INTERNATIONELLA HANDELSHÖGSKOLAN
HÖGSKOLAN I JÖNKÖPING

Smarta Kort

En del av en intelligent IT-lösning i hälso- och sjukvården?

Filosofie magisteruppsats inom Informatik

Författare: Johanna Isaksson
Therése Sanne

Handledare: Jörgen Lindh

Framläggningsdatum 2006-08-29

Jönköping Augusti 2006

JÖNKÖPING INTERNATIONAL BUSINESS SCHOOL
Jönköping University

Smart Cards

A part of an intelligent IT-solution within the Health Care field?

Master's thesis within Informatics

Author: Johanna Isaksson
Therése Sanne

Tutor: Jörgen Lindh

Jönköping Aug. 2006

Magisteruppsats inom Informatik

Titel:	**Smarta Kort – En del av en intelligent IT lösning i hälso- och sjukvård?**
Författare:	**Johanna Isaksson**
	Therése Sanne
Handledare:	**Jörgen Lindh**
Datum:	**2006-08-29**
Ämnesord	**Smarta kort, Aktiva kort, Informationssäkerhet, IT-säkerhet, Nationell IT-strategi, Hälso- och sjukvården, Carelink**

Sammanfattning

Bakgrund: IT-säkerhet ingår i begreppet informationssäkerhet som avser all säkerhet vid hantering av information inom en organisation. God IT-säkerhet handlar om att hitta rätt nivå med tillhörande åtgärder och nya IT-lösningar, men detta är inte enkelt att införa i organisationer och speciellt inte i vården som dagligen hanterar känslig information. Under senare år har regeringen tillsammans med landsting och kommuner fått upp ögonen för vilken nytta IT kan utgöra inom vården. Intresseorganisationen Carelink arbetar aktivt för att skapa förutsättningar att använda IT inom vården, och under våren 2006 har även regeringen presenterat en Nationell IT-strategi.

Projektet SITHS, Säker IT inom Hälso- och Sjukvården, drivs av Carelink och bygger på att använda smarta kort som säker identifikation. Korten kan bland annat användas som passerkort och vid inloggning till ett datasystem för att säkerhetsställa en identitet.

Syfte: Syftet med denna uppsats är att undersöka förutsättningarna för hur smarta kort, som en del av en total säkerhetslösning, kan förbättra IT-säkerheten inom hälso- och sjukvården.

Metod: Studien påbörjades med en genomgång av lämplig litteratur om informationssäkerhet, smarta kort samt vårdinformatik. Den empiriska studien utfördes sedan på Länssjukhuset Ryhov i Jönköping, som är ett av Sveriges nyaste sjukhus. Här genomfördes både kvalitativa och kvantitativa studier, då vi valde att göra ett antal intervjuer samt en enkätundersökning bland vårdgivarna. Intervjuerna gjordes för att få en djupare förståelse för organisationen, och enkätundersökningen för att undersöka attityderna till dagens datoranvändning samt hur säkerheten kring datoriseringen upplevs bland de anställda.

Resultat: Enligt studien kan smarta kort förbättra IT-säkerheten inom hälso- och sjukvården genom att skapa en säker identifiering vid användning av IT-stöd. Smarta kort kan även bidra till en förenklad in- och utloggningsprocess i ett datorsystem, vilket i sin tur leder till bättre spårbarhet samt ökad mobilitet bland användarna. Undersökningen visar att majoriteten av användarna inte är emot den förändring ett smart kort kan bidra till, utan snarare tvärt om.

Master's Thesis in Informatics

Title:	**Smart Cards – A part of an intelligent IT-solution within the health care area?**
Author:	**Johanna Isaksson**
	Therése Sanne
Tutor:	**Jörgen Lindh**
Date:	**2006-08-29**
Subject terms:	**Smart Cards, Information security, IT-security, IT-strategy, healthcare, Carelink**

Abstract

Background: IT-security is included in the concept of information security, which considers all the security of handling information within an organisation. Good IT-security is about finding the right level of measurement, however, it is hard to implemement new IT-solutions in an organisation, particularly within the health care field, where sensitive information are handled daily. Lately the Swedish government, together with county- and city council, understand the importance of IT and health care. Carelink, an organisation of interest, is working actively for the presumption of benefit by using IT within the health care field. During spring 2006 the Swedish government introduced a national IT-strategy. SITHS, Säker IT inom Hälso- och sjukvården, is a project running by Carelink and is based upon using Smart Cards as an identification. Smart Cards can be used as accesscards for logging on to a computersystem in an organsiation in order to secure an indentity.

Purpose: The purpose with this thesis is to investigate the assumptions for how Smart Cards, as a part of a total security solution, can increase the IT-security within the Healt Care field.

Method: The study was initiated with literature and suitable references to informationssecurity, Smart Cards and Healthcareinformatic. Our empirical study was carried out at Ryhov Hospital in Jönköping, one of Sweden's newest hospitals. Both qualitative and quantitative studies were conducted, because we chose to do interviews and surveys. The interviews were conducted in order to get a deeper understanding for the organisation and the survey was made in order to investigate the attitudes among the nurses and doctors about the security of computer use.

Result: Smart Cards can, according to our studie, increase the IT-security within the Health Care field by creating a safer identification with the use of IT-support. Smart Cards can also make the process of logging on and off to a computer system easier, which leads to better logging and mobilisation. The study also demonstrates that users are not afraid of the changes a smart card will represent within their organization.

Författarnas tack

Vi skulle vilja tacka följande personer som gjort den här studien möjlig för oss. All delaktighet, intervjuer samt goda råd har uppskattats av författarna.

Jörgen Lindh, Filosofie doktor
Universitetslektor informatik
Internationella Handelshögskolan i Jönköping

– för bra handledning och feedback i vårt uppsatsarbete

Jan Günther-Hanssen, IT-planeringschef, Länssjukhuset Ryhov

Inger Offenbacher, informationssäkerhets handläggare, Länssjukhuset Ryhov

Anders Jacobsson, IT-konsult på IT-Centrum, Landstinget Jönköping

Jan Svensson, IT-säkerhetsansvarig, säkerhetshandläggare samt personuppgiftsombud, Landstinget Jönköping

IT-kontaktpersoner samt anställda på **Ambulansenheten, Medicinkliniken, Radiologen, Rehabiliteringsmedicinska kliniken och Ögonkliniken**

– för bra handledning samt materialinsamling som gjorde den här studien möjlig

---

Övriga personer som hjälpt oss under arbetes gång med korrekturläsning samt viktig feedback

---

Johanna Isaksson och Therése Sanne

Internationella Handelshögskolan i Jönköping

2006-08-24

Innehåll

Figurer

Bilagor

1 Inledning

I följande kapitel kommer vi att redogöra syftet med uppsatsen samt de IT-säkerhets problem som kan uppstå inom vården. Vi kommer även att diskutera den Nationella IT-strategin, intresseorganisationen Carelink samt smarta kort, då dessa ligger till grund för vårt syfte. Vidare förklaras en del begrepp, avgränsningar samt vilka som kan vara intresserade av vår uppsats. I slutet på inledningen återges även dispositionen av uppsatsen.

