet ur fler synvinklar.



Figur 2, SBC modellen för informationssäkerhet, från Kowalski (1994, s. 19).

Det som SBC- modellen däremot inte pekar ut lika tydligt är de olika miljöerna som skyddsåtgärder kan sättas in i. SBC- modellen har däremot flera olika användningsområden, den kan användas för att analysera och utvärdera informationssäkerhet från individnivå till internationell nivå. Informationssäkerhet blir med det här angreppssättet en dynamisk process, förändring på en nivå kan även medföra konsekvenser på andra nivåer. Modellen har delvis använts som ett sätt att analysera överföring mellan datasystem med säkerhetsperspektiv och det finns beröringspunkter mellan SBC- modellen och exempelvis de olika lager och det holistiska angreppssätt som Chen och Doumeingts (2003) använder för interoperabilitet. Av skäl som angivits ovan, helhetssyn som även innefattar de sociala aspekterna och användarna, en tydlig struktur som möjliggör en viss generaliserbarhet, samt överensstämmelse med andra modeller inom dataområdet anser jag att SBC- modellen är den som bäst lämpar sig för den här formen av arbeten. Jag kommer därför att använda modellen vid redovisning och analys av resultatet.

2.2.1. Autentisering

En hörnsten för informationssäkerhet är hantering av autentisering. Pfleeger och Pfleeger (2003), anser att begreppet autentisering baseras på kunskap som delas mellan datasystemet och användaren. I Terminologi för informationssäkerhet (SIS, 2003, sid.28) finns följande definition; *”verifiering av uppgiven identitet eller av ett meddelandes riktighet”*. I Paginas stora IT-lexikon (Thorell, 2005) översätts ordet till det svenska verifiering vilket definieras som *”Kontroll av användares behörighet, oftast i samband med inloggning eller anslutning till dator eller ett nätverk”*. Jag kommer att använda mig av SIS:s definition som innefattar användaridentiteten. Implicit förstås även att termen även inrymmer någon form av behörighetstilldelning. Pfleeger och Pfleeger (2003) anger tre olika sätt att bekräfta användarens identitet.

- Något en användare vet.
  Lösenord, PIN-koder.
- Något en användare har.
  Nycklar, id-handlingar, kort.
- Något som en användare är.
  Biometrisk igenkännig av användare som fingeravtryck, irisskanning, röst- eller ansiktsigenkänning.

Genom kombinationer kan en starkare autentisering uppnås. Det överlägset vanligast sättet att autentisera en användare är att använda lösenord, ofta i kombination med exempelvis användarnamn. Det kan tyckas att lösenord som endast är kända av användare och system skulle vara ett bra sätt att säkra användarens identitet. Enligt Pfleeger och Pfleeger (2003) är användande av lösenord dock förknippade med flera risker. Lösenord kan knäckas på ett flertal sätt.

- Genom att pröva samtliga möjliga lösenord. Längden på lösenordet samt vilka kombinationer av tecken som ingår, stora och små bokstäver, siffror, specialtecken, avgör i det fallet hur säkert lösenordet är.
- Genom att endast pröva ord från ordlista. Genom att begränsa sökningen till ord som finns i ordlistan kan resurser i form av tid och datorkraft minskas.
- Genom att pröva lösenord som är troliga för just den användaren. Det kan vara ett namn,

tillexempel användarens eget andra namn eller namn på familjemedlemmar, eller en upprepning av användarnamnet.

- Genom att söka igenom systemfiler efter lösenordslistan.
- Genom att fråga användaren.

En angripare kan börja med att pröva troliga lösenord, för att fortsätta med ord som finns i ordlistan. Om inte lösenordet ändå inte kan hittas kan en *Brute force* attack användas, som prövar samtliga tänkbara kombinationer. Tiden och kraften som då åtgår för att hitta rätt lösenord beror på längden och komplexiteten på lösenordet (Pfleeger & Pfleeger, 2003). Ett lösenord som består av två små bokstäver kan endast ha 676 kombinationer. Om lösenordet däremot består av 8 bokstäver både stora och små är 53459 miljoner kombinationer möjliga. För att förhindra att lösenord kan hämtas från systemfiler krävs kryptering av dessa filer. Att fråga användaren om lösenordet genom att utge sig för att exempelvis vara systemadministratör eller på annat sätt uppträda under falsk identitet ingår som en del av vad som brukar benämnas *social engineering*. Begreppet definieras senare i detta kapitel. Pfleeger och Pfleeger (2003) gör följande sammanfattning av lösenordshantering.

- Använd både små och stora bokstäver, siffror och specialtecken.
- Välj långa lösenord.
- Välj inte namn eller ord som finns i ordlistan.
- Välj lösenord som har innebörd för dig, men inte något som utomstående kan gissa.
- Ändra lösenordet regelbundet.
- Skriv inte ner det.
- Tala inte om det för någon annan.

En angripare kan få kännedom om lösenord genom att användaren förvarar lösenordet på ett otillfredsställande sätt, som tillexempel fasttejpat på dataskärmen eller under skrivbordsunderlägget. En trojansk häst som lagrar användarnamn och lösenord kan även installeras på datorn, informationen skickas sedan vidare till angriparen (Pfleeger och Pfleeger, 2003).

Pfleeger och Pfleeger (2003) beskriver frustrationen som användare kan känna när de tvingas logga in gång på gång för att få tillgång till system som var och ett avkräver användaren användarnamn och lösenord. För att underlätta väljer användaren ofta samma lösenord för alla systemen. Lösningen på problemet skulle kunna vara att användaren vid första inloggningen får tillgång till de system som han eller hon är behörig till, så kallad *single-sign-on*. Detta ställer dock höga krav på säkerhet hos denna första och enda inloggning. Om användarnamn och lösenord kompromettеras är dörren öppen till alla system.

Ett sätt att lösa säkerhetsproblemen med *single-sign-on* skulle vara att använda *smart cards* tillsammans med *Public Key Infrastructure* (PKI) som bygger på asymmetrisk kryptering. Pfleeger och Pfleeger (2003) klargör arkitekturen för PKI. Det finns två olika nycklar, en publik nyckel som är allmänt känd och en privat nyckel som endast är känd av användaren. I infrastrukturen ingår en certifikatsutfärdare, CA, som är en tillförlitlig tredje part. Denne sköter hantering av publika nyckelcertifikat. I proceduren ingår även en *Registration authority*, RA, som sköter kontakten med användarna och hantering av identitet och autentisering. Den privata

nyckeln måste förvaras på ett säkert sätt. Ett sätt kan vara ett *smart card*. Detta är ett kort som kan lagra stora mängder information och skulle kunna användas för att till exempel lagra patientinformation eller bankinformation. En nyckel som lagras på ett sådant kort, använt tillsammans med pinkod eller lösenord anses idag vara ett mycket säkert identifikationssätt av användare. Tillämpningarna av PKI är många förutom *single-sign-on* till exempel; säker digital kommunikation via e-post eller e-handel och elektronisk signering (Pfleeger & Pfleeger 2003). Inom sjukvården har Säker IT i hälso- och sjukvård SITHS (Carelink, 2005) lagt grunden för en PKI-baserad arkitektur som tillsammans med *smart cards* erbjuder en säkrare inloggning.

En stor del av de problem som finns i samband med användare och informationssäkerhet anser jag vara förknippad med autentiseringssätt. Lösenord och användarnamn, som är den vanligaste formen, inbjuder, som vi sett, till en hel del sätt för en angripare att få tillgång till information och i förlängningen kanske även till hela systemet. Kostnadsmässigt finns idag inget annat sätt som tillnärmelsevis kan konkurrera, inom sjukvården finns som beskrivs ovan en PKI- baserad arkitektur framtagen sedan ett antal år tillbaka, men den har hittills inte fått någon större genomslagskraft. Ett sätt för autentisering som är säkert, billigt, enkelt och i linje med användarnas arbetssätt skulle höja informationssäkerheten rejält, men det är i dagsläget svårt att se hur ett sådant autentiseringssätt skulle vara konstruerat.

Det finns en svensk standard för informationssystem SS-ISO/IEC 17799:2005 (ISO/IEC 17799, 2005) , vilken ger mycket detaljerade instruktioner för hur säkerhetsarbete skall bedrivas på företagsnivå. Där återfinns bland annat regler för utbildning av anställda skall ske, samt hur rutinerna vid anställningars påbörjande och avslutande skall vara utformade. Även hantering av lösenord och åtkomst beskrivs. Krisberedskapsmyndigheten (2006a) har gett ut skriften Basnivå för informationssäkerhet som anger en miniminivå för informationssäkerhet. Även denna skrift bygger på standarden SS-ISO/IEC 17799:2005. Krisberedskapsmyndigheten (2007) påtalar även vikten av att informationssäkerheten lyfts upp på ledningsnivå, för att det skall bli genomslag i organisationen (Krisberedskapsmyndigheten, 2007). Jag tror att ledningens betydelse för informationssäkerheten inte nog kan betonas. Ledningen kan påverka genom sitt engagemang och genom att anslå medel för att förverkliga planerna. Utan stöd av ledningen, och en bra struktur som en standard kan innebära, får säkerhetsarbetet svårt att få genomslag i organisationen.

2.2.2. Social engineering

Social engineering är ett relativt nytt begrepp inom informationssäkerhet. Attacker som genomförs med hjälp av social engineering inriktas främst på människorna som använder informationssystemen och bygger på the *easiest way of penetration* (Pfleeger och Pfleeger, 2003). Begreppet är vidstäckt och ger utrymme för olika definitioner. Gulati (2003) anger social engineering som *"… the 'art' of utilizing human behaviour to breach security without the participant (or victim) even realizing that they have been manipulated."* (Gulati, 2003), sid. 29. Granger (2001) ger följande definition:

> *Social engineering is generally a hacker's clever manipulation of the natural human tendency to trust. The hacker's goal is to obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.*

En annan beskrivning är denna:

> *In computer security, social engineering is a term that describes a non-technical kind*

> *of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures./……./ Another aspect of social engineering relies on peoples inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are not aware of the value of the information they possess and are careless about protecting it.* (Searchsecurity, 2007).

Det är svårt att ge en kortfattad definition som innefattar hela begreppet. I mitt arbete kommer begreppet främst att belysas ur aspekten att någon skulle vilja ha tillgång till information eller system och Grangers definition är den som är mest precis och täcker in begreppet.

Enligt Granger (2001) är målet för social engineering detsamma som för hacking i största allmänhet. Tillgång till system eller information för att begå bedrägerier, göra intrång i nätverk, industrispionage, stöld av identitet eller helt enkelt för att förstöra anslutningar till system eller nätverk. De fysiska målen för attackerna skulle kunna vara militären eller myndigheterna, men även telefonbolag, finansbolag och sjukhus.

Därför fungerar social engineering

Social engineering fungerar av flera olika anledningar. Det kan vara att vi litar på auktoriteter eller personer i uniform (Granger, 2002), som reparatörer, poliser eller vårdpersonal, men som Gragg (2002) påpekar uniformer är billiga. Vi litar på beslut som fattas av andra människor inom gruppen. Argumentet ”Så här brukar vi alltid göra” är ofta gångbart. Inom social engineering manipuleras människor genom att man använder sig av människans vilja att vara omtyckt, vänlig, och hjälpsam. Även inställningen att obehagliga och negativa händelser oftast händer andra hjälper angriparen.

Bakgrunden till dessa olika reaktionsmönster kan delvis förklaras genom socialpsykologiska fenomen. Aronson et al. (2002) redogör experiment som genomfördes under mitten av 1900-talet för att utforska hur människor interagerar med auktoriteter eller andra människor i grupp. Sammanfattningsvis kan sägas att människorna lydde auktoriteten, förlitade sig på gruppens handlande och agerade inte självständigt. Detta även när det var helt uppenbart att agerandet skulle skada andra eller att gruppens slutsatser var helt orimliga. Att lita på att andra här bättre kapacitet att bedöma vad som är adekvat och relevant handlande benämns även *pluralistic ignorance* och ligger till grund för *bystander effect*. Det kan kort beskrivas så att alla i gruppen studerar varandra för att se vad som är ett adekvat beteende och korrigerar sitt eget beteende efter gruppens. När ingen annan reagerar eller handlar tas det som ett kvitto på att situationen inte kräver agerande. Åskådarnas passivitet vid en olycka brukar användas som ett exempel på *bystander effect.* (Aronson et al., 2002). När det gäller risker så tenderar vi att värdera risken för att något ogynnsamt, som tillexempel olyckor, dödsfall eller naturkatastrofer, skall hända just mig som mindre än för genomsnittet av befolkningen. Tvärtom anser vi att chansen för en positiv händelse är större för mig som enskild individ än för genomsnittet i gruppen (Aronson, et al., 2002). Människan tror sig även vara bra på att upptäcka när någon försöker att bedra henne. Vi tror oss vara över medel när det gäller att avslöja lögner och anser att våra medmänniskor är mycket lättare att lura (Levine, 2003). Dessutom utgår människor från att de flesta människor faktiskt talar sanning *the truth bias* (Martin, 2004). Våra reaktionsmönster tenderar även att automatiseras (Aronson et al., 2002). För den som kan spela på de här reaktionsmönstren ligger vägen öppen för manipulation och bedrägeri.

Genomförande av social engineeringattack

För en inkräktare som vill ha access till ett system är fördelen med att använda social engineering i jämförelse med enbart tekniska metoder, enligt Mitnick (2002) att det i de flesta fall är enklare att bara fråga efter information. En sedvanlig attack är mer komplicerad att planera och genomföra.

Mitnick (2002) beskriver ingående tillvägagångssätten som han använde sig av när han med hjälp av social engineering fick tillgång till ett antal stora och välbevakade system. I planeringen ingår att kartlägga målet för attacken. Då kan det mesta material vara användbart. Olika små fragment används för att pussla ihop helheten. Nyttig information kan hämtas från soptunnorna så kallad dumpster diving. Information som finns på skrivborden kan också användas, det kan vara allt från post-it lappar med lösenord till personallistor, möteskalendrar, olåsta dataskärmar eller genom att se över axeln när någon skriver sitt lösenord. Telefonen är mycket användbar vid social engineering. Andra sätt kan vara att skapa en falsk vänskapsrelation till någon. Ytterligare sätt att få information kan vara genom hot eller mutor, (Mitnick 2002) men det agerandet anser jag hamnar något vid sidan av definitionen som anger att offren på något vis skall manipuleras.

Social engineering kan även kombineras med teknik, till exempel genom att använda *phishing. Phishing* innebär i korthet att mail skickas till miljontals adresser i hopp om att några skall nappa och lockas i fällan och via bifogad fil eller länk luras att ladda hem skadliga program eller besöka falska hemsidor och lämna ifrån sig information tillexempel användarnamn och lösenord. Under den senaste tiden har riktade phishingattacker blivit vanligare så kallad *spear phishing*. Angreppen riktas endast mot några utvalda adresser eller ett företag, som kartläggs före attacken. Dessa attacker har större potential att lyckas då innehållet är skrivet på landets eget språk och kan se ut att komma från en känd avsändare. De har dessutom svårare att upptäckas av virusprogrammen (F- secure, 2006). Om fysisk tillgång till en dator kan uppnås, kan olika medhavda lagringsmedia, exempelvis ett USB- minne användas för att installera skadlig kod (SITIC, 2006).

Skydd mot angrepp

Framgången för dessa hot bestäms av användarnas beteende. Det är svårt att exakt peka ut vilka åtgärder som bäst skulle kunna stoppa dessa attacker och det finns troligen inte någon enkel ”one size fits all” lösning. Utbildning speciellt i kombination med en fungerande säkerhetspolicy är den lösning som det finns störst enighet om (Mitnick, 2002; Granger 2001). Gragg (2002) identifierar fyra områden för träning som mer specifikt skyddar mot social engineering. Dessa kan samman fattas i fyra påståenden. Ha kunskap om vad som kan vara värdefullt och därmed skyddsvärt, tänk på att vänner inte alltid är vad de utger sig för, det vill säga riktiga vänner, kom ihåg att lösenord är personliga, samt till sist glöm inte att uniformer är billiga i inköp.

För att utföra en attack med hjälp av dessa tekniker behövs det dels en vilja att lura människor, men även kunskap och förmåga att agera manipulativt. För den som råkar ut för en riktigt skicklig bedragare tror jag att det är det kan vara svårt att genomskåda bluffen. Nya sätt att bedra människor gör också det att det inte är enkelt att vara förberedd. Genom att medvetandegöra användarna kommer man en bit på väg. Medvetenhet om hoten, tillvägagångssätten, vad som är skyddsvärt och hur som man som användare skyddar informationstillgångarna minskar troligtvis ändå chansen för en attack skall bli framgångsrik.

2.3. Tidigare forskning

Åhlfeldt och Ask (2004) visar i sin undersökning om informationssäkerhet inom hälso- och vård att in- och utloggningsrutinerna inte fungerade tillfredställande. Rutinerna överensstämde inte med arbetssättet och det tog för lång tid att logga in och ut från systemen. Användarna använde andras login och glömde att logga ut. Lösenorden var enkla och var ofta relaterade till anhörigas namn. Deltagarna hade trots det problem att komma ihåg lösenorden och de hade inte heller önskvärd kunskap och medvetenhet om informationssäkerhetsfrågor och tillhörande hot och risker.

Svårigheten att forska om social engineering är problemen med att genomföra verklighetstrogna experiment. Orgill, et al. (2004) och Nohlberg (2005) gör båda undersökningar utan att de medverkande är fullt medvetna om det egentliga syftet. Orgill et al (2004) visar i sin studie att huvudparten av de utfrågade var villiga att lämna ut sitt användarnamn och lösenord under förespegling att detta ingick i en enkät som företaget initierat. Nohlberg (2005) undersöker i sitt arbete hur de anställda skulle agera på tre klassiska social engineering teman. Lämna lösenord via telefon, skicka uppgifter efter telefonförfrågan, samt ladda ned program via länk. Företaget och deras anställda antogs vara över medel, när det gällde säkerhetsmedvetande. Resultatet visade att de anställda inte var medvetna om hoten och att detta var en säkerhetsrisk som överskuggade de tekniska hoten.