1.1 Bakgrund

IT-säkerhet är något som berör oss alla. Hoten och riskerna för IT-brott ökar i takt med att datoranvändningen tilltar och numera tillåts en konstant uppkoppling till Internet. IT-säkerhet syftar till att förhindra obehörig åtkomst och obehörig eller ofrivillig förändring eller avbrott vid databehandling samt dator- och telekommunikation (Mitrović, 2005). IT-säkerhet är en del av begreppet informationssäkerhet som avser all den säkerhet vid hantering av information, som till exempelvis sekretess, inom en organisation. Sekretess innebär enligt Bishop (2005) att en organisation vill dölja information eller resurser som inte får göras tillgängliga eller avslöjas för obehöriga. Data är, enligt Bidgoli (2002), efter människor, det viktigaste som bör skyddas och därför krävs ett fullständigt dataskydd. Hot idag kan vara naturkatastrofer, avsiktliga och oavsiktliga intrång.

God IT-säkerhet handlar, enligt Mitrović (2005), om att hitta rätt nivå med tillhörande åtgärder. För att hitta rätt nivå gäller det att först inventera alla system och tjänster i organisationen för att på sätt hitta vad som passar för just den organisationen. Smarta kort är en del av en IT-lösning som enligt Bidgoli (2002) kan öka säkerheten i en organisation. Korten kan bland annat användas som passerkort och vid inloggning till ett datasystem, för att identifiera att det är rätt användare som har behörighet till informationen. Genom att använda någon slags accesskontroll kan sekretessen bevaras.

Nya IT-lösningar är inte lätta att införa i någon organisation och speciellt inte inom vården. Enligt Ruland (2002) har IT tidigare inte prioriterats inom hälso- och sjukvården, vilket har förhindrat dess utveckling. Övriga orsaker har varit att hälso- och sjukvården som organisation är komplex och besitter känslig information. Sjukvården i Sverige är indelad i 21 landsting och regioner som har ansvar för att tillhandahålla den hälso- och sjukvård som är nödvändig för dess invånare (Sveriges landsting och regioner, 2003). Den vård som erbjuds kan variera mellan de olika regioner och landstingen, men den uppdelning i primärvård, länssjukvård och regionssjukvård som finns är likartad i hela Sverige. Primärvården består av distriktsköterskemottagningar, vårdcentraler, husläkar- och familjemottagningar som många gånger utgör den första kontakten med patienter och som oftast har möjlighet att erbjuda den vård som patienten är i behov av. Inom länssjukvården i Sverige finns idag mer än 20 länssjukhus och cirka 40 länsdelssjukhus, vilka kan ses som nästa steg i vårdkedjan.

Under senare år har landsting och kommuner fått upp ögonen för vilken nytta IT kan ha inom vården och under år 2000 bildades intresseföreningen Carelink av Landstingsförbundet, Kommunförbundet, Privata vårdföretagarna samt Apoteket AB. Carelink arbetar med att skapa förutsättningar för IT inom vården på en nationell nivå och de driver idag flertalet projekt för att realisera detta.

1.2 Problemdiskussion

Stora delar av hälso- och sjukvården, speciellt sjukhusen, använder sig idag fortfarande av pappersjournaler i det dagliga arbetet, medan primärvården däremot i stor utsträckning är datoriserad (Westman, 2006). Detta har medfört både positiva och negativa konsekvenser för patienter och anställda inom hälso- och sjukvården (Datainspektionen, 2005). Den information som behandlas av och inom sjukvården idag är integritetskänslig och det kan få stora konsekvenser för en enskild person om sådan information hamnar i fel händer.

Några dagar efter att Anna Lind mördades i september 2003, misstänktes två personer ur sjukhuspersonalen för dataintrång. De hade varit inne i sjukhusets datasystem och läst hennes elektroniska journal utan behörighet (dn, 2004a). Detta sågs det allvarligt på från sjukhuset som startade en utredning gällande dataintrånget. Sommaren 2004 fälldes en kvinna till 30 dagsböter då hon erkänt att hon utan behörighet läst journalen (dn, 2004b). Detta är dock inte första gången det händer. Enligt Bjurman (2004) är det mycket vanligt att behörighet missbrukas, eftersom känslig data är så lockande att beskåda. Antalet datasystem med personuppgifter ökar och det gör även att säkerhetsproblemet ökar. Det är därmed av stor vikt att patientinformation behandlas på ett säkert och respektfullt sätt. Datainspektionen (2005) menar att en säker hantering av information inom vården kan öka patientsäkerheten. 1998 ersattes datalagen av den nuvarande personuppgiftslagen och detta gjorde att vissa tillstånd försvann (Bjurman, 2004). Innan behövdes ett tillstånd från Datainspektionen för att komma åt personuppgifter, men idag är kravet att vissa tekniska åtgärder ska genomgöras. Loggar ska exempelvis föras, så att det går att kontrollera spårbarheten, det vill säga, vem som varit inne i personuppgiftsregistret.

Inom sjukvården finns problemet att många människor har tillgång till registren över patienter. Enligt Bjurman (2004) kan detta förbättra servicen, men tyvärr ökar också missbruket. Datorer är en viktig resurs inom hälso- och sjukvården, och de bör därför vara noga med att inte skada patientens förtroende. Istället ska datorerna bidra till en mer ”aktiv patient”, det vill säga, att patienten själv skall kunna finna information på nätet, öka sin kunskap och därmed ställa högre krav på vården. (Ruland, 2002 och Datainspektionen, 2005)

Ruland (2002) menar att ett för stort ansvar läggs på sekretessavtal där uppföljning och kontroll är mycket svårt att utföra och vilket i och med datorisering av patientinformation behöver stöd i andra former av säkerhetsåtgärder. Enligt Datainspektionen (2005) skiljer sig säkerhetspolicys, tillvägagångssätt samt tillgång till patientinformation avsevärt mellan landstingen. Det är inte bara olikheter i säkerhetstänkandet som skapat skillnader i informationsåtkomst bland landstingen. Systemen som används både mellan och inom organisationer kan skilja i uppbyggnad och har då inte möjlighet att interagera med varandra, vilket i sin tur förhindrar viss åtkomst. Datainspektionen (2005) påpekar dock att vissa system är mycket fördelaktigt uppbyggda med många spärrar att passera innan åtkomst är möjlig. Det stora problemet enligt Datainspektionen (2005) är att säkerhetstänkandet inte har utvecklats i takt med tekniken och Datainspektionen (2005) anser att tekniska och administrativa verktyg för att förhindra obehörig åtkomst måste skapas och implementeras.