3. Problembeskrivning

Förändringens vind blåser inom sjukvården. Det finns idag en bred politisk enighet att genomföra målen i den nationella IT-strategin (Regeringskansliet, 2006, 2007). Det finns en stor vilja hos alla aktörer att öka tillgängligheten till patientens tidigare sjukdomshistoria för alla som vårdar denne och som behöver ha tillgång till informationen. Detta gäller såväl regionalt, inom exempelvis ett sjukhus upptagningsområde, som nationellt. Inom en inte allt för avlägsen framtid planeras att den nationella patientöversikten skall vara genomförd. Allt detta innebär i förlängningen att tillgång till patientinformation kommer att öka för varje användare och enhet.

Enligt Krisberedskapsmyndigheten (2006b) sker den i samhället ständigt pågående förbättringen av informationssäkerheten, främst inom det tekniska området. De hot som de anser ökar mest är däremot olika former av social engineering, främst phishing. Av den anledningen är det viktigt anlägga ett helhetsperspektiv som tar hänsyn till både tekniska och mjuka sidor, samt även kombinationer av dessa. De anser att individers säkerhetsmedvetande och agerande är en viktig säkerhetsfaktor. Problemen inom samhällets informationssäkerhet anses snarast bero på mänskliga beteenden än brister i tekniska lösningar. Ökad kunskap och medvetenhet framförs som en nyckelfaktor för alla nivåer i samhället för att informationssäkerheten skall förbättras. Inom organisationer anses det finnas ett stort behov av kunskap om de mjuka delarna inom informationssäkerhet. En trend som kan skönjas är att tack vare att de tekniska insatserna ökar, är virusspridingen stabil eller sjunkande. Förekomsten av spyware, spionprogramm som installeras med hjälp av trojaner ökar däremot. Trenden är att skadlig kod idag sprids genom att användaren genom olika former av manipulation besöker webbsidor eller laddar ner program som innehåller trojaner. Tendensen är även att riktade attacker ökar i antal, främst gäller detta överbelastningsattacker (DDoS-attacker) (Krisberedskapsmyndigheten, 2006b). Även F-Secure (2006) beskriver ett trendbrott som noterats under 2006 vilket innebär minskad volym på virusspridningen, men istället ses en ökning av riktade attacker av olika slag. Till exempel mail innehållande skadlig kod som enbart inriktas på någon eller några få mottagare. Krisberedskapsmyndigheten (2007) framhåller att viktiga samhällsfunktioner måste ha ett gott säkerhetsskydd som förhindrar intrång och som dessutom måste vara förankrat i ledningen.

Med hänsyn till förändringen, som beskrivs ovan, dels att fler patientjournaler sammankopplas inom vården och det samhällsansvar som vilar på hälso och sjukvården, dels genom att hot mot informationssäkerhet kan förväntas i högre grad involvera den enskilde användaren, blir då den naturliga frågan om det finns handlingsberedskap inom vårdens organisationer som kan möta de ökade hot som beskrivs?

För att förhindra intrång i informationssystemen krävs att en hög nivå på informationssäkerheten inom organisationerna. Kvalitetsskillnader mellan olika organisationer och säkerhetssystem handlar inte bara om tekniskt skydd, utan användarnas agerande och säkerhetsmedvetenhet kan vara det som skiljer ett gott försvar från ett dåligt. Det måste finnas balans mellan teknisk och administrativ säkerhet, då en attack kan gå via användarna istället för via tekniken, enligt principen om att angreppet sker mot den svagaste länken.

Även om vårdpersonalen som hanterar patientinformationen har insikt om att informationen är skyddsvärd, måste de även ha kunskap om hur den skall skyddas. Digitalisering av patientinformation kräver kännedom om vilka nya hot som detta innebär och hur man som användare bäst skyddar sig mot dessa. Det bästa sättet att få kunskap om vilka uppfattningar en användare har är att gå ut och fråga dem. Material från tidigare studier visar att användarna inte

har kunskap om säkerhetspolicys, inte agerar säkerhetsmedvetet när det gäller hantering av procedurer kring autentisering (Åhlfeldt &Ask, 2004) och dessutom lätt kan falla offer för social engineering (Orgill, et al., 2004; Nohlberg, 2005). Det saknas dock i mitt tycke studier som undersöker användarnas uppfattningar om hot och deras agerande.

3.1. Problemställning

Syftet med arbetet är att undersöka användarnas upplevelse av och medvetenhet om icke tekniska hot mot informationssäkerheten för digitalt lagrad patientinformation. Följande aspekter kommer speciellt att studeras.

Vad uppfattar sjuksköterskor som säkerhetshot mot datoriserade informationssystem och informationen som lagras där?

Hur agerar de, som användare, för att skydda informationssystemen och informationen?

3.1.1. Avgränsningar

Användarna kommer i detta arbete vara avgränsat till sjuksköterskor. Avgränsningen kan hänföras till författarens egen yrkesbakgrund som legitimerad sjuksköterska, men är även intressant ur följande synvinklar. De är ofta frekventa användare av de olika datasystemen. I sjuksköterskans åtaganden ingår även att vara ”alltiallo” och hjälpa patienter eller annan vårdpersonal med olika praktiska göromål. Sjuksköterskan utför ofta många parallella arbetsprocesser, detta kan medföra stress och tidsbrist. En stor del av verksamheten pågår dygnet runt och året runt.

4. Metod

När syftet hade med arbetet hade fastställts började arbetet med att undersöka vilken information som skulle kunna ge svar på frågorna och hur den informationen skulle kunna inhämtas. I metodavsnittet beskrivs processen som ledde fram till metoden som valdes, samt genomförandet av arbetet med hjälp av vald metod.

4.1. Val av metod

Syfte och problemställning i arbetet innebar att det som skulle undersökas var användarnas medvetenhet, upplevelser och uppfattningar samt deras agerande. Metoden som valdes var semistrukturerade intervjuer. Dessutom granskades dokumenten som reglerar användarnas agerande med avseende på informationssäkerhet. Vid metodval får hänsyn tas till vad som skall undersökas och vilka data som behövs för att besvara frågorna, samt även till det bästa sättet att inhämta relevanta data. När människors handlande och upplevelser skall undersökas skulle även andra metodval kunna komma ifråga.

Fallstudier är enligt Berndtsson et. al (2002) ett sätt att undersöka fenomen i deras naturliga sammanhang. Ett eller flera fall väljs ut och fakta samlas med många olika metoder. Fallstudien resulterar i en mängd data och det är även viktigt att fallen väljs ut på så sätt att slutsatserna kan generaliseras. Denna metod skulle ha kunnat ge svar på frågorna, men förkastades, då en sådan omfattande datainsamlingsmetod riskerat att på den korta tid som stod till buds, inte ha gett den djupa kunskap som problembeskrivningen efterfrågar.

Ett annat alternativ skulle kunna ha varit observationer. Patel och Davidson (2003) anser att observationer framförallt är användbara för datainsamling som rör beteenden och skeenden i naturliga situationer, vilket förmodas ha gett svar på frågor runt användarnas beteende. Observationer bedömdes däremot inte besvara frågan om sjuksköterskornas upplevelse och uppfattningar. Även om observationer kunde ge en bättre bild av hur användarna agerar, måste då ändå någon form av intervju göras för att få svar på hela problemställningen.

Ett tredje alternativ kunde ha varit enkäter. Att denna metod inte användes berodde främst på att enkäter inte kan anses ge den djupare förståelsen för vad användarna verkligen uppfattar som hot och även användarnas handlande kan vara svårt att få fram i en enkät.

En form av datainsamling hade varit experiment där användarna utsattes för situationer där de hade olika möjligheter att agera mer eller mindre säkerhetsmedvetet. Även om ett sådant experiment skulle ge svar på frågan om människors agerande bedömdes det av etiska skäl vara ogenomförbart. Det slutliga valet stod emellan olika intervjuformer.

En helt strukturerad intervju påminner till sitt upplägg om en enkät. Intervjuaren ställer frågorna och svaren är korta och det finns ingen möjlighet till vidareutveckling eller följdfrågor. Strukturerade intervjuer lämpar sig bäst för områden med välkända och väl utforskade fenomen (Berndtsson et al, 2002) och datamaterialet från sådana intervjuer kan med fördel användas till att beräkna statistiska skillnader. Däremot lämpar sig inte den formen av intervjuer för att utforska komplicerade ämnesområden.

Intervjuformen där helt öppna frågor används benämns även som en ostrukturerad eller en fokuserad intervju (May, 2001) eller helt enkelt en kvalitativ intervju med låg grad av strukturering (Patel och Davidson, 2003). När ostrukturerade intervjuer genomförs ges den intervjuade möjlighet att fritt berätta utifrån sin egen referensram. Intervjuerna blir sinsemellan

olika och karaktäriseras av flexibilitet (May, 2001). Patel och Davidson (2003) anser att det är en fördel om intervjuaren har förkunskaper och är förberedd inom det område som skall studeras. Denna form av intervju skulle med största sannolikhet kunna ge svar på de frågor som ställdes i inledningen. Att den intervjuformen inte valdes hade två orsaker. Intervjuaren hade ingen tidigare erfarenhet av att intervjua och risken var att frågorna och svaren inte skulle motsvara det som krävts för att besvara forskningsfrågorna. Det ansågs även vara en risk att områdets komplexitet inte skulle vara tillräckligt välbekant för respondenterna och att en fokuserad intervju därför inte skulle tillföra någon ny kunskap.

Valet föll därför på att genomföra det som May (2001) beskriver som en semistrukturerad intervju. Detta är en mellanform av fokuserad och strukturerad intervju. I denna intervjuform används specificerade frågor, men intervjuaren har större frihet att liksom vid fokuserade intervjuer förtydliga och utveckla svaren. Intervjuaren har därmed möjligheten att ha en dialog med den som intervjuas. Intervjuerna formulerades efter Patel och Davidsons (2003) beskrivning. Intervjuformuläret byggdes upp efter teman som valdes för att täcka in frågeställningarna i problemställningen. Dessa förväntades ge de intervjuade möjlighet att utveckla svaren. För att kunna få med aspekter som forskaren ville skulle belysas fanns även följdfrågor antecknade. Dessa kunde också utnyttjas för att få respondenten att utveckla sitt resonemang. Styrkan i tekniken är möjligheten att få djupare kunskap i ett ämne. Detta är enklare när intervjuaren kan improvisera och ställa följdfrågor utan att behöva vara styrd av ett färdigt manuskript. Svårigheten med tekniken är att som ovan intervjuare hitta den rätta balansgången mellan att improvisera och följa manus, det vill säga de fördefinierade följdfrågorna.

4.1.1. Analys av insamlat material

Analyser av kvalitativa intervjuer kan enligt Patel och Davidson (2003) ske på ett flertal olika sätt. Varje forskningsproblem kan hävdas kräva sin unika analysvariant. Slutprodukten består ofta av en text som består både av citat från intervjuerna och egna tolkningar. Genom att läsa igenom det insamlade materialet ett flertal gånger uppträder nya kategorier och teman. May (2001) beskriver svårigheten att göra jämförelser vid helt ostrukturerade intervjuer. Vid strukturerade eller semistrukturerade intervjuer kan det vara lättare att göra komparativa analyser.

4.1.2. Validitet och reliabilitet i kvalitativa studier

Termerna validitet och reliabilitet är väl definierade i kvantitativa studier. Kvalitativa studier är naturligt nog svårare att definiera utifrån de här termerna. Patel och Davidson (2003) använder enbart begreppet validitet, vilket får täcka in alla kvalitetsaspekterna. Validitet i en kvalitativ studie, anser de, berör forskningsprocessens samtliga delar. Det är svårt att skapa entydiga regler. Övergripande kan anges att då forskningsprocessen har så stor betydelse är det viktigt att den beskrivs noga. Resultatet kan därigenom ses i perspektiv av de val som gjorts genom hela processen. För att stärka validiteten i datainsamlingen kan triangulering tillämpas. Triangulering är ett vitt begrepp. Det kan innebära att flera insamlingsmetoder tillämpas, att flera forskare studerar samma fenomen eller att forskaren väljer flera olika datakällor, till exempel olika personer. Kvalitativa studier anses inte vara generaliserbara på samma sätt som kvantitativa studier. Resultatet kan däremot ge förståelse för fenomen och hur de varierar i sitt sammanhang. Resultatet skulle därför kunna tänkas vara överförbart till liknande situationer eller sammanhang.

4.2. Genomförande

Resultatet från arbetet kommer även att redovisas i Meliorstudien, som initierats av Forsknings och Utvecklingsavdelningen (FoU) på Skaraborgs Sjukhus (SkaS) för att undersöka olika aspekter i samband med införandet av den elektroniska patientjournalen. Intervjuerna genomfördes på ett sjukhus i västra Sverige. Innan arbetet påbörjades inhämtades godkännande från berörda parter på sjukhuset för att få genomföra en studie inom forskningsområdet. Genom kontakter på sjukhuset fick jag kunskap om sjuksköterskor som var intresserade av ämnet och som kunde tänkas vara villiga att delta. Det medförde att ett flertal av respondenterna hade någon form av anknytning till införandet av den elektroniska patientjournalen. För att få tillgång till respondenter att intervjua skickades E-mail till vårdföreståndare för olika avdelningar, där syftet med arbetet beskrevs. Vissa vårdföreståndare kontaktades även per telefon. Vårdföreståndarna förmedlade sedan kontakten med de sjuksköterskor som visat intresse i frågan. Sjuksköterskorna kontaktades och tid för intervjun bokades. Samtidigt informerades återigen om innehållet i intervjun och de medverkande tillfrågades om de fortfarande hade intresse av att medverka. De flesta intervjuerna genomfördes på sjukhuset, antingen i direkt anslutning till avdelningen eller i andra lokaler. En intervju utfördes utanför sjukhuset.

Semistrukurerade intervjuer kräver ett engagemang både från den som intervjuar och de som intervjuas. Respondenter som har intresse för frågan kan förväntas ge intervjuerna ett större djup. Forskaren måste däremot vara medveten om att detta sätt att välja ut medverkande inte ger en genomsnittsanvändare. Det är möjligt och även troligt att respondenterna som visat intresse för intervjun har ett större säkerhetsmedvetande än en genomsnittlig användare. Av olika orsaker kan det även finnas en skevhet mellan människors verkliga handlande och vad de säger att de skulle göra. Frågorna som ställdes för att undersöka användarnas beteende formulerades därför, när så var möjligt, mer allmänt exempelvis ”vad tror du att dina kollegor skulle göra om…”. Som påtalats tidigare är inte intervjuformen optimal när det gäller att samla in data för att undersöka hur människor agerar. Förhoppningen var att frågornas utformning ändå skulle tillföra ny kunskap om sjuksköterskornas handlande.

Intervjufrågorna (bilaga 1) bestämdes utifrån olika huvudteman som tillsammans täckte in problemställningen. Följdfrågor lades till som komplement. En pilotstudie av intervjun genomfördes och intervjun bandades. Efter att intervjuaren lyssnat på bandupptagningarna genomfördes korrigeringar både av formuleringen av frågorna och av övrig utformning. Under intervjuerna ställdes även andra följdfrågor än de förutbestämda för att fördjupa och förtydliga respondenternas svar. Vissa bestämda följdfrågor ansågs vara ovärderliga för studien och obligatoriska, medan andra utnyttjades vid behov som ett instrument för att få respondenterna att förtydliga svaren och hjälpa intervjun framåt. Intervjuformer som innebär att intervjuaren har möjlighet att delta aktivt ställer även höga krav på att intervjuaren inte påverkar de intervjuande med sina egna åsikter. Genom att intervjuaren själv är legitimerad sjuksköterska fanns en förförståelse för ämnet. Detta gör det lättare att genomföra intervjuerna, men det finns även en risk att forskarens förförståelse färgar både intervjumaterialet och tolkningen. Vid genomförandet av ostrukturerade eller semistrukturerade intervjuer har intervjuaren en aktiv roll. Av detta förstås att intervjuaren även påverkar intervjun. Intervjuarens intention var att frågor och följdfrågorna skulle ställas på ett sådant sätt att risken att påverka minimeras. Bandinspelningarna från pilotstudien gav tillfälle att lyssna på hur frågorna ställdes och gav en medvetenhet om hur formuleringen av frågorna och ordvalet kunde påverka respondenten.

Intervjuerna varade mellan 35 och 55 min. Före intervjustart gavs en kort information om varför intervjuerna gjordes, vilken intervjuform som skulle användas samt vilka olika teman frågorna skulle kretsa kring. De intervjuade fick även en skriftig information under vilka etiska förutsättningar som intervjun ägde rum (bilaga 2). Intervjuerna spelades in på band och därefter transkriberades materialet för att kunna analyseras. Det obearbetade materialet skickades till respondenterna så att de kunde godkänna materialet. Efter att materialet hade godkänts analyserades intervjuerna enligt kvalitativa metoder. Delarna som representerades av svaren i intervjumaterialet genomlästes och olika teman och kategorier utkristalliserade sig. Därefter fogades delarna samman och en ny helhet visade sig i resultatet. Inom vissa frågeteman svarade respondenterna på ett sådant sätt att svaren gick att jämföra. I de avsnitten genomfördes en komparativ analys, för att förtydliga för läsaren hur svaren fördelade sig inom intervjugruppen. Validiteten i denna studie styrks i och med att forskningsprocessen har beskrivits, att flera datakällor i form av flera personer har används, samt att en återkoppling skett till de intervjuade, då de har godkänt utskrifterna från bandinspelningarna.

4.3. Etiska aspekter

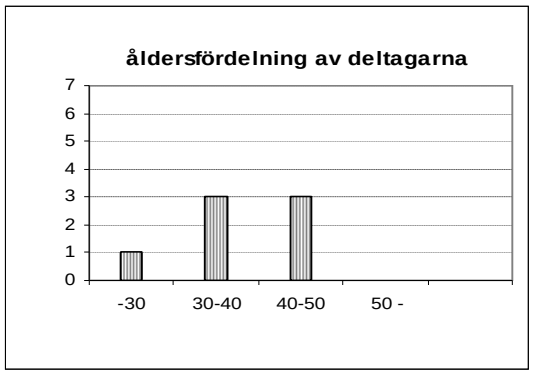
Tillstånd för att genomföra intervjuerna har dels erhållits från sjukhusledningen, dels har vårdföreståndarna på respektive avdelning informerats om syftet med studien. De intervjuade fick information om ämnesområdet för intervjuerna både när tiderna bokades och innan intervjuerna startade. Innan intervjuerna påbörjades fick de intervjuade även skriftlig information om det övergripande syftet med studien, hur materialet skulle publiceras, att materialet skulle behandlas konfidentiellt, att banden skulle bevaras, men utan att kunna knytas till någon enskild individ, samt att den intervjuade när som helst skulle kunna avbryta intervjun, utan att behöva ange något skäl (bilaga 2). Detta dokument skrevs under av både intervjuaren och respondenten.

5. Materialredovisning

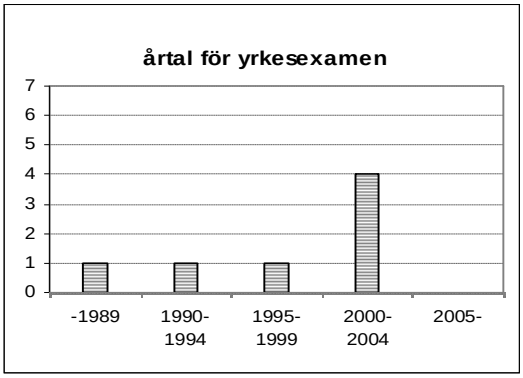
I avsnittet redovisas materialet från datainsamlingen. Intervjuerna genomfördes som semistrukturerade intervjuer på ett sjukhus i västra Sverige. Efter genomläsningen delades materialet upp i kategorier. Först presenteras deltagarna i intervjun. Därefter följer kategorierna etik och kultur, lagar, administration samt operativ och procedurell. Material som tillhör Meliorstudien finns i appendix 1. Förutom intervjumaterialet redovisas en kort sammanfattning av dokument som kan relateras till informationssäkerhet i del 5.4.1.

5.1. Deltagarna

Sju intervjuer med sjuksköterskor genomfördes. De kom från sex olika avdelningar. Sex av sjuksköterskorna var kvinnor, en var man. Åldern på deltagarna varierade mellan 25- 50 år. De hade varit verksamma som sjuksköterskor mellan 4 och 26 år. Fördelningen av ålder och tid i yrket visas i figur 3 och figur 4.



Figur 3



Figur 4

Flera av deltagarna hade olika utbildningar eller kortare kurser efter grundutbildningen till sjuksköterska. Tre hade specialistutbildning. Fyra hade datorrelaterade uppgifter på avdelningen. En var dokumentansvarig och en var förutom dokumentansvarig även IT-ombud. Två hade varit med vid införandet av elektronisk journal på avdelningen, en var med i referensgruppen för patientjournalen och en deltagare deltog i kvalitetsutveckling av patientjournalen. Två av deltagarna var även huvudhandledare för sjuksköterskestudenter som gjorde sina kliniska studier. Endast två av deltagarna hade inga speciella uppgifter relaterade till studenthandledning eller patientjournalen.

Ingen hade gått någon speciell datautbildning, utan alla var självlärda. Deltagarna använde alla datorer utanför jobbet om än i varierande omfattning och intresse. Ett par av deltagarna framhöll att de bara använde datorn när de hade behov av det, men inte mer, medan andra använde datorn varje dag. Vissa var intresserade av att lära sig mer och tyckte det var kul att behärska datortekniken. En hade arbetat med ordbehandling och Excel före sjuksköterskeutbildningen. De som hade gått högskolekurser eller genomfört sin grundutbildning under de senaste åren berättade att utbildningen hade givit dem större datavana. Elektronisk patientjournal hade införts på sjukhuset, med början under 2005. Deltagarna hade dokumenterat i elektronisk journal mellan ett halvt och ett och ett halvt år. Omdömena om att använda elektronisk journal var nästan genomgående positiva. Det beskrevs i termer som att uppgifterna blir mer lättillgängliga och det

är lättare att läsa än handskriven text. Nackdelen som nämndes var att olika avdelningar dokumenterar på olika ställen, därför kunde det bli svårt att få överblick och hitta uppgifter. Fler uppgifter om elektronisk patientjournal finns i Appendix 1

5.2.Etik och kultur

Skydd av patientuppgifter

Att skydda patientuppgifter bedömdes som viktigt. Om uppgifter från sjukvården fick spridning skulle det kunna få konsekvenser för hela personens framtid. Det var viktigt att möjligheten till obehörig åtkomst inte fanns, patienter skall till exempel inte frestas att läsa andras journaler. Flera av respondenterna kände obehag över att det fanns så mycket information tillgänglig i datasystemen. De refererade till hur de själva skulle uppleva det om deras uppgifter blev kända.

> *Jag tycker att det är väldigt obehagligt, kränkande om jag tänker mig själv, jag skulle inte vilja att det kommer ut/…./vart kommer det i cyberrymden, kan alla läsa det här, bara känslan, det är väl som att ha inbrott kan jag tänka mig, att man känner sig kränkt, vem har varit inne och rotat i mitt liv och även om det inte är så känsliga grejer kanske, men jag menar att det är ingen annan som har med det här att göra egentligen, vad jag ligger inne på sjukhuset för, det kan ju vara väldigt [känsligt], vi frågar ju en hel del i alla fall.*

Det skulle vara kränkande för den enskilda individen om uppgifterna kom ut, bara vetskapen om att någon haft tillgång till uppgifterna skulle kunna räcka. Journaler till exempel från psykiatriska vårdavdelningar gick inte att läsa, men uppgiften om att patienten hade vårdats där kunde ändå ses av alla som öppnade journalen. De kände att de själva skulle känna det obehagligt om de vid ett vårdtillfälle lämnat ifrån sig känslig information, som skulle kunna läsas vid ett annat tillfälle, då de kanske vårdades för en helt annan åkomma. De ville heller inte att vänner, anhöriga eller kollegor skulle kunna läsa deras journaler.

Patientuppgifter skyddades genom att man inte lämnade ut sina lösenord till patientjournalen. Vissa medarbetare skrev upp sina lösenord och det bedömdes av andra som en risk att anteckningarna tappades bort så att lösenordet komprometterades. Någon skulle även kunna ta del av ett lösenord genom att spionera på tangenttryckningarna när en användare loggade in. Alla användare var inte medvetna om riskerna och skyddade inte tangentbordet. De var inte heller så datavana och snabba att skriva. Även när datorer lämnades utan att man loggat ut ur patientjournalen bedömdes det vara en risk att andra gick in och läste information om patienter:

> *Ja, skulle man vilja, säg att du hade en granne du inte tyckte om, så kunde du gå till en dator som någon annan var inloggad på, det händer ju nästan varenda dag, så kunde du slå in det personnumret och titta, det är inte svårt.*

Uppfattningar om hot mot information och system

Det framhävdes det att man inte trodde att kollegorna var så illvilliga att de skulle utnyttja tappade lösenord eller öppna datorer. Man var kanske lite godtrogen och litade på sina kollegor, men alla hade ändå läsrättigheter till informationen om patienterna som de vårdade. Intrång upplevdes delvis vara svåra att förebygga, loggningen var ju bara ett stickprov och görs i efterhand och då skulle uppgifterna redan ha varit tillgängliga. Detta beskrevs som

> *skulle en person verkligen vilja komma åt ett användar- id till Melior för att sitta och läsa patientjournaler, då skulle den personen kunna göra det*

Detta skulle kunna ske genom att ringa och fråga efter lösenord eller genom hot mot en anställd.

> *Det kan ju vara att man känner någon som jobbar på sjukhuset, som man hotar eller tvingar till sig till det, det skulle ju kanske [vara] ganska lätt att spåra, men då är ju skadan redan skedd.*

Orsaker till att någon skulle vilja ta del av andra människors patientjournal uppgavs vara flera. Att en känd person ligger inne för vård uppgav de flesta skulle kunna vara en anledning. Orsaken att läsa den journalen skulle kunna vara nyfikenhet, men även möjligheten att omvandla informationen till pengar, genom att informera media. Personal skulle kunna tänkas vilja läsa journaler om anhöriga eller vänner och bekanta som var inlagda. Andra orsaker att läsa journaler som angavs var personliga motiv som nyfikenhet, illvilja, avundsjuka eller att man är ovänner. Patientuppgifter skulle även kunna användas för att få hållhake på någon, i utpressningssyfte. Patienten skulle även kunna vara en kriminell person. Organiserad brottslighet skulle även kunna tänkas handla med patientjournaler. Uppgifter om att patienter var inskrivna på sjukhus skulle kunna ge brottsliga personer tillfälle att göra inbrott i hemmet. Patienten själv skulle även kunna vara intresserad av att läsa sin journal. En av de intervjuade påtalade att dagens patienter oftast är ovana datoranvändare och att de inte skulle kunna utnyttja brister i informationssäkerheten. I framtiden kommer det däremot att finnas en annan vana vid att använda datorer, vilket gör att patienterna kommer att bli ett allt större potentiellt hot.

Hotet mot intrång ansågs i första hand vara riktat mot patientjournalen. Övriga system som innehöll patientinformation eller nätverket nämndes inte som något som skulle skyddas. Det ansågs inte speciellt troligt att det skulle finnas ett allmänt intresse av att ta del av patientuppgifter. Förutom kändisars journal, bekantas journaler och av allmän nyfikenhet hade de flesta deltagarna svårt att spontant ange fler motiv, både interna, men framför allt externa, för att någon skulle vilja ta del av patientinformationen. Brottslighet nämndes, likaså viljan att skada någon, patienterna kunde ju vara kriminella. Orimligheten av att någon extern aktör aktivt skulle begå intrång, genom att vara fysiskt närvarande på avdelningen uttrycktes av en deltagare som:

> *Om en okänd, helt främmande person kommer in på någon avdelning, det känns lite amerikansk action eller så/…/det är för mycket risk/…/för så väldigt viktig information har vi inte i våra journaler, som jag ser det*

En användare hade funderat på säkerheten gentemot allmänheten. Det borde vara möjligt för en riktigt duktig hackare att ta sig in i systemen. Att det skulle vara möjligt att ta sig in i systemen för att ändra eller läsa uttrycktes av en annan deltagare som:

> *Det tror jag ju att det finns möjligheter, det tror jag ju, jag menar att har man lyckas komma in i Pentagon, så kan man ju lyckas här också, men det är väl inget som man går och tänker på.*

Det ansågs som svårt att skydda sig mot ett sådant intrång och att ansvaret vilade på de tekniska resurserna. Ingen verkade göra någon koppling mellan ett sådant intrång och det egna agerandet. Ett intrång som skulle ge förövaren rättigheter att skriva och ändra upplevdes av några användare som obehagligt. Om uppgifter ändras skulle det kunna innebära hot mot patienter och patientsäkerheten, det skulle även kunna innebära att sjuksköterskorna skulle kunna ställas till ansvar för saker som de inte gjort. De flesta hade dock inte funderat i dessa banor och trodde inte heller att det var sannolikt att något sådant skulle inträffa. Då handlar det om brottslig verksamhet och patientinformation ansågs inte tillräckligt intressant ur ekonomisk synvinkel för att motivera externa aktörer att lägga ner resurser på att göra intrång i systemen.

5.3. Lagar och kontrakt

Deltagarna berättade om hur lagar påverkade deras handlande. De hade god kunskap om lagar, då de var desamma oavsett om uppgifterna lagrades i elektroniska journaler eller pappersjournaler. Lagen innebär att man endast har rätt att läsa journaler på de patienter som man vårdar. Exempel på när man skulle kunna bryta mot lagen var när en patient går till en annan avdelning eller annan patientgrupp inom avdelningen, eller man själv byter patientgrupp. Andra exempel som gavs var när en patient skrivs ut från sjukhuset, återkommer, men läggs in på en annan avdelning. I dessa fall vårdar inte sjuksköterskan patienten och har inte rätt att läsa journalen. Åter ett annat exempel är när avdelningen förvarnas om att en patient är på väg, sjuksköterskan läser journalen, men direktiven ändras och patienten läggs in på en annan avdelning. I det sistnämnda fallet har sjuksköterskan läst journalen på en patient som hon eller han inte har vårdat. Sjuksköterskorna skulle gärna vilja följa upp vården av patienter, som de inte längre vårdar, men de visar en medvetenhet om att det inte är tillåtet att gå in i journalen. Några sjuksköterskor ansåg, av den anledningen, elektroniska journaler som säkrare än pappersjournaler då det var lättare för en obehörig läsa en pappersjournal, utan att det märks. Någon av deltagarna menade att det fanns en gråzon för patienter som vårdades inom en avdelning. En sjuksköterska skulle kunna gå in och läsa på patienter som hon inte hade ansvar för. Det skulle i efterhand inte vara möjligt att bevisa eller motbevisa om sköterskan vårdat patienten och varit i behov att läsa journalen och av den anledningen skulle heller inget straff kunna utkrävas.

Vid anställningens början skrevs regler för datoranvändning under, bland annat reglerades där Internetanvändning, se även stycke 5.4.2.

Alla inloggningar sparades i loggfiler. Genom att gå igenom loggfilerna för de elektroniska journalerna kunde lagbrott eller brott mot interna regler för Internetanvändning uppdagas. Förekomsten av loggfilerna, samt att stickprov genomfördes, var en allmän kunskap och respondenterna tyckte att det var positivt att det fanns. Rädslan för att andra skulle använda sig av inloggade datorer eller lösenorden skulle gissas grundade sig delvis på det faktum att användaren skulle kunna ställas till svars för andras otillåtna åtgärder och inte enbart på att patientuppgifter skulle bli tillgängliga. Sjuksköterskestuderande, som hade sin kliniska placering på avdelningarna, informerades även om att loggfiler sparades både på patientjournaler och på Internet. En av deltagarna hade nyligen varit med om att en student, som hade eget inloggningskonto, kontrollerades. Studenten hade bara läst om de patienter som han/hon hade vårdat. Några av de intervjuade påtalade även patientens rättighet att begära utdrag av loggfiler från sin egen journal.

5.4. Administrativ

5.4.1. Utbildning och kunskap om informationssäkerhet

I samband med utbildning när den elektroniska patientjournalen infördes, förekom även utbildning i säkerhet. Några avdelningar hade även haft information på möten och andra träffar. Två användare hade inte fått någon utbildning i säkerhetsfrågor. En avdelning hade tagit upp säkerhetsfrågor i samband med utvärdering och repetition av rutiner kring den elektroniska patientjournalen och ämnet diskuterades mycket på avdelningen. Säkerhetsarbetet hade även tagits upp på träffar med huvudhandledare på avdelningarna och de som var IT-ombud hade kontinuerliga möten med nyheter och information om IT relaterade frågor.

Som exempel på dokument som styrde informationssäkerheten nämndes av en deltagare regler för dataanvändning, vilket undertecknas vid anställningen. Andra berättade att det fanns pappersdokument på avdelningen, ytterligare en talade om att beredskap och säkerhet hade dokument på Intranätet. Två av deltagarna kunde inte erinra sig att de hade sett några sådana dokument.

Man talade om att kunskaperna från utbildningen måste uppdateras, att det inte alltid fungerar i den dagliga stressen och när det blir slentrian. Någon tyckte sig se att brist på intresse och förståelse för datorer gav mindre kunskap om och motivation för säkerhetsarbete. Det uppgavs även att media skriver mycket om datasäkerhet, till exempel om bank och kontokortsbedrägerier och att det ökat deras eget säkerhetsmedvetande.

I denna fråga uppvisar svaren en stor variation. Några mindes inte att det förkommit någon undervisning, medan andra själva hade varit delaktiga i undervisningsupplägget på avdelningen. Utbildningen i informationssäkerhet var tätt förbundet med utbildningen i handhavandet av patientjournalen och det är osäkert hur stor andel som verkligen innehöll säkerhetsfrågor. Varje avdelning verkade ha ett stort eget ansvar för undervisningen, vilket kunde avläsas i de stora variationerna. De som hade funktioner som huvudhandledare informerade studenterna vid varje nytt pass, var 5: e vecka. En hel del av säkerhetsmedvetenheten verkar även härröra från kunskaper som är allmänna i samhället.

En av deltagarna påpekade att det finns många anställda i vården. Många är inte fast anställda utan går på kortare vikariat och timanställningar, de kan dessutom arbeta på flera avdelningar och även för olika arbetsgivare. När de arbetar måste de ha tillgång till systemen. Det är under sådana förutsättningar svårt att hålla reda på vilka som har tillgång till användar- ID men inte längre arbetar på sjukhuset.

5.4.2. Utformning av säkerhetsdokument

Efter kontakt med säkerhetsansvarig klargjordes att det fanns två dokument som de anställa fick ta del av. De fanns tillgängliga på Intranätet. De två dokumenten var dels ”Regler för datoranvändning inom sjukhusgruppen” som mer hade form av ett kontrakt som undertecknades vid anställningens början. Den styr främst regler mellan arbetsgivare och arbetstagare. Dessutom finns broschyren ”Informationssäkerhet på jobbet”, som kan ses som en kortfattad sammanfattning av främst lagar och föreskrifter. När skrifterna ställdes i relation till studien framkom bland annat att följande innehåll saknas.

- Övergripande information om hot mot och intrångsskydd av system.
- Service personal skall ha ID bricka.
- Lösenordshantering.
  - Säkra lösenord.
  - Lösenordsbyte.
  - Att lösenord inte får lämnas ut.

Ingen privat användning av Internet var i princip tillåten under instämplad tid, och följaktligen fanns inte några anvisningar för hantering av bifogade länkar och filer.

- Hantering av mail och länkar på arbetsplatsen, som skydd mot oavsiktlig nedladdning av skadlig kod.