För att, som sagt var, möjliggöra säker tillgång av patientinformation för både vårdgivare och patient oberoende av plats utlovade vårdministern Ylva Johansson under 2004 att en Nationell strategi för IT inom vården skulle tas fram till årsskiftet 2005/2006. Den Nationella IT-strategin (se 2.1) presenterades i början på mars i år, 2006, men ännu har inga beslut tagits. Bohlin (2006) menar att det är av stor vikt att den nya strategin sätts i bruk under snar framtid då landsting annars befaras gå sin egen väg och implementera system som inte kan interageras i en gemensam infrastruktur. Författaren menar även att rapporten bör

vara så konkret som möjligt speciellt gällande vilka system som är framtidssäkra och ska användas nationellt för att landstingen ska våga satsa på dessa. Enligt Hellblom (2006) krävs ett bättre samarbeta mellan landsting samt en lagändring (vilket dock har utlovats av ministern Ylva Johansson) för att möjliggöra en Nationell IT-strategi. Det är inte bara vikten av korrekt vård som har varit en drivande faktor i skapandet av den Nationella IT-strategin utan även ekonomiska aspekter finns att beakta (Bohlin, 2006). Bohlin (2006) menar att många miljarder finns att spara i administrationskostnader inom hälso- och sjukvården, vilket kan lösas med ett nationellt journalsystem.

Organisationen Carelink (se 2.2) har tagit fram ett antal olika projekt för att hitta IT-lösningar inom hälso- och sjukvården. Ett av dessa projekt är SITHS, Säker IT i Hälso- och Sjukvård. SITHS- modellen bygger på att anställda i vård och omsorg har ett personligt elektroniskt ID-kort, ett så kallat smart kort, som sedan förses med ett särskilt ”anställningscertifikat”. Certifikaten ger också möjlighet att signera en handling digitalt, vilket motsvarar en vanlig namnteckning. Enligt Finkenzeller (2004) är smarta kort den yngsta medlemmen i familjen av elektroniska identifikationskort och karaktäriseras av vissa egenskaper som är inbäddade i kortet. Dessa egenskaper gör det möjligt att överföra, förvara och processa data med kortet. Den viktigaste fördelen är dock att data på kortet kan skyddas mot obehöriga och manipulation. Då IT-stöd är relativt nytt inom hälso- och sjukvården kan ett visst motstånd uppstå vid en stor förändring som nu är i antågande. Smarta kort är en ny teknik som enligt Carelink bör införas inom hälso- och sjukvården, men det är i samband med detta viktigt att diskutera hur spridningen av den nya informationen kommer att ske inom och mellan Landstingen.

1.2.1 Problemformulering

Vi har i vår uppsats valt att använda oss av fyra forskningsfrågor. Dessa skall tillsammans bidra till att undersöka på vilket sätt smarta kort kan vara en del av en total säkerhetslösning inom hälso- och sjukvården.

De tre första forskningsfrågorna är direkt relaterade till den Nationella IT-strategin och Carelink vilka vill skapa en total säkerhetslösning för hälso- och sjukvården med smarta kort som en del i detta. Den fjärde frågan är kopplad till hur användarna ser på detta och hur det egentliga behovet ser ut och om smarta kort därmed är en lämplig lösning att implementera inom hälso- och sjukvården.

Den Nationella IT-strategin vill skapa en ny säkerhetslösning för hälso- och sjukvården i Sverige och Carelink vill använda smarta kort som en del av denna totala säkerhetslösning. Vi undrar därmed följande:

- Hur kan smarta kort förbättra IT-säkerheten inom hälso- och sjukvården i enlighet med den Nationella IT-strategin och Carelink?

Den Nationella IT-strategin lyfter fram mobilitet inom vård- och omsorg som en viktig aspekt. En anledning till detta är att dagens patienter blir mer och mer mobila. Vi vill därmed med följande fråga undersöka hur smarta kort kan bidra till detta.

- Hur kan smarta kort öka mobiliteten bland vårdgivare och patienter?

Vi har förstått att det är av stor vikt för vårdgivare att ha tillgång till en patients information för att kunna ge bästa möjliga vård. Då patienter blir mer mobila undrar vi i enlighet med den Nationella IT-strategin om det finns ett behov och en möjlighet rent säkerhetsmässigt för åtkomst av information över landstingsgränserna.

- Hur ser behovet samt säkerheten ut kring elektroniska journaler i förhållande till pappersjournaler?

Som ett uppdrag av Länssjukhuset Ryhov vill vi även undersöka hur attityderna ser ut idag gällande förändringar i organisationen, datoranvändningen samt säkerheten kring den för att på så sätt utreda om smarta kort kan implementeras som en del av en total säkerhetslösning. Därav följande fråga:

- Hur ser attityderna ut till förändringar, datoranvändning, samt säkerhetsaspekterna som idag finns inom hälso- och sjukvården bland vårdgivarna?

1.3 Syfte

Syftet med denna uppsats är att undersöka förutsättningarna för hur smarta kort, som en del av en total säkerhetslösning, kan förbättra IT-säkerheten inom hälso- och sjukvården.

1.4 Avgränsningar

Vi har valt att avgränsa uppsatsen till att diskutera smarta kort som en möjlig IT-lösning inom hälso- och sjukvården samt titta på de attityder som användarna har gällande datoranvändningen idag. Vi kommer dock inte att gå in på några ingående tekniska detaljer kring smarta kort eller datasystem, utan endast redovisa några av de alternativ som finns på marknaden idag. Vi kommer likaså inte att analysera ur en affärsstrategisk synvinkel med parallell infrastruktur, då vi anser att detta är en annan typ av studie.

Vi kommer heller inte att gå djupare in på de kostnader som kan komma att uppstå vid ett möjligt införande, då detta är beroende på val av kort, önskade funktioner, leverantörer, etc.