5.5. Operativ och procedurell

5.5.1. Hantering av lösenord

Alla deltagarna valde lösenord som skulle vara lätta att komma ihåg utom en som istället valde ett som skulle gå fort att skriva. De flesta kom ihåg sina lösenord utan att skriva upp dem. En av deltagarna skrev upp lösenorden. Lösenorden bestod av ord eller namn, en använde sig av tangenternas placering på tangentbordet Att använda namn på familjemedlemmar trodde deltagarna var vanligt bland kollegorna. Flera försökte välja lösenord som de inte trodde skulle vara så lätta att gissa. En sammanfattning av trenderna i lösenordshanteringen visas i tabell 1

Tabell 1 Sjuksköterskornas lösenordshantering

Val av lösenord	**antal**	**Hantering av lösenord**	**antal**
Lätt att komma ihåg	6	Skriver upp	1
Gå fort att skriva	1	Byter regelbundet	0
Namn inom familjen	1	Ökar med en siffra	2
Ord eller andra namn	5	Samma/ liknande lösenord inom sjukhuset	5
Tangentplacering	1	Samma lösenord utanför sjukhuset	1
Svårgissade ord	4	Lånar ut till en kollega	0

På arbetsplatsen fanns flera system som krävde lösenord. Genom att först logga in till nätverket kunde användaren sedan logga in på respektive system och även gå ut på Internet. De flesta räknade upp 5-7 system som användes dagligen. För att komma ihåg lösenorden använde, de flesta deltagarna, samma eller likartade lösenord till vissa eller alla system. Ibland kunde det likväl vara svårt att komma ihåg vilket lösenord som hörde till vilket system. Om lösenord glömdes bort var det oftast i samband med lösenordsbyte eller efter längre ledighet. Lösenordet till patientjournalen och även till många av de andra systemen behövde inte bytas. Ingen talade om att de frivilligt bytt lösenord, utan lösenorden byttes endast när systemen begärde det. Till nätverket krävdes lösenordsbyte var 3: e månad. För inte glömma bort det nya lösenordet förekom det att lösenordet räknades upp med en siffra. Lösenord som användes på sjukhuset användes endast av en användare på ett ställe utan för sjukhuset. Ingen deltagare redogjorde i detalj hur deras lösenord var konstruerade, hur många tecken eller specialtecken de själva hade i lösenordet, eller vad de olika systemen krävde. Vid test av systemen visade det sig att lösenorden till nätverket och patientjournalen endast krävde minsta möjliga längd på lösenordet. Patientjournalen hade en låsningsfunktion som trädde i kraft efter tre misslyckade försök.

Ingen av deltagarna i studien hade kunskap om andras lösenord och hade inte heller lämnat ut sitt eget till någon. Detta var inte heller något som användarna trodde förekom bland andra anställda. Enda händelsen som skulle kunna leda till att man lämnade ut lösenordet var om någons inloggning inte skulle fungera, men det skulle i så fall inte kunna användas på patientjournalen, då dokumentationen i så fall skulle registreras på fel person. På en del avdelningar fanns

användarnamn och lösenord som var gemensamma. På tre avdelningar var det inloggningen till nätverket, på andra inloggning till andra system, som var gemensamma. Två avdelningar förvarade lösenorden i pärmar. På tre av avdelningarna var lösenorden så inarbetade att alla kom ihåg dem och man hade något behov av att skriva upp dem. Gemensamma lösenord till nätverket behövde inte bytas efter 3 månader.

Deltagarna arbetade dagligen med över 5 system som krävde lösenord. Dokumentationen i den elektroniska patientjournalen signeras även med lösenord. Ingen av deltagarna kunde uppskatta hur många gånger de skrev lösenord under en arbetsdag. Alla ansåg att det var många gånger per dag, lite varierande på vilka arbetsuppgifter man hade den dagen. En sjuksköterska berättade att kombinationen av system som krävde starka lösenord, regelbundna byten och system vars innehåll uppfattades som mindre väsentligt, fick till följd att man till slut inte använde systemen, därför att man inte längre kom ihåg lösenordet. Arbetssituationen har säkert en avgörande betydelse för val av lösenord. Så gott som samtliga av de intervjuade berättade att de någon gång har haft svårt att komma ihåg lösenorden. Med tanke på att många med lätthet räknar upp 5-7 system som de har lösenord till, vilket innebär att det troligtvis finns fler system, vilka inte används lika frekvent, måste svårigheten på lösenorden stå i relation till vad användarna kan förväntas komma ihåg. Jag har svårt att tänka mig att användarna skall komma ihåg kanske upp mot 10 olika lösenord, 8 bokstäver långa med stora och små bokstäver, siffror och tecken och dessutom veta vilket lösenord, som hör till vilket system och användarnamn, byta lösenorden med jämna mellanrum till ett som inte liknar det gamla och inte skriva upp dem – det känns utopiskt. Om man dessutom betänker att lösenorden skall användas varje gång ett system öppnas under dagen eller en patientanteckning signeras, får man även en förståelse för motiven till att välja lösenord som är lätta att komma ihåg, samma för flera system och vilka går snabbt att skriva.

5.5.2. Skydd av lösenord via telefon

Ingen av deltagarna trodde att de utan vidare skulle lämna ut användarnamn och lösenord till en systemansvarig, om denne ringde och bad om det. Svaren redovisas i tabell 2 och tabell 3. De olika deltagarna kommenterade det på följande sätt:

> *…… det har väl inte han med att göra……inte skulle jag bara lämna ut det, det skulle jag inte göra……om någon ringde och frågade mig jag tror inte att jag skulle säga det i och med att jag inte vet vem som ringer egentligen, jag skulle inte göra detta, absolut inte……*

Endast en säger att man absolut inte skulle lämna ut lösenordet. Fem säger att de skulle fråga vad han skulle använda det till och att det skulle krävas en mycket, mycket bra förklaring för att de skulle lämna ut det. Två av respondenterna föreslog att han kunde komma upp på avdelningen, antingen så att man istället kunde logga in honom, och på det viset undvika att uppge lösenordet eller för att visa ID brickan innan man talade om lösenordet.

> *……jag skulle väl ta reda på varför han ville ha det……jag skulle ju fråga varför han vill ha det, det skulle nog sitta långt inne innan jag uppgav det, då skulle jag nog vilja att dom kom hit och att jag loggar in dom här……då skulle dom få förklara bra, ge en väldigt bra förklaring……jag skulle väl reagera med att fråga varför han skulle ha dom och så, jag skulle nog inte lämna ut dom i första hand……*

Tabell 2 Eget agerande vid telefonförfrågan om inloggningsuppgifter

Lämna ut lösenord på telefon, eget agerande	**antal**
Jag skulle inte lämna ut	1
Jag skulle lämna ut under vissa förutsättningar	5
Ej besvarat frågan	1

Tabell 3 Kollegornas agerande vid telefonförfrågan om inloggningsuppgifter

Lämna ut lösenord på telefon, kollegors agerande	**antal**
Jag tror att andra inte skulle lämna ut	1
Jag tror att andra skulle lämna ut under vissa förutsättningar	1
Jag tror att det skulle vara möjligt/troligt att andra skulle lämna ut	4
Jag kan inte svara på hur andra skulle agera	1

De har svårt att spekulera i hur kollegorna skulle tänka, men fyra anger att de tror att det skulle vara möjligt, till och med troligt att få lösenord på detta viset, speciellt under vissa premisser. Det kunde till exempel vara att datorerna krånglat mycket eller att den som ringer är tillräckligt myndig eller skicklig. De övriga tror att kollegorna skulle tänka som de och antingen inte lämna ut lösenorden alls eller kräva en bra förklaring. En ville inte spekulera i andras beteende. De allra flesta av de intervjuade ansåg ändå uppenbarligen att det skulle kunna finnas förnuftiga argument som skulle ge en systemansvarig legitim användning av användarnamn och lösenord. Ingen av de intervjuade hade varit med om något telefonsamtal där någon hade frågat efter lösenord.

5.5.3. Skydd av nätverk och information

Att logga in och logga ut

Nästan alla deltagarna tyckte att inloggningsprocedurerna var tidskrävande. Det som framförallt tog tid var inloggningen på nätverket. För att spara tid försökte man att logga in på nätverket på morgonen och vara inloggad under hela dagen. Ibland kunde det dock hända att man blev utloggad av en läkare eller annan kollega, eftersom man var flera som delade på datorerna. Att under tidspress behöva starta upp en dator under dagen uppgav en deltagare som ett irritationsmoment. En lösning var att, redan när arbetspasset började på morgonen, starta de datorer som man behövde under dagen och logga in sig mot nätverket. Det var vanligt att användaren inte loggade ut sig från nätverket när han gick hem efter ett arbetspass. Samma person som loggat in på morgonen kunde vara inloggad även under hela kvällspasset.

Den elektroniska patientjournalen som innehåller patientdokumentation har en automatisk låsningsfunktion som träder i kraft efter 20 min. Hur ofta den lämnades öppen skiljde sig åt mellan avdelningarna. På två avdelningar angavs att man i stort sett alltid loggade ut eller låste skärmen, medan användare på två avdelningar tyckte att det var vanligt eller mycket vanligt att patientjournalen var öppen. På de resterande avdelningarna glömde man att logga ut ibland. De flesta användare lämnade någon gång programmet utan att logga ut. Deltagarna angav olika skäl; ibland var man tvingad att springa iväg snabbt, man gick bara ett kort ärende, det tog för lång tid

att logga ut, tidsbrist, bekvämlighet, dåligt uppfostrade och att man litade på sina arbetskamrater En personalkategori som sällan loggade ut ur nätverket eller programmen var läkarna.

Förutom patientjournaler används även andra system som innehåller person och patientuppgifter. Dessa system innehåller svar från olika röntgenundersökningar, provsvar från laboratorier och blodgrupperingar från blodcentraler, samt patientadministration, avdelning och sängplats för inskrivna patienter. Även där skilde sig rutinerna åt. På en avdelning loggade användarna alltid ut om inte systemen användes, medan en andra användare inte loggade ur dessa system någon gång under dagen. Anledningen till att man var inloggad på de systemen var tidsbesparing. Det är svårt att säga varför det fanns så stora skillnader mellan avdelningarna, en anledning kan vara att rutinerna skilde sig åt, men den troligaste orsaken var olika kulturer, att ansvaret för utbildningarna verkade vara delegerade till avdelningsnivå och att man på vissa avdelningar hade haft mera utbildningar och träffar där man tryckt på grundläggande rutiner, som till exempel att logga ut.

Placering av datorer

De flesta datorer var placerade på expeditioner där mycket personal arbetade och de var nästan aldrig obevakade. Det fanns dock datorer även på andra utrymmen som inte var bemannade hela tiden, till exempel rum som användes för att skriva in patienter, undersköterskornas datorer och läkarexpeditioner. Det är en paradox att det enda system som användarna genomgående anger kräver lösenordsbyte, nätverket, är det system som så gott som alltid ligger öppet på de datorer som är i bruk, ibland även på datorer som står obevakade och inte används just för tillfället.

På vissa avdelningar fanns redan datorer på patientrummen och det planerades på fler avdelningar. När varje patientrum får en egen dator ansågs det naturligtvis bli ännu viktigare att logga ur patientjournalen eller andra system som innehåller patientuppgifter.

Någon avdelning hade tidigare haft dataskärmarna i korridoren så patienterna kunde läsa över axeln, det upplevdes som mindre säkert och hade nu tagits bort. En användare berättade att de hade skärmar som var placerade så att de inte kunde skyddas för insyn av obehöriga, patienter, anhöriga eller personal från andra avdelningar. De hade påtalat detta, men ännu hade ingen förändring kommit till stånd.

Skydd mot fysisk tillgång till datorer

Om en okänd tekniker från IT-avdelningen skulle komma upp och börja arbeta med en dator som står öppen mot nätverket, skulle de flesta inte ta någon större notis om det. Olika svar visas i tabell 4. Man vet ofta att de skall komma i förväg, men det skulle inte vara otänkbart att de dök upp oanmälda. De flesta skulle kanske gå fram och fråga varför han kom, vad han skulle göra och vad som var fel, men de trodde inte att kollegorna skulle bry sig om det. Alla skulle godta svaret att han kom från IT-avdelningen och att han skulle laga något fel på datorn. Det skulle även kunna förekomma att han skulle bli inloggad till nätverket.

Ingen ansåg att han skulle behöva ha några speciella arbetskläder eftersom teknikerna ofta kommer i sina egna civila kläder. Intervjufrågan var formulerad som att han skulle ha en tröja med IT-avdelningens och sjukhusets logga. Den klädseln skulle väcka misstänksamhet hos någon. En nämner att de brukar ha sjukhustelefon i bältet, en talar om arbetsordern. Fyra av sjuksköterskorna skulle titta efter ID brickan, men övriga nämner inte detta. Kommentarer från olika användare:

……det händer ju titt som tätt här, eftersom vi har så mycket datorer, jag brukar alltid kolla först att de har ID-brickan på sig……om det kommer någon frågar man ju vad han vill, men säger han att han är från IT avdelningen och skall kolla datorerna, så skulle jag nog[tro på det]. För det har ju varit så pass mycket folk här uppe vi har haft mycket krångel med dom [datorerna]……ja, man är så koncentrerad på vad man gör själv, att man tar för givet, att så är det, dom är från IT……

Deltagarna tror att de själva är mer misstänksamma än kollegorna. Anledningen till att man inte skulle reagera är att det är så mycket folk som kommer och går. Det händer ofta att det kommer folk och reparerar datorerna och man är så koncentrerad på sitt eget jobb. Ingen av de intervjuade hade upplevt något ovanligt i samband med reparationer av datorer eller att det kommit upp personer på avdelningen som uppträtt oförklarligt. Däremot har det förkommit stölder av datorer från utrymmen som obehöriga inte skulle ha haft tillgång till.

Tabell 4 Sjuksköterskornas agerande inför en okänd IT tekniker

Okänd IT-tekniker som kommer till arbetsplatsen	**antal**
Jag skulle troligen fråga vem han var och vad han skulle göra	4
Jag tror att andra inte skulle ta någon större notis om honom	7
Han skulle kunna komma i civila kläder	7
Jag skulle titta efter attribut	4
▪ Id bricka	4
▪ Arbetsorder	1
▪ Sjukhustelefon	1

5.5.4. Internetanvändning

De flesta användare uppgav att man enligt reglerna inte fick använda datorerna till privata ärenden på arbetstid. En orsak som uppgavs var att nätet överbelastades, att bandbredden inte räckte till, okynnesanvändning skulle försvåra för dem som verkligen behövde använda nätet. Ingen uppgav att det skulle vara säkerhetsaspekter som låg bakom regeln. Trots förbudet var det ganska vanligt att man läste sin privata mail, läste tidningen eller utförde andra privata sysslor på Internet. Generellt ansågs det dock inte finnas mycket tid över för privata Internetärenden under ett normalt dagpass. De flesta menade att detta var vanligast under natten. Då var även risken för överbelastning av nätet mindre. Någon angav att Internet i dagens samhälle har blivit ett vanligt sätt att hämta information på och flera tyckte att reglerna kändes föråldrade. På en avdelning var alla arbetsdatorer spärrade mot icke arbetsrelaterade Internetsidor. Istället fanns det speciella datorer som kunde användas på utstämplad tid, vilka dessutom enligt respondenten hade bättre säkerhetsskydd än de andra datorerna.

Ingen av deltagarna uppger att de chattade på sjukhusets datorer. De flesta hade heller ingen större egen erfarenhet av chattsidor. De hade därför svårt att uttala sig om de själva eller deras arbetskamrater skulle öppna länkar på arbetsplatsen från chattvänner, vilka var för dem obekanta personer. Fördelningen av svaren visas i tabell 5. Om man var nybörjare på att surfa, av okunskap eller av obetänksamhet, tror deltagarna att deras arbetskamrater kanske skulle kunna öppna sådana länkar. Deltagarna uppgav att de var noga med att inte öppna mail från okända avsändare,

både hemma och på arbetsplatsen. Någon hade varit med om att få spam på sin E-post på arbetet. Den intervjuade ringde då till IT - avdelningen, så att de fick ta bort dem. Förutom spam hade ingen varit med om några konstiga mail på sjukhusets E-post. En av deltagarna hade varit med om ett tillfälle då ett flertal obehagliga popuprutor kommit upp på skärmen.

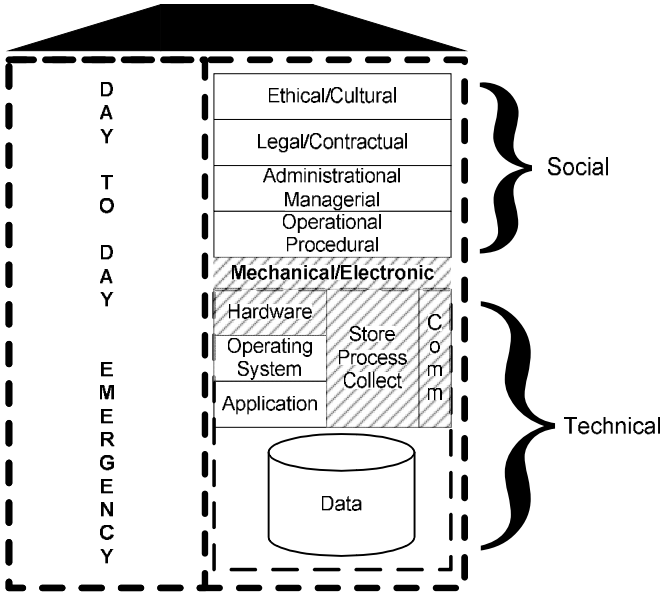
Tabell 5. Hur sjuksköterskorna ser på att öppna länkar från Internetkontakter

Öppna länkar från vänner på Internet	**antal**
Jag använder sällan eller aldrig chatt sidor för egen del	7
Jag kan inte besvara frågan om hur andra skulle agera	3
Jag tror att sådana länkar kunde öppnas under vissa premisser	4
Jag öppnar aldrig mail från okända avsändare	5

Det fanns en medvetenhet hos alla användare om att det rådde totalförbud att gå in på vissa Internetsidor, pornografiska sidor, uppgavs som exempel. Deltagarna hade även kunskap om att även besökta Internetsidor sparades i loggfiler. Ett problem som påtalades var att när någon inte loggat ut från nätverket kunde någon annan gå in på Internetsidor och den inloggade fick då stå för det. Ett annat problem var när nätverksinloggen var gemensam, då inte någon enskild användare kunde knytas till användningen av Internet. En avdelning med gemensam inloggning hade löst problemet genom att dessa datorer endast hade tillgång till arbetsrelaterade sidor. Datorer som finns i på patientrummen hade ingen access till Internet.