1.5 Intressenter

De främsta intressenterna för vår uppsats är förmodligen IT-Planering och IT-Centrum (ITC) på Länssjukhuset Ryhov här i Jönköping, eftersom det är de som ansvarar för att IT-säkerheten ska bli så bra som möjligt. Andra intressenter kan vara de olika medlemmarna på Carelink, då uppsatsen kan ge en ökad förståelse för vad användarna ute på sjukhuset vill ha för framtida förbättringar gällande datoranvändningen. Vår uppsats kan användas som underlag för fortsatta IT-satsningar.

Uppsatsen kan även vara intressant för informatikstudenter som funderar på att arbeta med IT-säkerhet i olika organisationer och vill ta del av användarnas erfarenheter. Vården hanterar dagligen känslig information och om informatikstudenter eller andra personer med intresse för området får en djupare insikt inom ämnet har de ha lättare att förstå framtida situationer.

Vi tror även att olika företag som levererar IT-lösningar kan vara intresserade av denna uppsats, då vi klarlägger hur viktigt det är att skydda känslig information inom hälso- och sjukvården. Uppsatsen kan då ses som ett hjälpmedel att förstå medicinsk informatik, samt användarnas behov av en fungerande IT-lösning som skyddar från obehörigt intrång och underlättar samarbetet mellan klinikerna vid informationsutbyte.

1.6 Definitioner

- **Smarta kort:** Vi har valt att använda begreppet smarta kort då vi diskuterar smart card eller aktiva kort.
- **IT:** Informationsteknik (eng. Information Technology) Ett samlingsbegrepp för de tekniker som används vid Informationssystem såsom hårdvara, mjukvara och kommunikation (Beekman och Rathswhol, 2003).
- **PKI**: Den infrastruktur som gör det möjligt att med hjälp av kryptering med publika nycklar öka informationssäkerheten, då informationsutbyte ska ske mellan användare (Carelink, 2006c).
- **Hårda certifikat:** Grundas på metoder för signaturframställning där den privata nyckeln är placerad i ett chip på till exempelvis ett kort. Genereras oftast med en engångskod (Bishop, 2004).
- **Mjuka certifikat:** Här är den privata nyckeln oftast placerad på en dators hårddisk och kan kombineras med en pinkod (Bishop, 2004).
- **Branschcertifikat**: Certifierade egenskaper som är branschspecifika eller kopplade till arbetsplatsen samtidigt som de är knutna till en fysisk person (Carelink, 2006c).
- **Primärcertifikat**: Personligt certifikat och används som identifiering (Carelink, 2006c).
- **Sekundärcertifikat**: Döljer uppgifterna i primärcertifikaten och kan spärras utan att primärcertifikatet spärras. Branschcertifikatet är ett sekundärcertifikat (Carelink, 2006c).

1.7 Disposition

- **Kapitel 1: Inledning**

I det här kapitlet kommer vi att redogöra för bakgrunden till informationssäkerhet samt IT-säkerhets problem inom vården. Vi kommer även att diskutera den Nationella IT-strategin, intresseorganisationen Carelink samt smarta kort, då dessa ligger till grund för vårt syfte. Forskningsfrågor samt syfte presenteras och vidare förklaras begrepp, våra avgränsningar samt vilka som kan vara intresserade av uppsatsen. I slutet på inledningen förklaras även dispositionen av uppsatsen.

- **Kapitel 2: Skapande av förståelse**

I denna del kommer vi att fördjupa oss i den Nationella IT-strategin samt intresseorganisationen Carelink. Vi valde att i samband med vår studie utföra en förundersökning omfattande Carelink och deras projekt samt den nyligen utkomna IT-strategin för vård- och omsorg. Detta för att skapa oss en grund samt uppfattning om det ämne vi valt att studera och detta ledde oss fram till forskningsfrågorna samt syftet för studien. Vi har därför valt att lägga detta kapitel före metoden och referensramen. Den Nationella IT-strategin samt Carelink har fungerat som en utgångspunkt till hälso- och sjukvården som en organisation, som vi tidigare inte varit insatta i mer än från ett patientperspektiv.

- **Kapitel 3: Metod**

I metoddelen kommer vi att diskutera vårt val av metod med utgångspunkt från syftet och forskningsfrågorna. Vi kommer även att redogöra vårt planerade tillvägagångssätt för datainsamlingen på Länssjukhuset Ryhov samt göra en värdering av studien.

- **Kapitel 4: Referensram**

I referensramen kommer vi att redovisa de kunskaper och teorier som vi har införskaffat oss genom den genomförda litteraturstudien. Teorierna syftar till att ge en bättre förståelse kring ämnet informationssäkerhet och vården samt bakgrund till vad smarta kort är för något.

- **Kapitel 5: Fallstudie på Länssjukhuset Ryhov**

I det här kapitlet kommer vårt studieobjekt att beskrivas närmare och vi kommer även att redovisa de resultat vi fått genom de intervjuer och den enkät som genomfördes på Länssjukhuset Ryhov. Vi har valt att dela in intervjuobjekten efter erfarenheter och uppgifter inom organisationen för att skapa en bättre helhetsbild.

- **Kapitel 6: Analys**

I den här delen har vi använt oss av de referenser som vi byggt upp uppsatsen kring samt de intervjuer och den enkät som redovisats i den empiriska delen av uppsatsen. Intervjuerna har försett oss med information om hur IT-säkerheten fungerar på Länssjukhuset Ryhov idag, medan enkäten har gett oss mer information om vad användarna anser om den nuvarande datoranvändningen och IT-säkerheten. I analys delen kommer den insamlande datan att kopplas ihop med teorier och information från kapitel 2 och 4.

- **Kapitel 7: Slutsatser**

I detta avsnitt kommer vi att redovisa slutsatserna för uppsatsen. Dessa har vi skapat från analysen av teorier och den data som samlats in.

- **Kapitel 8: Avslutande diskussion**

I det här kapitlet reflekterar vi över uppsatsen samt de erfarenheter vi fått. Vi ger även förslag på fortsatta studier inom ämnet.

2 Skapande av förståelse

Vi valde i samband med vår studie att utföra en förundersökning omfattande intresseorganisationen Carelink och den nyligen utkomna Nationella IT-strategin för vård- och omsorg. Detta för att skapa oss en grund samt uppfattning om det ämne vi valt att studera. Förundersökningen ledde oss även fram till forskningsfrågorna samt syftet med studien. Den Nationella IT-strategin samt Carelink hjälper oss att förstå hur hälso- och sjukvården fungerar eller rättare sagt strävar efter att fungera.