6. Resultat

Avsnittet innehåller resultatet som redovisas och analyseras med hjälp av *Security by consensus*; SBC – modellen (Kowalski, 1994) (figur 5). Redovisningen följs av en kort sammanfattning, analys och syntes av de huvudsakliga resultaten. SBC-modellen har ett flertal olika användningsmöjligheter. I det här arbetet användes den för att ge en tydlig konceptuell struktur av säkerhetsuppfattningar på individnivå på ett svenskt sjukhus. De vita fälten är de som finns med i resultatet. Då arbetet fokuserats på användarnas medvetenhet och agerande är det naturligt att intervjufrågorna ställdes inom de områden som innefattas av den sociala delen. Förväntan var även att svaren skulle inrymmas där. Vid analysen av materialet framkom däremot även uppgifter som måste anses höra hemma inom den tekniska sfären.



Figur 5, SBC-modellen, de vita fälten analyseras i resultatet.

Resultat relaterat till användare

Användarna hade lite olika profiler vad det gällde datavana, ålder, intresse för att använda IT-stöd och olika specialuppgifter på avdelningen. Det förekom inte så stora avvikelser mellan svaren och det går inte att relatera skillnaderna till någon speciell profil. Deltagare som var yngre eller mer datavana visade mer förståelse för problemen med säkerhet och hade även mer funderingar kring hot och risker. Orsaker till skillnader i agerande när det gäller informationssäkerhetsfrågor, kan däremot inte relateras till någon speciell profil utan får till största delen anses bero på andra orsaker, som exempelvis personlig läggning.

6.1. Social

Etik

Användarna hade medvetenhet om etik. Det fanns en samstämmig uppfattning om vikten att skydda patientinformation och patientens integritet. Att utan skäl läsa uppgifterna skulle medföra obehag för patienten och kunna vara oerhört kränkande. Att patientuppgifter kom till obehörigas kännedom skulle även kunna skada patienten. Deltagarna hade tillgång till alla journaler som

fanns lagrade i den elektroniska patientjournalen. Eget ansvar och den egna etiken avgör till viss hur detta faktum hanteras. Man tog inte del av information som man inte hade rätt till och generellt sett litade man på att andra inte heller gjorde det. Att kollegor skulle kunna göra övertramp föreföll dock inte orealistiskt. Patienter som skulle vara utsatta var de som hade en relation till någon i personalgruppen eller kända personer. Orsaken skulle kunna vara nyfikenhet, ekonomisk vinning, illvilja eller brottsligt uppsåt.

Ett par sätt att komma åt informationen nämndes. Dels genom att helt enkelt använda sitt eget inloggningskonto och i efterhand hävda att man haft legitimt skäl. Dels genom att utnyttja kollegornas inloggningsuppgifter, som man hade fått kännedom om, eller genom att utnyttja en redan inloggad dator. Detta berörs mer under avsnittet operativ. Under stycket som berör lagar visas att alla handlingar där någon tar del av information som man inte har rätt till är olaglig. Var gränsen går mellan etik och lag kan vara svårt att säga.

Kultur och uppfattningar om hot

Av tradition och kultur fanns en stark medvetenhet om vikten av att skydda informationen, den data som lagrades i patientjournalen, det ansågs som ett absolut krav. Däremot ansågs det inte finnas något egentligt strukturerat externt hot mot informationen. Interna hot av främst personal ansågs, som visas ovan vara det största hotet. Att någon patient eller anhörig av en tillfällighet skulle kunna läsa på en öppen dataskärm kunde var möjligt, men att någon utifrån skulle vilja tillskansa sig uppgifter genom att vara fysiskt närvarande på avdelningen, kändes osannolikt. Hot mot system i form av hackers ansåg vara svårt att skydda sig mot. Man hyste tillförsikt till de tekniska resurserna, intrång var inget som man kände berörde det egna säkerhetsagerandet. Det fanns inte någon medvetenhet om att de själva skulle kunna orsaka ett intrång. Få, om ens någon, hade tidigare tänkt på att någon med access till systemen skulle kunna, förutom att få rätt att läsa, även få rättigheter att skriva och ändra och vilka konsekvenser det skulle innebära.

Information i andra system t.ex. provsvar, röntgensvar och vilken patient som just för tillfället är inneliggande på vilken avdelning, är även de sekretessbelagda och kan vara känsliga för patienten, vilket i stort sett inte alls påtalades.

Lagar och kontrakt

Att studera hur sjuksköterskorna hanterar lagar ingår inte i problemställningen för detta arbete. Lagar har däremot stort inflytande på sjuksköterskornas uppfattning och agerande. Exempelvis vårdregisterlagen, som säger att anställda inom vården inte har rätt att ta del av journaluppgifter för personer, som man inte vårdar. Inom detta område är det svårt att skilja på etik och lag. Sjukhuset för loggfiler över inloggningar till alla system. Förekomsten av lagen gjorde att sjuksköterskorna många gånger satte likhetstecken mellan att följa lagen och skydd av information och system.

Även policy på sjukhuset påverkade sjuksköterskorna. I anställningsvillkoren ingick att de anställda skrev på ett avtal som innehöll regler för dataanvändning. Denna innehöll även en passus om vilka Internetsidor som var förbjudna, exempelvis pornografiska sidor. Missbruk kunde leda till avskedande. En orsak till att deltagarna i intervjun var rädda om sina olika inloggningskonton och att de var rädda för att lämna öppna datorer var att någon skulle utföra handlingar som antingen var olagliga eller stred mot interna regler. Händelser vilka de själva då skulle få stå till svars för.

Administrativ

Användarna agerade troligtvis inte med säkerhetsdokumenten som stöd. Det fanns skrivna säkerhetsdokument som de anställda fick skriva under eller erhöll på annat sätt. De flesta hade dock en diffus uppfattning om dokumenten, innehållet och var de fanns. Några kunde inte erinra sig att de någon gång hade sett dem. För genomsnittsanvändaren inkluderades information i säkerhetsfrågor i utbildningen i patientjournalen och det fortsatta ansvaret verkade delvis ligga ute på avdelningarna. Det budskap som de flesta hade tagit till sig var att logga ur, vara rädda om lösenorden, förbud mot att vara inne på Internet, samt förekomsten av loggfiler och att man var ansvarig för åtgärder som utfördes under tiden man var inloggad. Säkerhetsdokumenten verkade ha två funktioner, förutom att vara stöd i säkerhetsarbetet, reglerade de även förhållanden och regelverk mellan arbetsgivare och arbetstagare. Det saknades vissa uppgifter för att dokumenten skulle ha kunna ha varit ett fullödigt stöd för användarna. Några exempel på föreskrifter som saknas.

- Övergripande information om hot mot och intrångsskydd av system.
- Service personal skall ha ID bricka.
- Lösenordshantering.
  - Säkra lösenord.
  - Lösenordsbyte.
  - Att lösenord inte får lämnas ut.

Ingen privat användning av Internet var i princip tillåten under instämplad tid, och följaktligen fanns inte några anvisningar för hantering av bifogade länkar och filer.

- Hantering av mail och länkar på arbetsplatsen, som skydd mot oavsiktlig nedladdning av skadlig kod.

Operativ

Lösenord

Användarnas hantering av lösenord visas i tabell 1. Sjuksköterskorna skrev till övervägande del inte upp lösenorden, utan valde istället lösenord som de kom ihåg och av den anledningen bytte de inte heller lösenord. Det är ganska vanligt att lösenord återanvänds ibland i modifierad form i flera system. Flera uppgav att de tänkte på att inte välja lättgissade lösenord.

Tabell 1 Sjuksköterskornas lösenordshantering

Val av lösenord	**antal**	**Hantering av lösenord**	**antal**
Lätt att komma ihåg	6	Skriver upp	1
Gå fort att skriva	1	Byter regelbundet	0
Namn inom familjen	1	Ökar med en siffra	2
Ord eller andra namn	5	Samma/ liknande lösenord inom sjukhuset	5
Tangentplacering	1	Samma lösenord utanför sjukhuset	1
Svårgissade ord	4	Lånar ut till en kollega	0

Tabellen visar även att användarna var rädda om sina lösenord och inte delade personliga inloggningsuppgifter med varandra. Även om ett program kanske lätt skulle knäcka löseorden finns det ändå en viss säkerhetstanke bakom val och hantering av lösenorden. Ingen av de intervjuade skulle i första hand lämna ut lösenord på telefon till en anonym systemansvarig (tabell 2). Däremot lämnade det stora flertalet möjligheten öppen, under vissa förutsättningar, som ett tillräckligt bra skäl. Majoriteten tror att det skulle vara möjligt och till och med enkelt att få inloggningsuppgifter från kollegor via telefonförfrågan (tabell 3) Det stora flertalet användare anser ändå uppenbarligen att en systemansvarig skulle kunna ha en legitim anledning till att vilja ha inloggningsuppgifter. Detta är ett klassiskt sätt att angripa med hjälp av social engineering.

Tabell 2 Eget agerande vid telefonförfrågan om inloggningsuppgifter

Lämna ut lösenord på telefon, eget agerande	**antal**
Jag skulle inte lämna ut	1
Jag skulle lämna ut under vissa förutsättningar	5
Ej besvarat frågan	1

Tabell 3 Kollegornas agerande vid telefonförfrågan om inloggningsuppgifter

Lämna ut lösenord på telefon, kollegors agerande	**antal**
Jag tror att andra inte skulle lämna ut	1
Jag tror att andra skulle lämna ut under vissa förutsättningar	1
Jag tror att det skulle vara möjligt/troligt att andra skulle lämna ut	4
Jag kan inte svara på hur andra skulle agera	1

De flesta datorer som var i bruk under dagen var inloggade mot nätverket. Det tog lång tid att logga in igen, därför loggade man ogärna ut frivilligt. Deltagarna uppfattade inte det som skyddsvärda datorer, eftersom det mesta, förutom Internet, var skyddat av lösenord. Datorer som var startade och inloggade till nätverket fanns ofta på expeditioner, som sällan var obemannade, men kunde även finnas i andra mer obevakade lokaler.

Sjuksköterskorna hade däremot intentionen att logga ur patientjournalen, även om det fanns stora variationer mellan avdelningar och mellan enskilda användare. Generellt sett torde det dock inte vara svårt att hitta en dator som inte var utloggad mot patientjournalen.

En okänd IT-tekniker som kom för att reparera en dator skulle inte väcka någon större uppståndelse, de intervjuades reaktioner visas i tabell 4. De flesta skulle fråga efter ärendet, men de skulle nöja sig med svaret att det var fel på datorn. Några uppger att de skulle titta efter attribut, tillexempel i form av ID-bricka. Att någon kom upp för att laga datorer, i civila kläder, var ett vanligt förekommande fenomen. Det skulle vara enkelt att få tillgång till en dator som var inloggad not nätverket och därmed kanske även tillgång till patientjournalen om angriparen i förväg hade fått de inloggningsuppgifterna med hjälp av telefonen enligt ovan.

Tabell 4 Sjuksköterskornas agerande inför en okänd IT tekniker

Okänd IT-tekniker som kommer till arbetsplatsen	**antal**
Jag skulle troligen fråga vem han var och vad han skulle göra	4
Jag tror att andra inte skulle ta någon större notis om honom	7
Han skulle kunna komma i civila kläder	7
Jag skulle titta efter attribut	4
▪ Id bricka	4
▪ Arbetsorder	1
▪ Sjukhustelefon	1

Att använda Internet för att chatta var inte något som just dessa deltagare gjorde. Därför hade de svårt att svara på om en länk från en i övrigt okänd vän på Internet skulle öppnas på arbetsplatsen. Svaren redovisas i tabell 5. Internet användes på de flesta avdelningar, om det tidsmässigt fanns utrymme. En majoritet uppgav dock att de alltid var mycket restriktiva med att öppna E-post med okänt innehåll. Svaren på denna fråga kan vara relaterad till ålder på deltagarna och ger möjlighet till olika tolkningar. Genom att inte vara ute på chattsidor utsätter man sig inte för risken att någon med dolda motiv skickar en sådan länk. Frånvaron av erfarenhet skulle även kunna innebära att användaren har mindre kunskap och därför lättare skulle falla offer för manipulation. När en användare på det här sättet luras att besöka vissa sidor eller öppna länkar, kan det vara ett sätt att använda spear phishing.

Tabell 5. Hur sjuksköterskorna ser på att öppna länkar från Internetkontakter

Öppna länkar från vänner på Internet	**antal**
Jag använder sällan eller aldrig chattsidor för egen del	7
Jag kan inte besvara frågan om hur andra skulle agera	3
Jag tror att sådana länkar kunde öppnas under vissa premisser	4
Jag öppnar aldrig mail från okända avsändare	5

6.2. Teknisk

Applikationer

Flera av de interna systemen var försedda med förvånansvärt svag lösenordshantering. Kraven på lösenordens utformande var minimala och på vissa förekom inga krav på lösenordsbyte.

Utformningen av arkitekturen som gav tillgång till systemen, med en nätverksinloggning, som tog lång tid och ingen automatisk skärmlåsning eller dylikt, gjorde att datorer inte loggades ut och ibland lämnades obevakade i detta öppna läge, många med obehindrad tillgång till Internet.

Data

Det primära målet att skydda var data (information) som fanns lagrad i patientjournalen. Alla respondenter visade stor medvetenhet om vikten att skydda informationen som lagrades i den

elektroniska journalen. Patientjournallagen gäller för elektronisk journal, likaväl som för pappersjournal. När lagringsmediet ändrades överfördes skyddet till den elektroniska journalen. Det var angeläget att skydda datasekretessen i dessa system vilket gjordes främst på följande sätt. Lösenorden hölls hemliga. Intentionen var att logga ut ur patientjournalen. Det var viktigt att skydda skärmarna från insyn.

6.3. Sammanfattning och resultatanalys

Säkerhetsuppfattningarna byggde till stor del på att patientuppgifter skall skyddas från obehörig åtkomst. Hoten ansågs i första hand vara riktade mot patientjournalen i form av förlust av sekretess och de som till största del ansågs vilja eller kunna ta del av informationen var övrig vårdpersonal. Det ansågs viktigt att skydda lösenorden och inte lämna patientjournalen utan att logga ut. Däremot fanns det en omedvetenhet med vilka övriga åtgärder, en användare skulle kunna påverka informationssäkerheten.

Sättet att agera påverkades av:

- Etik. Ur etisk synpunkt ansågs det viktigt att skydda patientinformation, då det kan anses vara uppgifter som man har fått ett förtroende att förvalta.
- Lagar. Lagen säger att det endast är tillåtet att se på uppgifter på patienter som man har vårdrelation till. Det innebar att lösenord hölls hemliga och att det fanns en intention att logga ur programmet för att inte bli anklagad för åtgärder som någon annan hade utfört.
- Kultur. Av tradition har uppgifter om patienter skyddats och hållits hemliga. Det gäller oavsett sätt att lagra informationen.
- Tekniska förutsättningar. Utformning av informationssystemen, med många system som krävde lösenord och långsam inloggning till nätverket försvårade möjligheterna att handla på ett säkert sätt.
- Funktionalitet. Funktionaliteten fick ibland gå före informationssäkerheten. Av den anledningen valdes lösenord som var enkla att komma ihåg och gick fort att skriva. Det var även en anledning till att olika system och nätverk, inklusive patientjournalen lämnades öppna.
- Säkerhetsdokument. Dokumenten och innehållet var inte välkända för alla. Det troliga är att de inte spelade någon avgörande roll för säkerhetsmedvetenheten.
- Omedvetenhet om hot, konsekvenser och teknik. Hot som härrörde sig från andra kategorier än vårdpersonal, patienter eller deras anhöriga ansågs inte som troliga. Konsekvenser av ett obehörigt intrång ansågs till övervägande del vara förlust av sekretess eller möjligen spårbarhet. Konsekvensen för den drabbade patienten var i första hand förlust av den personliga integriteten. Däremot visades ingen medvetenhet om andra konsekvenser som förlust av tillgänglighet till data eller dataintegritet. Medvetenhet var hög om att det egna agerandet påverkade sekretessen för informationen. Däremot saknades medvetenhet om hur man som användare kunde påverka skydd för informationssystemen och hur hoten mot dem skulle kunna ta sig uttryck, och även hur en angripare rent tekniskt skulle kunna gå tillväga. Genom manipulation eller på annat sätt använda bedrägligt beteende skulle det vara ganska enkelt att få tillgång till inloggningsuppgifter och även fysisk tillgång till systemen.

7. Diskussion

I kapitlet kommer resultatet jämfört med problemställningen att diskuteras. Resultatet kommer även att jämföras med andra studier inom ämnesområdet. Processen över hur arbetet utfördes beskrivs, innehållande svagheter och styrkor, upplevda problem och de erfarenheter som kan dras. Arbetet avslutas med mer generella slutsatser och förslag på framtida forskning.

Problemställningen

Resultatet diskuteras utifrån trovärdighetsaspekter. I avsnittet undersöks i vilken mån studien kan anses ha besvarat de problemställningar som formulerats, samt vilka förklaringsmekanismer som kan knytas till användarnas handlingar. Resultatet jämförs även med tidigare forskning.

Det finns flera aspekter på svagheter i arbetet, mer ingående beskrivning finns i skildringen av arbetsprocessen. Några betänkligheter får ändå tas upp här. Antal respondenter var få. De hade till viss del likartad bakgrund och ålder. Intervjun var semistrukturerad, vilket innebar att intervjuerna till viss del skilde sig från varandra, beroende på vad varje respondent ansåg vara viktigt. Det skulle kunna innebära att påståenden som tas upp av några få, kanske skulle få motstridiga svar från de övriga intervjuade, om även de hade uttalat sig i frågan. Vid tolkningen av svaren får någon form av avvägning användas, för att se om det var rimligt att även andra respondenter kunde ha samma åsikter utifrån deras övriga svar. Vid forskning i största allmänhet och kanske vid kvalitativ forskning i synnerhet, måste frågan alltid ställas huruvida resultatet som åstadkommits är det enda möjliga. Att syntetisera ett material innebär alltid en generalisering. Forskaren får försöka att efter bästa förmåga vara trogen mot materialet. Genom att gå ut och fråga människor om deras upplevelser tankar och reflektioner tillkommer likväl ett djup i materialet som inte kan uppnås på något annat sätt.