2.1 Nationell IT-strategi för vård och omsorg

Under 2004 utlovade vårdministern att en Nationell IT-strategi för vård och omsorg skulle tas fram till år 2006. Anledningen var att möjliggöra en säker tillgång av patientinformation för både vårdgivare och patienter oberoende av var de befinner sig i landet. Den Nationella IT-strategin för hälso- och sjukvården presenterades således i början av mars detta år (2006) (Regeringen, 2006).

Genom den Nationella IT-strategin för vård och omsorg har sex insatsområden identifierats inom hälso- och sjukvården som ska se till att vården blir säker, tillgänglig och effektiv med hjälp av IT (Regeringskansliet, 2005). De sex områdena är följande:

- 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

De tre första punkterna har utarbetats för att skapa bättre grundförutsättningar för IT inom hälso- och sjukvården medan de tre efterföljande är till för att förbättra Medicinsk Informatik, MI, det vill säga, de IT-stöd som används i vårdarbetet samt att anpassa dem till patienternas behov.

2.1.1 Harmonisera lagar och regelverk med en ökad IT-användning

Vid användning av IT-stöd inom hälso- och sjukvården måste de självklart följa de lagar och bestämmelser som finns (Regeringen, 2006). Ett av problemen med IT-stöd inom vården har dock varit att de lagar och bestämmelser som finns inte varit fullt anpassade till hälso- och sjukvården. Det vill säga att lagar och regler inte utvecklats i takt med den datoriserade miljö som skapats och kan därför inte stödja alla verksamhetens behov. Det pågår därmed enligt Regeringen (2006) för tillfället en översyn av de lagar och bestämmelser som reglerar informationshanteringen inom hälso- och sjukvården. En av de viktigaste frågorna inom hälso- och sjukvården har varit och är hur patientinformation skall skyddas från obehörigas insyn. Det finns lagar och bestämmelser, så som sekretess, vilka reglerar detta, men vid införandet av IT-stöd har hälso- och sjukvården behövt se över sina rutiner gällande detta. Den Nationella IT-strategin menar dock att IT-stöd ger en bättre möjlighet att säkerställa patienters integritet, då de kan förebygga och spåra intrång (Regeringen, 2006).

2.1.2 Skapa en gemensam informationsstruktur

Inom hälso- och sjukvården är det många gånger viktigt för vårdgivarna att ha tillgång till information om patienten för att bedriva säker och bra vård (Regeringen, 2006). Enligt den Nationella IT-strategin (2006) kräver patientsäkerheten att information om patienten följer denne och är tillgänglig för alla behöriga vårdgivare. Det är även av stor vikt att informationen kan förstås av samtliga vårdgivare och bör då vara så entydig att den bara kan förstås på ett sätt. För att patientsäkerheten på sikt skall möjliggöras och för att informationen ska vara en långsiktig resurs måste den enligt den Nationella IT-strategin lagras elektroniskt, vara sökbar samt ha en enhetlig struktur. Strukturen gäller enligt Regeringen (2006) både skapandet av en enhetlig infrastruktur samt ett gemensamt regelverk/struktur för hur informationen skall bli enhetlig. Detta är under utveckling, då regeringen gett i uppdrag till socialstyrelsen att förbereda införandet av en enhetlig informationsstruktur inom hälso- och sjukvården (Regeringen, 2006).

Prioriterade frågor inom detta område enligt den Nationella IT-strategin är följande (Regeringen, 2006):

- Ansluta många mindre vårdgivare till kommunikationsnätet Sjunet.
- Anpassning av lokala elektroniska kataloger till den nationella HSA-katalogen, Hälso- och Sjukvårds Adressregister.
- Utveckla och införa säkerhetslösningar baserade på nationella elektroniska id-kort.

2.1.3 Skapa en gemensam teknisk infrastruktur

De olika verksamheterna inom hälso- och sjukvården ansvarar själva för den egna tekniska infrastrukturen (Regeringen, 2006). Det har dock framkommit att kommunikation mellan de olika verksamheterna, nationellt sätt, är av stor vikt. För tillfället är det få system som kommunicerar med varandra över gränserna och den Nationella IT-strategin framhåller behovet av att utveckla en nationell teknisk infrastruktur som en hög säkerhet och kvalitet vid överföring av data. Vid skapandet av ett gemensamt kommunikationsnät, som nämnts ovan, är det viktigt enligt Regeringen (2006) att hälso- och sjukvården kan garantera att patienters integritet inte kränks. Under utveckling är kommunikationsnätet Sjunet, vilket idag dock inte uppfyller de krav som bland annat möjliggör anslutning av ett stort antal små vårdgivare till nätverket. HSA-katalogen är ytterligare ett projekt som drivs av Carelink där vårdgivare genom en nationell elektronisk verksamhetskatalog kan dela information med varandra. Carelink har även under några år arbetat med projektet SITHS, vilket är meningen att bli en nationell säkerhetslösning med fokus på elektroniska id-kort.

2.1.4 Skapa förutsättningar för samverkande och verksamhetsstödjande IT-system.

Då det har legat ett ansvar på landstingen, kommunerna och de privata vårdgivarna själva att utveckla och implementera sina egna IT-stöd har variationen av system blivit stor både inom och mellan verksamheterna (Regeringen, 2006). Systemen har olika arkitektur, användningsområden och leverantörer, vilket kan försvåra en interaktion mellan dem som det idag strävas efter. Det är enligt Regeringen (2006) inte bara kommunikationen som blir lidande utan även personalen, patienter och antagligen även budgeten i slutändan. För personalen resulterar det stora antalet system i extra arbete genom att de blir tvungna att hantera flertalet gränssnitt, funktionaliteten och inloggningsprocesser. Detta påverkar i sin tur

att omvårdnaden av patienten påverkas negativt. Därmed är målet att utveckla system som kan interagera med varandra både lokalt och nationellt samt att skapa IT-stöd som underlättar personalens arbete. En satsning på att ta fram nationellt gemensamma lösningar, gemensamma kravspecifikationer etc. är således en viktig del i det framtida arbetet (Regeringen, 2006).

2.1.5 Möjliggöra åtkomst till information över organisationsgränser

Enligt den Nationella IT-strategin har behovet av att få tillgång till tidigare lagrad information om patienter ökat. Information som kan vara lagrad hos flertalet olika vårdgivare. Anledningen till detta är att förbättra vårdkvaliteten för patienten samt att kunna öka kunskapen om vårdens samlade resultat (Regeringen, 2006). De uppgifter som det finns ett behov av att få tillgång till på nationell nivå är patientjournaler, uppgifter om läkemedelsanvändning på grund av risk för motmedicinering eller felmedicinering, laboratorieprover samt radiologisk information. Idag används elektroniska journaler (e-journaler) på i stort sätt samtliga delar inom primärvården samt på ca 50 % av sjukhusen, vilket dock beräknas öka kraftigt under de kommande åren. Även inom detta område driver Carelink ett projekt kallat nationell patientöversikt där de e-journalerna och övrig vårddokumentation skall kunna nås nationellt (regeringen, 2006).

2.1.6 Göra information och tjänster lättillgängliga för medborgarna

Enligt Regeringen, (2006) skall medborgare ha möjligheten att enkelt och säkert få tillgång till vården oavsett när och var behovet uppstår. De skall även kunna få tillgång till hälsorelaterad information samt kunna kommunicera med sin vårdgivare på olika sätt. Enligt den Nationella IT-strategin finns det idag mycket elektronisk information att tillgå, men kanske inte på det heltäckande och lättillgängliga sätt som önskas. Därav har Regeringen (2006) sätt behovet av att skapa en gemensam portal till samlad kvalitetssäkrad vårdinformation för medborgarna. Att utveckla vårdinformation samt vårdkommunikation kan även främja glesbygden samt äldre människor. Det är även tänkt att olika bokningstjänster skall kunna utföras elektroniskt i större utsträckning än idag. Vidare bestämdes det 1 juli, 2005 att läkemedelsförteckningar skall upprättas av apoteket samt att det ska vara möjligt för apotekskunder att hämta ut sina recept, vilka så är elektroniskt lagrade, vid flera uthämtningstillfällen. Sammanfattningsvis är det meningen att hälso- och sjukvården skall underlätta vårdrelationen samt skapa möjligheter för bättre och säkrare informationstillgång för medborgarna (Regeringen, 2006).

Målen med samtliga av dessa områden och de krav som ska uppfyllas för vården är att den vård som ges ska vara av god kvalitet och lättillgänglig. Den ska dessutom se till patienternas integritet och självbestämmande samt säkerställa en effektivare resursbehandling och öka tillgängligheten av information för alla parter (regeringen, 2006). Westman (2006) menar att tillgången till adekvat information om en patient kan vara livsavgörande. Det är dock inte bara information om patienter som är viktig utan även tillgången för vårdpersonalen till den senaste kunskapen inom det aktuella kliniska området (Ruland, 2002). För att säkerställa vårdkvaliteten bör vårdgivare snabbt kunna uppdatera sina kunskaper på ett säkert sätt. Detta kan realiseras genom att främja användandet av MI, vilket dock kräver utbildning och kunskap i hur IT kan användas inom vården.

2.2 Carelink

Organisationen Carelink driver sin verksamhet genom en intresseförening samt aktiebolaget Carelink. Intresseföreningen består av Landstingsförbundet, Svenska Kommunalförbundet, Vårdföretagarna samt Apoteket och alla landsting, kommuner och enskilda vårdföretag inbjuds att vara medlemmar (Carelink, 2006a).

Carelink har som uppgift att se förmågan med IT värdet ur ett nationellt och övergripande perspektiv och det är därför viktigt att organisationen har ett nära samarbete med sina medlemmar och andra intressenter. Detta för att de ska kunna åstadkomma en utbyggd tekniks infrastruktur med en enhetlig informationsstruktur och få igenom vissa ändringar i lagstiftningen. Organisationen kan delas upp i Utveckling, Förvaltning och Information & Kommunikation (Carelink, 2006b).

- Utvecklingsarbetet sker framför allt i ett antal projekt som har tagits fram gemensamt av medlemmarna. Vissa utvecklingsprojekt bedrivs i form av förstudier och uppdrag.
- Förvaltningen är den del av verksamheten där utvecklingsarbetena har kommit i den fas där de ska övergå till någon form av kontinuerlig förvaltning.
- Information och Kommunikation är den del av verksamheten där erfarenhetsutbyte, kunskapsökning och samverkan sker kontinuerligt. Här skapar Carelink nätverk, mötesplatser och är informationsspridare i olika sammanhang.

2.2.1 HSA

HSA står för Hälso- och Sjukvårds Adressregister och är en nationell katalogtjänst för svensk vård och omsorg (Carelink, 2006d). HSA är ett verktyg för att kommunicera elektroniskt och är en katalogtjänst för att hantera olika slags information och har som huvudsyfte att alltid ha tillträde till aktuell information oavsett var patienten eller vårdgivaren befinner sig. Här går det att hitta olika personer, befattningar samt olika system. Många kommuner och landsting har idag egna kataloger, men det går inte att nå information nationellt med dessa. Därför menar Carelink (2006d) att HSA katalogen är en viktig bastjänst i den nationella IT-infrastrukturen.

2.2.2 SITHS

Ett av projekten som Carelink driver är SITHS, Säker IT i Hälso- och sjukvård. Det är ett projekt som från början startades av SPRI, men då denna organisation lades ner, tog Carelink över (Carelink, 2006c). SITHS har arbetats fram tillsammans med olika landsting för att säkerhetskälla informationshanteringen i vårdkedjan. Tankarna på att använda en nationell PKI (Public Key Infrastructure) föddes i slutet på 90-talet och startade i landstingen Östergötland, Skåne och Stockholm. Carelink anser att kraven på säkerheten inom vården är så hög att en PKI måste förvaras på ett smart kort, då endast mjuka certifikat inte är tillräcklig (Carelink, 2006c).