Syftet med arbetet var att undersöka användarnas upplevelse av och medvetenhet om icke tekniska hot mot informationssäkerheten för digitalt lagrad patientinformation. Med speciell tonvikt på två aspekter.

> Vad uppfattar sjuksköterskor som säkerhetshot mot datoriserade informationssystem och informationen som lagras där?
>
> Hur agerar de, som användare, för att skydda informationssystemen och informationen?

Frågorna kommer att delas upp i två delar som behandlas var för sig.

Hot mot och skydd av informationssystem.

- Sjuksköterskan såg inte några hot mot informationssystemen, som kunde relateras till den sfär som kunde påverkas av det egna handlandet.
- Datorer som var inloggade mot nätverket, lämnades ibland obevakade.
- En okänd tekniker skulle relativt enkelt kunna få tillgång till ett inloggat system.
- Internet användes mer för att hämta information, än för sociala aktiviteter .

Deltagarna uppfattade inte att de genom sitt agerande kunde påverka skyddet av informationssystem. Hoten i form av intrång uppfattades som diffusa och nästan lite ödesbestämda och var inte relaterade till dem som användare. Datorer enbart öppna mot nätverket uppfattades inte som sårbara, då de inte innehöll någon direkt tillgång till information.

Hot mot och skydd av information

- Förlust av sekretess i patientjournaler var det allt överskuggande hotet.
- Hotet ansågs i första hand komma från personal, i andra hand patienter eller deras anhöriga, övriga externa aktörer sågs inte som något reellt hot.
- Datorerna lämnades ibland utan att de var utloggade från system som innehöll patientinformation.
- Lösenorden valdes i första hand så att de inte skulle glömmas bort.
- Lösenorden skyddades, de skrevs inte ned eller lånades ut till kollegor.
- Säkerhetsdokumenten var ofullständiga och styrde inte agerandet.
- Det skulle vara möjligt för en okänd systemadministratör att via telefon få tillgång till användarnamn och lösenord.

Lagar reglerar tillgång till patientinformation och är teknikneutrala. Det finns därför av tradition en starkt uttalad vilja att skydda patientjournalerna, oavsett om de är datalagrade eller är i pappersformat. Etiskt sett ansågs även att det var ett oavvisligt krav att uppgifterna måste förbli skyddade då förlust av datasekretess både kunde innebära skada för patienten samt vara i allra högsta grad kränkande. Att alla kollegor inte antogs ha samma höga moral förstås av att det ändå var annan vårdpersonal som sågs som det största hotet mot datasäkerheten. Icke utloggade datorer skulle kunna ge både personal och övriga möjlighet att ta del av information. Lösenorden var personliga och lånades inte ut. De skrevs inte heller ned, det resulterade i sin tur i att lösenord valdes som var enkla att komma ihåg, användes på mer än ett system och att de inte heller byttes utan anmodan av systemet. Förhållandet att inte log-ut rutinerna fungerar tillfredställande och att enkla lösenord valdes bekräftas även av Åhlfeldt och Ask (2004). Stanton et al (2005) visar det för säkerheten tyvärr negativa sambandet, att säkrare lösenord och mera frekventa byten leder till att lösenorden oftare skrivs ned. Gällande lösenordsbyte visade även hans arbete att många inte byter lösenord. Däremot visades det i den studien att många skriver ned sina lösenord, trots att de inte har speciellt säkra lösenord och att över en femtedel någon gång under sista halvåret hade lämnat ut sitt lösenord till någon inom arbetsgruppen, något sådant framkom inte i denna studie.

Agerandet baserades inte i första hand på utbildning eller riktlinjer i säkerhetsdokument. Mitnik (2002) och Granger (2001) framhåller båda vikten av säkerhetspolicy och utbildning i kampen mot social engineering. Åhlfeldt och Ask (2004) visar även i sin studie användarna var i avsaknad av utbildning och klara riktlinjer som kunde ge kunskap och stöd i det dagliga arbetet. Få av deltagarna i denna studie kunde med klarhet redogöra för vilka dokument som fanns och utbildningen verkade variera från person till person och mellan avdelningarna. Det var känt för de flesta var man skall vara rädd om sitt lösenord och logga ut ur journalen. Motiven var delvis att skydda informationen, men även skydd för personalen mot att bli ställda till svars för andras otillåtna handlingar.

Social engineering

Tre frågor baserade på en tänkbar social engineering attack ställdes. En visade att en okänd IT-tekniker inte skulle väcka någon större uppmärksamhet, och lätt få tillgång till nätverket, några skulle leta efter olika attribut som ID-bricka eller fråga vad han skulle göra. De trodde inte att deras kamrater skulle vara lika misstänksamma. En sådan attack har alltså goda chanser att

lyckas, med en förfalskad ID bricka är den närmast hundraprocentig. Den andra frågan om att lämna ut användarnamn och lösenord till systemansvarig på telefon ser vid första påseendet ut att vara ett misslyckande för bedragaren. Ingen skulle lämna ut sitt lösenord. Ser vi närmare på svaren så ser vi att de allra flesta skulle lämna ut lösenordet, under vissa premisser, främst ett gott skäl. Ett mycket gott skäl är just vad en bedragare kommer att ha. De flesta trodde att deras kamrater skulle kunna lämna ut även utan ett bra skäl. Att dessa två bedrägerier fungerar har delvis samma grund. *Auktoritet.* Både systemansvarig och IT tekniker får betraktas om auktoriteter, speciellt som deltagarnas inte har egna kunskaper inom området (Aronson et al., 2002). *Uniformer*. IT-teknikernas civila vardagskläder och attribut är också ett slags uniform (Granger, 2002), intervjuaren överarbetade frågan och satte på honom en tröja med sjukhusets och IT avdelningens logga på, vilket väckte viss misstänksamhet. *Sanning och lögn*. Vi utgår från att människor talar sanning och även om så inte vore fallet, tror vi att vi själva skulle genomskåda lögnerna, vilket vi anser våra medmänniskor tyvärr inte är så bra på. Det kan vara en förklaring att till de stora skillnaderna mellan hur respondenterna trodde att de själva skulle reagera och hur de bedömde kollegornas handlande (Levine, 2003; Martin, 2004). *Pluralistic ignoranc*, I fallet med IT tekniken skulle det även kunna vara så att gruppen omedvetet rättar sig efter vad de andra gör, om ingen annan reagerar tas det som intäkt för att det inte finns någon anledning att reagera (Aronson et al., 2002). *Olyckor drabbar andra*. Vi tror inte att vi själva skall drabbas av olyckor eller andra obehagliga händelser (Aronson et al., 2002).

Den tredje frågan på detta tema handlade om att öppna länkar från Internet. Det visade sig att många inte använde nätet på detta sätt för egen del och därför är det svårt att säga något om detta skulle vara en möjlig väg för en förövare. Några av deltagarna trodde att inte att andra skulle ha något motstånd mot att öppna sådana mail eller länkar på arbetsplatsen. Många poängterade däremot spontant att de själva aldrig öppnade okända mail. Anledning till att frågan togs med var att detta skulle kunna vara en variant på en riktad attack som använder kombination av social engineering och teknik, som benämns för spear pfishing. Denna typ av attack är den typen av bedrägerier som haft en markant ökning under det sista året. (Krisberedskapsnämnden, 2006b, 2007; F-secure, 2006) och kan vara något som vi får se mer av i framtiden. Anledningen till att den skulle lyckas bygger delvis på samma klassiska principer. *Olyckor drabbar andra* och. *Sanning och lögn* kan även appliceras på detta tema.

En verklig social engineering attack skulle ha så många fler manipuleringssätt att ta till. Det går inte att jämföra en skicklig bedragare, med några frågor i en intervju som ställs utan något riktigt sammanhang. I verkligheten kanske många skulle manipuleras utan att de enligt Gulatis (2003) definition, ens vet om att de blivit manipulerade. Eller motsatsen skulle kanske även vara möjlig, om än inte lika trolig, en yrkeskår som jobbar med människor kanske genom att använda sin magkänsla skulle genomskåda tricken. Att social engineeringsattacker är en säkerhetsrisk bekräftas även av tidigare forskning (Nohlberg, 2005; Orgill et al., 2004). För att få riktigt genomslag kan attacken även kombineras med teknik. De oskyddade nätverken öppnar upp för både en falsk IT-tekniker, en städerska, en anhörig eller en patient att genom tillexempel ett manipulerat USB - minne eller via Internet installera program som kan registrera tangenttryckningar, inloggningar till de olika programmen eller ta över datorn.

Det får betraktas att problemställningen med de förbehåll som angetts tidigare får anses vara besvarad. Resultatet belyser hur sjuksköterskor, enligt sina egna värderingar, ser på hot och hur de handlar för att skydda det som är värdefullt. Resultatet innehåller även material som kanske inte till fullo innefattas av problemställningen. Det kan ses som en svaghet i arbetet att resultatet och

materialredovisningen är bredare än vad problemställningen anger. Jag övervägde att utesluta vissa delar, men fann att allt var en enhet. Lagar och etik styrde agerandet, likaså hade handlingarna samband med säkerhetsdokumenten och applikationernas utformande. Mitt ställningstagande att behålla dem grundar sig på att jag anser att de delarna ger en ram och en förståelse för övriga svar. Utan att de uppgifterna finns med skulle slutsatser som dras inom ramen för problemställningen inte anses som lika vederhäftiga, då upphovet inte finns redovisat.

Arbetsprocessen

Området valdes därför att ett intresse fanns för just säkerhetsrelaterade aspekter inom vården ur ett administrativt/icke-tekniskt användarperspektiv. Inriktningen var initialt bred, men smalnade så småningom av. Svårigheten i den delen var att få en problemställning som var tillräckligt smal. Under litteraturstudierna till bakgrunden väcktes många intressanta frågor, som var och en kändes lika omöjliga att förkasta. Det var dessutom svårt att klä sina tankar med ord och ge dem en betydelse som var tydlig och klar och som inte kunde missförstås.

- Utformning av intervjufrågor

Då intervjuer valdes som metod för datainsamlingen innebar det att intervjufrågor måste utarbetas som kan tänkas ge svar på frågeställningarna. Även här är det svårt att föreställa sig vilka frågor som skall ställas och hur frågorna skall formuleras för att ge svar som motsvarar problemställningen. Det kan alltid diskuteras varför vissa frågor finns med och varför andra frågor inte finns med. Detta var en semistrukurerad intervju. Vid sådana intervjuer är det viktigt att de intervjuade berättar om sina åsikter, erfarenheter och upplevelser inom ett ämnesområde. Frågorna är därför formulerade så att de kan förväntas täckas in av vardagliga situationer och sjuksköterskornas kunskap. Trots det upptäcktes det under intervjun att vissa frågor inte var relevanta för huvuddelen av respondenterna. Frågan om att chatta på Internet, gav inte som förväntat svar på hur respondenterna skulle hantera länkar från osäkra källor på Internet, utan svaret blev istället att dessa representanter för användarna inte utnyttjade chattsidor på Internet. Vissa frågor kan tyckas ligga utanför ramen för problemställningen, det gäller till exempel de som enbart handlar om den elektroniska patientjournalen. De fanns med därför att inställning, upplevt funktionalitet och så vidare även kan ha betydelse för upplevelsen av informationssäkerhet. I efterhand visade det sig även att patientjournalen förknippades så starkt med informationssäkerhet av respondenterna, att utan frågor på den hade troligtvis även annat intervjumaterial blivit lidande. Den egna förförståelsen som sjuksköterska var till hjälp vid utformningen av frågorna.

- Val av respondenter

Respondenterna anmälde sitt intresse för att delta. Vissa av namnen vidarebefordrades från sjukhuset, därför att de var intresserade av elektronisk journal och aktiva på ett eller annat sätt i den vardagliga administrationen av journalen. Andra kontakter gick genom avdelningarna och vårdföreståndarna. Deltagarna kan därför antas vara mer positiva till att använda IT som stöd för det dagliga arbetet, urvalet kan därför på intet sätt ses som slumpmässigt. Rekryterings sättet gjorde att alla deltagarna var kända för någon annan i organisationen. Det är ett förfaringssätt som är vanligt inom denna sektor. Detta faktum påverkade redovisningen av materialet. Genom att göra en profil över varje användare som sedan användes vid citat och även vid andra avvikande åsikter, hade det varit lättare att koppla ihop användare, bakgrund och resultat. Citaten hade även visat tydligt om det endast var en användare som citerades, eller om flera olika källor använts. Detta förfarande hade givit ett positivt tillskott till arbetet, men min åsikt är att det inte

hade gått att göra användarprofiler utan att löftet som givits om konfidentialitet hade brutits, enligt vad som redovisas ovan. Det är ett argument som inte går att ifrågasätta, därför förkastades det sättet att redovisa.

- Vet respondenten svaren

Anledningen, vilken till viss del berörts redan vid metodvalet är svårigheten att fråga en person hur denne eller andra skulle kunna tänkas agera. Bedömningen av sitt eget och andras handlande kan inte bli mer än en uppskattning av sannolikheter och måste givetvis värderas efter det. Svaren i en intervjuundersökning kan däremot ge en extra dimension, som inte kan fås vid till exempel en observation. Respondenten får tillfälle att kommentera och reflektera över sitt och andras handlingssätt, vilket ger en djupare förståelse för bakomliggande mekanismer och värderingar som styr handlingarna. I det här arbetet gavs förklaringar som ibland var intressantare än agerandet i sig, men själva resultatet måste trots allt ses med en viss sund skepsis.

- Vill respondenten ge sanningsenliga svar

En annan svårighet med just intervjuer i detta ämne, är att det ofta ligger en öppen eller underförstådd kritik av handlingssättet. På de flesta frågor finns ett politiskt korrekt svar, det vill säga vad instruktioner, policys och sunt förnuft säger att man borde svara och ibland ett annat svar, som är det verkliga agerandet. Var de intervjuade så ärliga, speciellt när de visste att resultatet skulle komma att presenteras för arbetsgivaren att de gav ett uppriktigt svar? Min uppfattning är att en hel del svar var av den arten, att handlingarna gick stick i stäv med vad som respondenterna visste var rätt. Av den anledningen anser jag att svaren lämnades med en vilja att berätta om de verkliga förhållandena.

- Intervjuarens påverkan på intervjuerna

Syftet med olika former av kvalitativa intervjuer är att få respondenten att tala fritt om ett ämne. I och med intervjun har en mer samtalsliknande form är det oundvikligt att intervjuaren påverkar resultatet. Under intervjuernas gång lär sig även intervjuaren materialet, vilket gör att den sista intervjun skiljer sig från den första. Att intervjua är en teknik som kräver träning. Då intervjuaren var ovan med tekniken var det ofrånkomligt att frågor ibland ställdes som kunde uppfattas som ledande eller att intressanta uppslag då och då inte följdes upp. Intensionen var dock att påverka respondenterna så lite som möjligt och att låta alla få berätta fritt utifrån de olika temana.

- Hur intervjuarens förförståelse påverkar materialet

Då intervjuaren själv är sjuksköterska var det lätt att förstå facktermer och kontexten inom vilka de intervjuade arbetade. Det gjorde det roligt och lätt att genomföra intervjuerna. Men det kan även innebära en risk på flera sätt. Intervjuaren kan omedvetet fylla i luckor i materialet från sin egen erfarenhet. Det finns även en risk att den intervjuade identifierar sig mer med respondenterna än med sitt forskningsuppdrag. Att lyfta fram brister och kritisera sin egen yrkeskår känns som att svika ett förtroende. Förförståelsen skulle även kunna ha medfört att analysen av intervjuerna hade forskarens erfarenheter som mall och att viktiga fakta då hade förbisetts och resultatet hade inte blivit korrekt. Det går aldrig att bortse från tidigare erfarenheter, men medvetenhet om problemen gör att förhoppningsvis påverkan blir mindre.

- Att tolka kvalitativa intervjuer genom att räkna

Antalet medverkande vid intervjuerna var endast sju stycken, Det är givetvis ett för litet antal för ett statistiskt säkert material. Dessutom var intervjuformen semistrukturerad, vilket innebar att frågorna kanske inte ställdes i samma kontext och på samma sätt varje gång. I de fall där det var möjligt att ge någon uppfattning om svarsfördelningen har tabeller och grafer används. De skall inte ses som någon absolut sanning utan visar enbart trenderna inom frågeställningen. De finns främst med för att öka läsbarheten.

- Tolkning av resultat

Intervjuerna generade 5-6 timmars inspelade band, vilka i sin tur transkriberades till ett sextiotal sidor text. Ifrån den textmassan syntetiserades resultatet, som endast är på några sidor och slutsatserna är ännu kortare. Varje gång som texten omarbetas försvinner ett visst innehåll. Ett svar på bandet, som genom sitt sätt att uttalas, får en viss entydig betydelse, kan vid utskrift ge ett mer mångfacetterat intryck. Att vara trogen materialet innebär på detta vis inte enbart att vara trogen varje bokstav i texten, utan att även på ett annat mer subtilare plan återge innehållet. Varje gång texten syntetiseras utelämnas vissa fakta. Kopplingar och mönster som inte genast är tydliga framstår under tiden som materialet bearbetas. Arbetets resultat är beroende på den person som utfört tolkningen. Under arbetets gång måste forskaren hela tiden ställa frågan om sammanställningar och tolkningar görs på ett riktigt sätt. Under tiden som arbetet med att bearbeta materialet pågått har därför det alltmer syntetiserade materialet jämförts med källan, det vill säga utskrifterna av intervjuerna och ibland även med banden.