- Några exempel på vad en PKI kan möjliggöra är:
- Säker e-post med identifikation av avsändare.
- Säker E-handel med digitalt signerade dokument

- Singel Sign On
- Digitalt signerade recept, journalhandlingar mm
- Säkra överföringar av medicinsk information

Enligt Björner (2001) arbetar Carelink för att vårdgivarna och informationen ska bli lika mobila som dagens patienter är. Det är särskilt viktigt att ha en öppen PKI i större regioner, då det är ansenlig rörlighet bland personalen och antalet dubbelanställningar är stort. Organisationen anser att en säker informationshantering i vårdkedjan är en nödvändighet och att vården därför kräver en öppen och branschspecifik PKI-lösning. Detta innebär att lösningen måste;

- Bygga på standarder (certifikat, kort)
- Fungera på alla typer av huvudmän
- Fungera på nationell nivå
- Baseras på smarta kort (mobilitet)
- Medge branschcertifikat

Carelink anser att ett vanligt tjänstekort med ett tjänstecertifikat inte är tillräckligt för att lösa de säkerhetskrav som ställs inom hälso- och sjukvården. Tidigare erfarenheter visar att det slarvas mer med vanliga tjänstekort, medan personliga kort med flera tjänster inprogrammerade bevarades med större aktsamhet. Carelink anser heller inte att det går lika bra att ha uppgifter lagrade i olika kataloger, då tillförlitligheten och kvalitén inte blir detsamma. Med smarta kort kan uppgifternas trovärdighet i ett certifikat garanteras lättare av utgivaren, då certifikatet signeras digitalt, och detta är viktigt vid ett signerat dokument såsom journalanteckningar, e-recept samt dokumentation av patientsamtycken (Björner, 2001).

2.2.3 Mobilitet

Sjukvården är en plats där det ständigt är mycket rörelse, personal förflyttar sig mellan patienter och kliniker, och de behöver vara mer mobila. Mobilitet är ett samlingsnamn som sträcker sig över många områden, däribland bärbara datorer, handenheter och remoteaccess lösningar (eEurope, 2005). En mobilitetslösning kan effektivisera en organisation och speciellt då inom sjukvården. För läkare, som ständigt behöver förflyttar sig, kan med hjälp av mobilitet effektivisera läkarens eller sjuksköterskans arbete (Björner, 2001). Dock krävs det en ny infrastruktur som gör att korten kan användas på de områden som önskas och det är viktigt att myndigheter samt leverantörer kan arbeta tillsammans. Detta för att gemensamma specifikationer ska kunna formas för till exempelvis säkerhet, användarroll och privatliv.

3 Metod

I metoddelen kommer vi att diskutera vårt val av metod med utgångspunkt från syfte samt forskningsfrågor. Vi kommer även att redogöra för vårt planerade tillvägagångssätt för datainsamlingen på Länssjukhuset Ryhov samt göra en värdering av studien.

3.1 Inledande diskussion om metodval

Beroende på forskningsfrågor finns det, enligt Järvinen (1999), olika vägar att gå för att kunna svara på dessa. Bland annat diskuterar författaren att forskningen kan genomföras genom att testa teorier samt skapa teorier och dessa sker då med hjälp av kvantitativa och kvalitativa studier (se 3.3.3). Enligt Hansagi och Allebeck (1994) styrs valet av forskningsmetod också av problemets natur och syftet med analysen. Då vårt syfte med uppsatsen är att studera hur smarta kort kan vara en del av en IT-lösning inom hälso- och sjukvården, anser vi att vi måste få en djupare förståelse i landstinget som organisation och hur känslig information hanteras där idag. Genom att använda oss av intervjuer samt en enkät, vilket kommer att diskuteras i avsnitt 3.3, anser vi oss få en bättre och djupare förståelse för hälso- och sjukvården.

Smarta kort som är i fokus i denna studie kommer också att studeras samt attityder och förändringsarbete. Vidare måste vi även studera lagar gällande sekretess, personuppgiftshantering med fokus på IT som media ur ett sjukvårdsperspektiv, etc. Detta kommer att ske genom en litteraturstudie samt en empirisk studie på Länssjukhuset Ryhov. Vi har valt att studera Länssjukhuset Ryhov i Jönköpings län, då det finns i vår närhet samt att detta sjukhus har funderingar på att använda smarta kort i sin organisation.

3.2 Val av forskningsmetod

Enligt Hansagi och Allebeck finns det två sätt att samla in information om olika händelser;

- Genom egna iakttagelser
- Genom att fråga någon som kan ge upplysningar antingen muntligt eller skriftligt.

Dessa två sätt att samla in information på kan också beskrivas som insamling av primärdata och sekundärdata. Enligt Wiedersheim-Paul och Eriksson (1991) är primärdata något som forskare/författare samlar in själva för att uppnå sitt syfte med undersökningen eller uppsatsen. Primärdata kan samlas in med hjälp av intervjuer, enkäter eller fältstudier. Enligt Lundahl och Skärvad (1991) är sekundärdata däremot redan insamlad data i form av tidigare undersökningar eller skrivna teorier så som böcker, rapporter och vetenskapliga journaler.

3.2.1 Litteraturstudie

Litteraturstudier är, enligt Lundahl och Skärvad (1991), väsentliga för att få en så bra grund som möjligt inom det ämne som studeras. Detta är något som Hansagi och Allebeck (1994) också håller med om, då en viktig del i planeringsfasen är att sätta sig in i området som ska studeras vilket kan göras genom att studera litteratur samt var den aktuella forskningsfronten befinner sig. Då vårt syfte avser att undersöka möjligheten att använda smarta kort inom hälso- och sjukvården, anser vi oss behöva fördjupa oss i de olika delarna med hjälp av flertalet teorier. Genom att göra detta hoppas vi få en bättre förståelse om möjligheten

finns att implementera smarta kort som en del av en IT-lösning inom hälso- och sjukvården.

Vi kommer använda sekundärdata till hjälp för vår analys, men också som underlag för empiriforskningen. Litteraturstudien kommer här användas för att konstruera relevanta frågor till intervjuerna samt den enkät som ska ges ut till användarna, då vi anser att det inte räcker med att bara utföra en litteraturstudie för att uppnå syftet.

3.2.2 Källkritik

Enligt Holme och Solvang (1997) kan källor definieras på olika sätt. En källa kan vara muntligt eller ”skriftligt nedtecknat material” (Holme och Solvang, 1997, s.125) och anses bli en källa först då vi använder det. I vårt arbete har alla källor granskats enligt de fyra faser som författarna beskiver;

- Observation: Efter att ha tittat på vår problemställning och vårt syfte, har vi kommit fram till vi måste använda både primär- och sekundärkällor. Vår princip är att i första hand använda oss av primärkällor, men vi behöver ändå titta på olika teorier för att få en djupare förståelse för det område vi studerar.

- Ursprung: Här måste vi avgöra om källan är vad den utger sig att vara. Då vi träffat våra primärkällor vid olika intervjutillfällen, anser vi att den information vi fått från dessa är äkta. I vår litteraturstudie har vi tittat på vem som står bakom källan och om informationen kommer från böcker, tidskrifter och vetenskapliga rapporter. Vi har använt oss av Internet, men då endast av hemsidor som vi anser oss har förtroende för såsom Regeringen, Carelink, etc.