- Sammanfattning av processen

Den roligaste delen av arbetet har varit att genomföra intervjuerna, deltagarna har alla varit positiva till att medverka och de har med stor generositet delat med sig av sina erfarenheter. De svåraste momenten i studien har varit att skriva intervjufrågorna och att sedan sammanställa intervjuerna. Efter intervjuernas genomförande sågs luckor i materialet, inom vilka områden fler fördjupningsfrågor borde ha ställts, eller frågor som var ställda så att svaren gav möjligheter till olika tolkningar. Att intervjuer som metod är tidskrävande var inte okänt för författaren. Det är även svårt att beräkna tiden som åtgår, då möten skjuts på framtiden på grund av förhinder av olika slag. Att inte genomföra intervjuerna för komprimerat upplevdes dock vara en fördel, då intervjumaterialet på så sätt transkriberades och bearbetades kontinuerligt. På så sätt växte materialet fram successivt, vilket gjorde det lättare vid den slutliga bearbetningen. Om det hade varit möjligt att avsätta mer tid hade det varit värdefullt med fler intervjuer. Fördelningen av deltagarna hade kunnat bli bredare, med bättre fördelning både åldersmässigt och med avseende på bakgrund.

Validiteten i kvalitativa intervjuer fastställs i och med att forskningsprocessen går att följa. De steg som utstakades i metodavsnittet har sedan i stort sett följts under hela processen och av den anledningen kan anses att validiteten är fastställd.

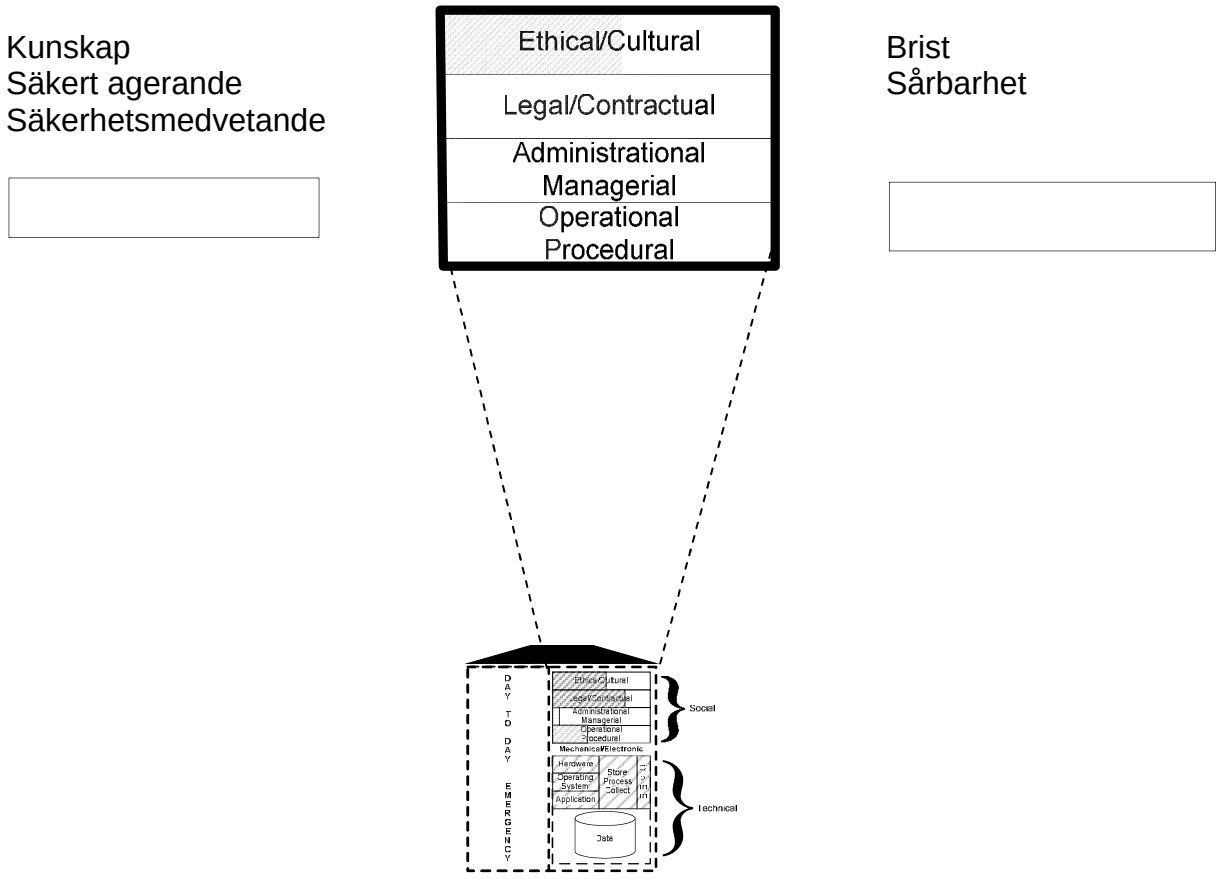
7.1. Slutsatser

Antalet intervjuade var litet, vilket gör att det finns en viss osäkerhet i materialet. Det kan vara svårt att generalisera kvalitativa resultat. Trots det finns det vissa genomgående tendenser som gör att jag anser att vissa mer generella slutsatser kan dras.

Även om det kan sägas finnas brister i skyddet av den elektroniska patientjournalen, med troligen svaga lösenord som inte byts, datorer som lämnas öppna mot journalen och dataskärmar som inte är optimalt placerade, så får det till viss del anses att en för övrigt god lösenordshantering, där lösenorden hålls hemliga, en hög medvetenheten om lag och etik samt en stark intention att skydda informationen kan antas till viss del väga upp en del av dessa brister.

Däremot kan användarna sägas utgöra en risk därför att inga kopplingar görs mellan användarbeteende och externa intrång i system, kunskap om säkerhetsdokument är låg och dokumenten har luckor och är inte utformade för att ge riktlinjer för skydd av informationssystemen. Säkerhetsdokumenten fokuserar i första hand på att skydda information i patientjournalen och på interna hot, snarare än på att skydda system från intrång.

Arbetet visar två sätt att angripa med hjälp av social engineering som skulle kunna betecknas lyckosamma. Användarna kan därmed visas vara en stor riskfaktor. Social engineering tillsammans med de ovan påtalade bristerna i lösenordshantering, icke fungerande utloggningsrutiner och användarnas omedvetenhet om sin egen roll för att avvärja intrång, gör detta till ett hot som måste tas på största möjliga allvar.



Figur 6 Användarnas säkerhetsmedvetande och sårbarhet relaterat till olika områden.

I figur 6 visas användarnas säkerhetsmedvetande och inom vilka områden sårbarheten är störst. Den skuggade delen anger en uppskattning av användarnas säkerhetsmedvetande inom respektive

område och den ofärgade sårbarheten. Bilden visar att sårbarheten främst återfinns i bristen på utbildning och en kultur som säkerhetsmässigt inte ser övergripande på hot utan endast inriktas på skydd av en specifik del. Dessa två faktorer tillsammans bidrar till att agerandet på den operationella nivån visar brister i säkerhetsmedvetande.

Arbetet ger svar på användarnas uppfattning om hot och deras agerande och jag vill ändå poängtera att de visar en stor medvetenhet om vikten att skydda informationen för obehörig åtkomst. Det ligger inte inom ramen för detta arbete att spekulera över orsaker till brister. Men kan det vara på plats att påpeka att säkerhetsarbete är en managementfråga, som kräver stöd och prioritet från högsta ledningen i en organisation. Det krävs ekonomiska resurser för att genomföra tekniska förbättringar för att öka användbarheten av systemen ur informationssäkerhetssynpunkt. Utbildning som ger användarna förståelse för sin egen roll som säkerhetsvakter för systemen kräver likaså ekonomiska satsningar. Arbetet fokuserar inte heller på att bedöma sannolikheten för en attack mot sjukhuset. Däremot är hälso- och sjukvård en samhällsviktig verksamhet, vilket ställer höga krav på en acceptabel basnivå på informationssäkerheten Det kan vara värt att nämna några tänkbara konsekvenser av att informationssäkerheten korrumperas. Medborgarnas förtroende kunde undergrävas. Tillgång till information om patienter skulle kunna ligga till grund för brottslig verksamhet. Ett kusligt scenario är intrång som innebär att dataintegriteten eller tillgången till systemen skadas. Ett sådant scenario måste en samhällsinstitution som vården göra allt för att förhindra. Det här arbetet visar att det är en lång väg att gå.

Framtida forskning

SBC- modellen möjliggör jämförelser av resultat från olika studier. Den skulle kunna användas för att undersöka och jämföra tekniska såväl som sociala sårbarheter, både inom vården som inom andra branscher. Forskningsområdet skulle kunna vara informationssäkerhet i allmänhet, men även social engineering med den form av självskattning som används i denna studie. Social engineering är som redan nämnts ett svårt område att bedriva forskning inom. Ett annat sätt att gå vidare vore att genomföra någon form av penetrationstest, som kunde realiseras under acceptabla etiska former. Mycket av resultatet i det här arbetet kan förknippas med formen för autentisering, användarnamn och lösenord, därför skulle det vara ett ämne för jämförande forskning att undersöka användarbeteende under andra betingelser exempelvis där smarta kort används som identifikation och behörighetstilldelning

Referenslista

Aronson, E. Wilson, T.D. & Akert, R. M. (2002) *Social psychology* (4th ed). Upper Saddle River: Prentice Hall.

Berndtsson, M. Hansson, J. Olsson, B. & Lundell, B. (2002) *Planning and implementing your final year project- with success!* London: Springer- Verlag.

Boddy, D. Boonstra, A. & Kennedy, G. (2005) *Managing information systems.* Essex: Pearson Education Limited.

Carelink. (2005) [Online]. http://www.carelink.se/dokument/om_carelink/doc_20051123132036.pdf. [Hämtad 2007-03-26].

Chen, D. & Doumeingts, G. (2003) European initiatives to develop interoperability of enterprise applications—basic concepts, framework and roadmap. *Annual Reviews in Control, 27,* 153–162.

F-secure (2006) [Online]. http://www.f-secure.com/2006/2/ [Hämtad 2007-04-15].

Gragg, D. (2002) *A Multi-Level Defense Against Social Engineering* [Online]. SANS Institute. Available from: http://www.sans.org/rr/papers/index.php?id=920 [Hämtad 2007-03-25].

Granger, S. (2001) *Social Engineering Fundamentals* [Online]. Security Focus. http://www.securityfocus.com/printable/infocus/1527 [Hämtad 2007-03-20].

Gulati, R. (2003) *The Threat of Social Engineering and Your Defense Against It* [Online]. SANS Institute. http://www.securitytechnet.com/resource/security/hacking/1232.pdf [Hämtad 2007-03-27].

Haux, R. (2006) Health information systems- past, present, future. *International Journal of Medical Informatics, 75,* 268-281.

ISO/IEC 17799 (2005) *Ledningssystem för informationssäkerhet - Riktlinjer för styrning av informationssäkerhet* Stockholm: SIS förlag.

Kowalski, S. (1994) *IT Insecurity: A Multi-disciplinary Inquiry.* Diss. University of Stockholm. Report series No. 94-040, Stockholm.

Krisberedskapsmyndigheten (2006a) *Basnivå för informationssäkerhet (BITS)* [Tillgänglig online]. www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/KBMs%20publikationsserier/Rekommenderar/bits_rek_2006_1.pdf [Hämtad 2007-03-01].

Krisberedskapsmyndigheten (2006b) *Samhällets informationssäkerhet, lägesbedömning, 2006*. [Tillgänglig online]. www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utredningar%20och%20remissvar/Utredningar-uppdrag/lagesbedomning_infosakerhet_%202006_slutlig.pdf [Hämtad 2007-04-02].

Krisberedskapsmyndigheten (2007) *Samhällets informationssäkerhet, lägesbedömning, 2007*. [Tillgänglig online]. http://www.krisberedskapsmyndigheten.se/EPiBrowser/Publikationer/Utredningar%20och%20remissvar/Utredningar-uppdrag/lagesbedomning_infosakerhet_%202007_slutlig.pdf .se. [Hämtad 2007-04-02].

Levine, R. (2003). *The Power of Persuasion.* Hoboken, NJ: John Wiley & Sons Inc.

Martin, B. (2004). Telling lies for a better world? *Social Anarchism*, 35, 27-39.

May, T. (2001) *Samhällsvetenskaplig forskning.* Lund: Studentlitteratur.

Mitnick, K. (2002) *The art of deception.* Indianapolis: Wiley Publishing, Inc.

Nohlberg, M. (2005) *Social Engineering Audits Using Anonymous Surveys – Conning the Users in Order to Know if They Can Be Conned.* In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005

Orgill, G., Romney, G., Bailey, M., Orgill, P. (2004) The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems, Proceedings of SIGITE'04, Salt Lake City, UT 2004

Patel, R & Davidson, B (2003) *Forskningsmetodikens grunder* (3dje uppl.). Lund: Studentlitteratur.

Pfleeger, C. & Pfleeger, S. H. (2003) *Security in computing* (3rd ed.). Upper Saddle River: Prentice Hall.

Raghupathi,W. (2002) Information technology in healthcare. A review of key applications. I: K. Beaver (red.) *Healthcare information systems* (2nd ed.) Auerbach Publishers Inc.

Regeringskansliet (2006) *Nationell IT-strategi för vård och omsorg*. [Tillgänglig online]. http://www.regeringen.se/content/1/c6/05/96/62/abac6cb0.pdf. [Hämtad 2007-01-10].

Regeringskansliet (2007) *Nationell IT - strategi för vård och omsorg. Lägesrapport 2007.* [Tillgänglig online]. http://www.regeringen.se/content/1/c6/07/95/69/3e99ef98.pdf. [Hämtad 2007- 04-05].

Search security. (2007) [Online]. http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html. [Hämtad 2007-06-01].

SFS 1980:100. Sekretesslag. [Tillgänglig online]. http://rixlex.riksdagen.se. [Hämtad 2007-01-20].

SFS 1985:562. Patientjournallag. [Tillgänglig online]. http://rixlex.riksdagen.se . [Hämtad 2007-01-20].

SFS 1998:544. Lagen om vårdregister. [Tillgänglig online]. http://rixlex.riksdagen.se. [Hämtad 2007-01-20].

SFS 1998:204. Personuppgiftslag. [Tillgänglig online]. http://rixlex.riksdagen.se. [Hämtad 2007-01-20].

SIS (2003). SIS Handbok 550. *Terminologi för informationssäkerhet.* Stockholm: SIS Förlag AB.

SITIC (2007) [Online]. http://www.sitic.se/publikationer/rapporter/risk-vid-anvaendning-av-usb-minnen-med-u3-funktionalitet [Hämtad 2007-04-18].

Socialstyrelsen (2004) *Patientsäkerhet och patientsäkerhetsarbete* [Tillgänglig online]. http://www.socialstyrelsen.se. [Hämtad 2007-02-15].

SOSFS 2005:12. Socialstyrelsens föreskrifter om ledningssystem för kvalitet och patientsäkerhet i hälso- och sjukvården. [Tillgänglig online]. http://www.sos.se/sosfs/2005_12/2005_12.htm. [Hämtad 2007-06-01].

SOU 2006:82: Patientdatalag. [Tillgänglig online]. http://www.regeringen.se. [Hämtad 2007-01-20].

Stanton, J. M. Stam, K. R: Mastrangelo, P. & Jolton, J. (2005) Analysis of end user security behaviours. *Computers & security.* 24, 124-133.

Stuewe, S. (2002) Interface tools for healthcare information technology. I: K. Beaver (red.) *Healthcare information systems* . Auerbach Publishers inc.

Thorell, J. (2005) *Paginas stora IT-lexikon.* Sundbyberg: Pagina Förlags AB.

UsersAward. (2004) *Vård IT-kartan-Användare och IT-system inom svensk vård och omsorg*. Stockholm: UsersAward.

Wikipedia (2007) [Online]. http://en.wikipedia.org/wiki/Information_security. [Hämtad 2007-06-01].

Åhlfeldt R.-M. & Ask, L. (2004) *Information security in electronic medical records: A case study with the user in focus.* In CD-ROM Proceedings of the 4th Security Conference, Las Vegas, USA, 30 – 31 March 2005.

Bilaga 1

Intervjufrågor

1. Inledning
   Först vill jag be dig att berätta lite om dig själv, din yrkesbakgrund och datavana.
   Följdfrågor.
   a. Vilka andra utbildningar har du?
   b. Hur länge har du jobbat i Melior?

2. Datajournaler och tillgänglighet.
   Kan du berätta lite vad du tycker om att använda data journaler?
   Följdfrågor.
   a. Hur tycker du det är med tillgängligheten till uppgifter när du jobbar i journalen?
   b. Ligger systemen nere?
   c. Tycker du att inloggningen är tidsödande?
   d. Från vilket läge loggar du in?

3. Lösenord.
   Jag vill att du berättar lite om vad som är viktigt för dig när du väljer lösenord.
   Följdfrågor.
   a. Vad gör du när du glömmer bort lösenorden?
   b. Var förvarar du ev nedskrivna lösenord?
   c. Återanvänder du lösenord inom sjukhus eller utanför sjukhuset?

4. Logga in och logga ut och loggfiler.
   Kan du berätta lite mer om det här med att logga in och framförallt logga ut?
   Följdfrågor.
   a. Loggar man alltid ut?
   b. Om inte hur vanligt är det att man inte gör det?
   c. Vad tror du att det i så fall beror på att man inte loggar ut?
   d. Vad tror du att det kan bli för konsekvenser av att man inte loggar ut?
   e. Har man kollegor emellan kännedom och/eller använder sig av varandras inloggningsuppgifter användarnamn och lösenord i de olika systemen? Vad är din uppfattning i den frågan?
   f. Har ni gemensamma inlogg någonstans?
   g. Var förvaras i så fall lösenorden?
   h. Jag skulle gärna vilja höra vad du tycker om att allt du gör på datorn sparas i loggfiler?
   i. Tänker du även på, när du är inne på Internet på sjukhuset, att även de sidorna loggas och vad är din åsikt om det?
   j. Vill du tillägga något om lösenord och login?

5. Korta scenarion.
   Du skall få några korta frågor som du får besvara och gärna fundera högt över och fråga om du vill ha fler uppgifter.
   a. Systemansvarig ringer och frågar efter användarnamn och lösenord. Hur tror du att dina kollegor skulle reagera och hur skulle du själv reagera?

b. En kille från It avdelningen kommer upp och skall fixa något fel på datorerna. Han har en tröja med sjukhusets och it avdelningens logga. Hur tror du att du och dina arbetskamrater i allmänhet skulle regera om han satte sig vid en ”öppen dator” (till nätverket) och började jobba?

c. Idag är många inne på olika sidor för specialintressen där man har vänner. Om man går in när man är på sjukhuset och en sådan chatt kompis skickar en länk till en sida med en häftig motorcykel eller en fin hund antingen via nätet eller via e-mail adress. Tror du att det skulle göra någon skillnad på om man var hemma eller på jobbet när man öppnade den? Hur skulle du och hur tror du att dina kollegor skulle tänka?

6. Vad tror du om sannolikheten för att något av det här skulle hända på din arbetsplats?
   Har du någon gång hört talas om eller själv varit med om någon liknande incident?
   Telefonsamtal?
   Någon som kommer till jobbet och ställer fel frågor?
   Konstiga mail?

7. Berätta lite om hoten som du anser finns både mot patientens uppgifter och mot hela datasystemen när fler och fler uppgifter blir tillgängliga på samma plats.
   Följdfrågor.
   a. Av vilken anledning skyddar vi patientuppgifter och vad skulle kunna hända om vi inte gjorde det?
      Vad skulle kunna hända om tillgången till Melior och patientuppgifterna där skulle hamna i fel händer?
      Vem skulle vara intresserad?
      Vad skulle man använda uppgifterna till?

   b. Hur tror du att det skulle kunna gå till att. ta sig in i datasystemen dvs få rättigheter att förändra systemen?
      Vem tror du skulle vilja göra det?
      Vad skulle det användas till?
      Vad skulle hända?

8. Berätta lite om hur, var och av vem du har fått utbildning eller kunskap om säker datahantering.
   Säkerhetspolicy.
   Kan man läsa om detta någonstans?
   Är utbildningen kontinuerlig?

9. Är det något mer som du vill berätta som du tänkt på när det gäller det här ämnet?

Sista frågan Kan du göra en uppskattning hur många gånger du skriver lösenord per dag?

Bilaga 2
Till dig som medverkar i intervjustudie.

Denna intervju kommer att ingå i en studie på Högskolan i Skövde, som behandlar informationssäkerhet i samband med användandet av datajournaler. Resultatet kommer att publiceras i form av en C-uppsats på Högskolan i Skövde under 2007 och ingår även i Meliorstudien som genomförs på SkaS.

Innehållet i denna intervju kommer att behandlas helt konfidentiellt och i det slutgiltiga resultatet kommer inte något som kan identifiera den intervjuade att finnas med. Bandupptagningar kommer att bevaras, men de kommer inte att kunna knytas till någon person. Bandupptagningarna kommer att transkriberas och renskrivas, därefter kommer du som intervjuad ges tillfälle att läsa igenom materialet och förtydliga eller rätta till efter dina önskemål.

Du som intervjuas kan när som helst under intervjun avbryta denna, utan att behöva ange något skäl.

Som intervjuare förbinder jag mig att följa ovanstående.

:……..

Kerstin Karlsson Student Högskolan i Skövde SSE 02 IT

Jag har som intervjuad läst igenom dessa villkor och godtagit dem.

Ort…… Datum……

Namn……

Förtydligande……
Appendix 1.

Material till Meliorstudien

I samband med att elektronisk patientjournal infördes på SkaS initierades Meliorstudien av Forsknings och utvecklingsavdelningen FoU på Skaraborgs Sjukhus SkaS. Under hösten 2006 gick inom ramen för Meliorstudien en enkät ut till Melioranvändare. Enkäten är inte publicerad men material som berör den här studien återfinns efter den här texten. I enkäten framkom att användarna kände en tveksamhet inför frågan om patientens integritet alltid kunde skyddas i elektroniska patientjournaler. Så många som 61,9 % av läkarna och 38,6 % av sjuksköterskorna instämde inte alls eller till liten del på den frågan. Gällande SkaS säkerhetspolicy svarade nära 60 % av läkarna och 50 % av sjuksköterskorna att de ansåg sig ha ganska god kännedom om säkerhetspolicys. Dock instämde runt 30 % till liten del eller inte alls på frågan. När det gäller utloggningsförfarandet instämde en stor majoritet helt eller delvis i påståendet att de alltid loggar ut när de lämnar datorn. Likafullt var det ändå över 20 % av sjuksköterskorna och över 25 % av läkarna som inte alltid loggade ut.

Syftet med min studie var specifikt inriktat på informationssäkerhet och användarnas uppfattning om hot och agerande. Det föll sig dock naturligt att mycket i intervjuerna kom att handla om Melior och den elektroniska patientjournalen. Även aktuella säkerhetsdokument på sjukhuset lästes igenom. De två områdena behandlas i detta appendix.

Inställning till den elektroniska patientjournalen Melior
Deltagarna hade dokumenterat i elektronisk patientjournal i mellan ett halvt till ett och ett halvt år. Omdömena om att använda elektronisk journal var nästan genomgående positiva. Fördelarna beskrevs exempelvis i termer som att systemet är ganska lätt och användarvänligt, smidigt, uppgifterna blir mer lättillgängliga, uppgifterna kunde vara medicinering, konsultsvar eller uppgifter från tidigare vårdtillfälle. Övriga synpunkter var att man har alltid tillgång till patienternas journal, att det är lätt att hitta data, lättläst i jämförelse med handskriven dokumentation eller att elektronisk journal spar tid, förhindrar dubbelarbete och ökar patientsäkerheten i och med att alla uppgifter som behövs finns åtkomliga. Elektronisk journal ger även mer struktur åt dokumentationen och patientarbetet. Bra utarbetade mallar kunde ge stöd i det dagliga arbetet för sjuksköterskan och stöd för uppföljningar.

Det som i stort sett av alla framhölls som en nackdel, var att olika kliniker och avdelningar hade olika riktlinjer för under vilka rubriker i journalen sjuksköterskorna skulle dokumentera. Även inom avdelningarna kunde det i början vara svårt att få alla att dokumentera på samma ställe. Detta fick till följd att sjuksköterskorna, speciellt när patienter flyttades mellan avdelningarna, fick leta i hela journalen för att hitta informationen. Som en sjuksköterska uttryckte det:

> *”Från början när Melior infördes hade det varit väldigt bra om man hade bestämt att här och så här dokumenterar vi, klart slut, inget folk som dokumenterat på något annat sätt...då hade vi hittat i varandras journaler.”*

Dessutom ansågs det vara svårt att se helheten, att journalen var svåröverskådlig, något som blev extra tydligt när patienter vårdades under längre tid på sjukhuset. Sökfunktion eller någon form av sammanfattning av det viktigaste som hänt med patienten efterfrågades. Journalen innehöll inte heller någon rättstavningsfunktion. Om användarna inte lärde sig sökvägar och

kortkommandon och kunde det ta tid att navigera i journalen. Det fanns en del tvivel om att just Melior var det bästa patientjournalsystemet, men ingen av deltagarna var negativ till övergången till elektronisk journal. En av de intervjuade hade vid ett tillfälle varit med om att en läkaranteckning kunde ändras av en sjuksköterska. Förutsättningen var att läkaren dikterat anteckningen, som sedan lagts in i journalen, men att den ännu inte blivit signerad. Att något sådant var möjligt hade förvånat sköterskan.

Ingen av användarna hade varit med om att de inte fått tillgång till patientjournalen på grund av oplanerat driftstopp, under tiden som de använt systemet. Det fanns reservsystem där sjuksköterskan har läs- men inte skrivrättigheter. Några av deltagarna var oroliga för den dagen då ett större oplanerat avbrott skulle komma. Att inte ha möjlighet att skriva under en kortare period upplevdes som hanterbart, men tanken att inte komma åt journalen vare sig för att kunna skriva eller för att läsa, upplevdes som en närmast katastrofal situation.

Hur är användarnas agerande relaterat till sjukhusets informationssäkerhetspolicy
Användarna hade främst tillgång till två dokument om informationssäkerhet. Det va dels Regler för datoranvändning inom sjukhuset, vilket alla nyanställda fick skriva på vid anställningens början och innan de tilldelas behörighet till nätverk och system. Dels delades en broschyr, Informationssäkerhet på jobbet, ut till de anställda. I den mån de inte fanns i pappersformat på avdelningen, fanns de att hämta på Intranätet, Där fanns även en mer omfattande skrift Instruktioner för informationssäkerhet, samt mer information exempelvis hur granskningen av loggfiler går till. Om inget annat anges är källan i den fortsatta texten till Regler för datoranvändning eller Informationssäkerhet på jobbet.

Lösenordshantering
Säkerhetsdokumenten anger

> ”Varje användare ska logga in på nätverk med sitt personliga användar ID och lösenord. Identitetsinnehavaren ansvarar för att datorn används till avsett ändamål om denne inte kan visa annat.”
>
> ”Du skall ha ett användarnamn och lösenord som aldrig får lånas ut Användar- id och lösenord får aldrig vara identiska med varandra. Tänk även på att inte använda lättgissade lösenord. Och kom ihåg att du alltid är skyldig att skydda dina lösenord. Om en otillåten åtgärd spåras till ditt användar- id och du har lånat ut det till din arbetskamrat, kan du bli ansvarig”.

Användarnas agerande stämde till stor del överens med policyn, dock förekommer det lösenord som skulle kunna vara lätta att gissa.

Det som saknas i säkerhetsdokumenten är
- Säkra lösenord
- Lösenordsbyte
- Att lösenord *aldrig* får lämnas ut

Flera av de testade systemen medgav *mycket* låg säkerhet för lösenord, de krävde varken en viss längd eller teckenkombination av lösenorden eller lösenordsbyte. Ett sätt, visserligen långt ifrån

optimalt, att ändå erhålla en viss säkerhet skulle då istället vara att ange riktlinjer i säkerhetsdokumenten för hur lösenorden skulle väljas och bytas. Idag får man anta att de en del lösenord skulle kunna listas ut av kollegor och flesta skulle knäckas av ett program på kort tid. Dilemmat med att säkra lösenord under förutsättningarna som sjuksköterskorna arbetar har tagits upp i redovisningen av intervjuerna. Det är svårt att ha säkra lösenord till så många system, utan att skriva upp dem. Som det ser ut idag har de flesta samma lösenord till många system. Så många har liknande eller samma lösenord till systemen att om ett lösenord knäcks är risken stor alla systemen ligger öppna. Deltagarna var noga med att inte låna ut lösenorden, däremot poängterade ett flertal att de inte skulle lämna ut lösenord till en förmodad systemansvarig utan en bra förklaring, En rejäl höjning av säkerhetsnivån på policyn skulle därför vara att tillägga att det *aldrig finns ett skäl för att lämna ut sitt lösenord till någon under några förutsättningar*.

Procedurer kring att skydda information och system från tillträde av obehöriga

Säkerhetsdokumenten anger:

> ”Lämna inte ett påloggat system utan uppsikt. Lika självklart som att du inte låter känslig information ligga framme på ditt skrivbord, lika naturligt är det att skydda vad som står i din dator. Placera därför din datorskärm så ingen obehörig kan ta del av informationen. Går du ifrån din dator skall du alltid logga av eller använda en skärmsläckare med lösenord.”
>
> ”Varje användare ska logga in på nätverk med sitt personliga användar- ID och lösenord. Identitetsinnehavaren ansvarar för att datorn används till avsett ändamål om denne inte kan visa annat.”

Här finns möjligheter till olika tolkningar av texten. Om dokumenten tolkas som att ett påloggat system även innebär nätverkssystemet, så följer ingen av de intervjuade dokumenten

- Inloggningen till nätverket lämnades påloggat, utan uppsikt
- Den som loggat in på nätverket avslutade ibland sitt arbetspass utan att logga ut
- Andra program inklusive patientjournalen lämnades ibland öppna
- Några datorskärmar var placerade på ett sådant sätt att obehöriga kunde ta del av systemen
- Det användes gemensam inloggnings ID till nätverket.

Då de intervjuade uppgav att det tog lång tid att logga in på nätverket, har jag svårt att tänka mig att det går att få efterlevnad av en regel som anger att nätverket skall loggas ut. Det fanns deltagare som inte tyckte sig hinna logga ur patient journaler eller övriga system. Datorer som var öppna mot nätverket, var även i de flesta fall öppna mot Internet. Det var inte heller ovanligt att patientjournalen lämnades utan att logga ut, detta varierade dock mellan olika avdelningar och olika användare. Datorer som var startade och inloggade till nätverket kunde till exempel finnas på läkarexpeditioner, patientrum eller lokaler som användes för att skriva in patienter. Jag kan tänka mig att ett presumtivt intrångsförsök skulle kunna genomföras av en patient, en anställd, med eller utan befogenheter att använda datorerna, men även en helt utomstående person. Dessa datorer var sårbara därför att de stod öppna för manipulation utan att de upplevdes visa någon sekretessbelagd information och de anställda därför kanske inte alltid tänkte på att skydda dem.

Det som saknas i säkerhetsdokumenten är att alltid se efter ID bricka när personer som inte är kända kommer till avdelningen för att hämta utrustning eller utföra servicearbete.

Internetanvändning

Dokumenten säger:

> ”Datorer, programvara inklusive e-post system är arbetsredskap. Det är förbjudet att ladda ner, installera, lagra, sprida eller titta på material som t ex innehåller pornografi, rasistisk propaganda, hot, förtal, uppmaning till droganvändning, våld, diskriminering.”
>
> ”Undantagsvis är det tillåtet att använda datorutrustningen i begränsad omfattning, på icke arbetstid med beaktande av ovanstående och enligt överenskommelse med närmsta chef.”

De intervjuade följde dokumenten i så måtto att de var medvetna om förbudet att gå in på vissa Internetsidor. Däremot var det ganska vanligt, att de anställda, när de hade tid, använde Internet till privata ärenden. En anledning för de anställda att vara restriktiva med Internetanvändning var begränsningar i kapaciteten. Jag anser att Internet i dagens samhälle har blivit ett så etablerat kommunikationssätt, att det får anses vara svårt att få efterlevnad av policyn genom att helt förbjuda användningen.

Det som saknas i säkerhetsdokumentet är hantering av länkar och mail på arbetsplatsen, detta för att förhindra att de anställda av misstag eller genom manipulation laddar hem skadlig kod, som virus, trojanska hästar eller annat spionprogram.

Sekretesshantering

Dokumenten säger:

> ”Inga ändringar i lagen pga att man datoriserar. Dina registreringar loggas och granskningsrutiner finns. För att kontroller att gällande regler efterföljs har arbetsgivaren rätt att utan underrättelse till användaren kontrollera/granska enskilds användning av datorutrustning”

Här har sjuksköterskorna kännedom om rutinerna och lagar. Loggningen och granskningsrutinerna anses dock vara ett grovmaskigt nät. Under vissa förutsättningar skulle den som ville kunna missbruka tillgången till patientuppgifter utan att bli upptäckt eller genom att hävda att de hade behov av att läsa journalen.

Utdrag ur Meliorenkäten. Genomförd 2006 på SkaS

	Jag kan alltid lita på att patientens integritet skyddas med elektronisk journal				Total N=518 92,3%
	Instämmer helt	Instämmer till stor del	Instämmer till liten del	Instämmer inte	
Läkare	3	21	25	14	63
	4,8%	33,3%	39,7%	22,2%	100,0%
Sjuksköterska	14	140	64	33	251
	5,6%	55,8%	25,5%	13,1%	100,0%
Undersköterska	27	66	32	15	140
	19,3%	47,1%	22,9%	10,7%	100,0%
Kurator	2	4	0	2	8
	25,0%	50,0%	,0%	25,0%	100,0%
Sjukgymnast	2	11	4	2	19
	10,5%	57,9%	21,1%	10,5%	100,0%
Arbetsterapeut	0	11	0	0	11
	,0%	100,0%	,0%	,0%	100,0%
Dietist	0	1	1	0	2
	,0%	50,0%	50,0%	,0%	100,0%
Annan	5	14	2	3	24
	20,8%	58,3%	8,3%	12,5%	100,0%
Total	53	268	128	69	518
	10,2%	51,7%	24,7%	13,3%	100,0%

	Jag har god kunskap om SkaS regler och riktlinjer för informations- ochsäkerhetsfrågor (policy)				Total N=535 95,4%
	Instämmer helt	Instämmer till stor del	Instämmer till liten del	Instämmer inte	
Läkare	5	38	16	6	65
	7,7%	58,5%	24,6%	9,2%	100,0%
Sjuksköterska	46	130	75	6	257
	17,9%	50,6%	29,2%	2,3%	100,0%
Undersköterska	33	69	35	10	147
	22,4%	46,9%	23,8%	6,8%	100,0%
Kurator	4	4	0	0	8
	50,0%	50,0%	,0%	,0%	100,0%
Sjukgymnast	5	10	4	0	19
	26,3%	52,6%	21,1%	,0%	100,0%
Arbetsterapeut	4	4	3	0	11
	36,4%	36,4%	27,3%	,0%	100,0%
Dietist	0	0	2	1	3
	,0%	,0%	66,7%	33,3%	100,0%
Annan	11	8	6	0	25
	44,0%	32,0%	24,0%	,0%	100,0%
Total	108	263	141	23	535
	20,2%	49,2%	26,4%	4,3%	100,0%

	Jag loggar alltid ut från den elektroniska journalen när jag lämnar datorn				Total N=535 95,4%
	Instämmer helt	Instämmer till stor del	Instämmer till liten del	Instämmer inte	
Läkare	19	28	11	7	65
	29,2%	43,1%	16,9%	10,8%	100,0%
Sjuksköterska	71	130	35	21	257
	27,6%	50,6%	13,6%	8,2%	100,0%
Undersköterska	104	38	6	0	148
	70,3%	25,7%	4,1%	,0%	100,0%
Kurator	7	1	0	0	8
	87,5%	12,5%	,0%	,0%	100,0%
Sjukgymnast	11	6	1	1	19
	57,9%	31,6%	5,3%	5,3%	100,0%
Arbetsterapeut	5	5	1	0	11
	45,5%	45,5%	9,1%	,0%	100,0%
Dietist	0	1	0	2	3
	,0%	33,3%	,0%	66,7%	100,0%
Annan	18	4	1	1	24
	75,0%	16,7%	4,2%	4,2%	100,0%
Total	235	213	55	32	535
	43,9%	39,8%	10,3%	6,0%	100,0%