- Tolkning: Vi har här tittat på om innehållet från källan är det vi har för avsikt att skriva om.

- Användbarhet: Tillsist här vi tittat på om källan verkligen är användbar för vårt syfte och kan belysa de centrala faktorerna som vi vill ha svar på.

För att på ett bra sätt kunna säkerhetsställa uppsatsens pålitlighet och giltighet har vi för avsikt att använda oss av uppdaterat material. Detta för att det kommer ha en avgörande inverkan på vilka slutsatser vi kommer dra.

3.2.3 Kvalitativa och kvantitativa metoder

Enligt Holme & Solvang (1997) kännetecknas kvalitativa metoder genom att ha en närhet till den källa vi hämtar vår information ifrån. Detta innebär att en eller flera miljöer studeras mer ingående i sin helhet (Repstad, 1999). Vi anser därför att vi bör göra flera intervjuer, men respondenterna ska komma från olika delar av organisationen. Med en kvalitativ intervju söker en forskare en djupare förståelse inom ämnet från respondenten. Vi väljer därför att göra intervjuer på Länssjukhuset Ryhov för att få en bättre förståelse för organisationer och dess ingående delar. Vi vill också få en djupare förståelse för de känslor och tankar som de olika respondenterna har för samma fenomen.

Enligt Holme och Solvang (1997) finns det inga centrala syften som statistisk generalisering eller representativitet i kvalitativa studier, men urvalet har ändå en stor betydelse för undersökningen. Fel personer kan leda till att hela undersökningen blir fel. Tillsammans med vår kontaktperson har personerna valts ut efter erfarenheter och arbetsområden. Syftet med

kvalitativa intervjuer är också att skapa grund för informationsflödet och öka informationsflödet för det fenomen vi studerar. Det är enligt Holme och Solvang (1997) viktigt att vi som undersökare försöker komma respondenterna så nära inpå livet som möjligt, så att vi förstår den situation som individen, grupperna eller hela organisationen upplever.

Då kvalitativa studier är tidskrävande, valde vi att också göra en kvantitativ studie i form av en enkät på användarna gällande datoranvändningen på Länssjukhuset Ryhov. Enligt Lundahl och Skärvad (1991) är kvantitativa studier ett sätt att mäta och sedan förklara ett visst fenomen. Vi hoppas genom att göra detta få med så många som möjligt i undersökningen och skapa någon slags generalisering för Länssjukhuset Ryhov. Enligt Lundahl och Skärvad (1991) görs en enkätundersökning för att nå ut till en större grupp på kortare tid och vi kan få reda på mer om de attityder som finns bland användarna än vad vi skulle ha fått med intervjuer.

Enligt Hansagi och Allebeck (1994) är det viktigt att noggrann planering och systematik sker då data ska samlas in via intervju eller enkät. De metoder som används måste också dokumenteras på ett sätt att utomstående undersökare ska kunna bedöma värdet av den insamlande data. Med utgångspunkt till de delar som syftet har, anser vi att ett bra tillvägagångssätt är att kombinera kvalitativa och kvantitativa metoder för att få en så bra helhets bild som möjligt. Andersen (1998) beskriver den kvalitativa metoden som den förstående inriktningen där djupare förståelse av problemområdet vill skapas, medan den kvantitativa metoden syftar till att bevisa ett visst fenomen och nå generalisering i form av att analysera resultatet. Vi anser att en kombination av dessa två metoder kan resultera i en djupare och bredare förståelse inom det område vi valt att studera.

3.3 Datainsamling i form av intervju och enkät

Då empirisk forskning genomförs används oftast termerna mätningar eller observationer, och menas då insamling av data eller uppgifter. Enligt Hansagi och Allebeck (1994) skiljs det på direkta och indirekta observationer.

- Direkta: Räknar, väger eller mäter objekt som är omedelbart tillgängliga för observation.
- Indirekta: Data som samlas in genom att intervjua eller ställa frågor via enkäter till individen om deras upplevelser, beteende, känslor och attityder.

Som tidigare nämnt har vi valt att använda oss av både intervjuer och enkät för att på så sätt uppfylla syftet med uppsatsen.

3.3.1 Val av respondenter

Länssjukhuset Ryhov har, som tidigare nämnts, valts som studieobjekt till vår studie, då de finns i vår närhet samt har funderingar på att använda sig av smarta kort i verksamheten.

Tillsammans med vår kontaktperson på Länssjukhuset Ryhov valdes ett bestämt antal personer ut till de intervjuer som skulle genomföras på sjukhuset. Då smarta kort tillsammans med IT-säkerhet är huvudämnet i uppsatsen, valdes personer inom IT-området ut och resultatet blev två personer på IT-Centrum (ITC), två personer på IT-Planering samt 5 personer från fem olika kliniker på sjukhuset Ryhov. De fem sista nämnda personerna fungerar som IT-kontaktpersoner på klinikerna gentemot ITC och IT-Planering.

De fem IT-kontaktpersonerna var också de som hjälpte oss att dela ut enkäten. De fick själva välja ut de 10 personer som skulle svara på enkäten på deras klinik och resultatet blev att de valde både läkare, sjuksköterskor samt undersköterskor enligt våra rekommendationer. Enkäterna lades i enskilda kuvert, så att vi kunde garantera anonymitet och respondenterna behövde inte känna att IT-kontaktpersonen kunde läsa svaren.

3.3.2 Val av intervjumetod

Enligt Repstad (1999) är det bra att göra ett visst inledande förarbete då en miljö ska beskrivas. Genom att göra detta kan vi få en förståelse över vilka som bör intervjuas för att uppfylla vårt syfte. Vi gjorde en förstudie genom att boka ett möte med vår kontaktperson, där vi gick igenom de olika IT-områdena på Ryhov. Vår kontaktperson hjälpte oss också med att få kontakt med dessa personer, så att rätt personer kunde hjälpa oss att uppfylla vårt syfte.

Enligt Holme och Solvang (1997) finns det olika sätt att strukturera upp en intervju;

- Strukturerad: Intervjuaren har i förväg klart fastställt intervjun målsättning. Såväl de frågor som formuleras i förväg som uppföljningsfrågor har utformas för att stödja en systematisk genomgång av de områden som intervjuaren är intresserad av. Intervjun är fokuserad och informationsinriktad.

- Semistrukturerad: Ämnesområdena kan vara bestämda och frågorna formuleras efterhand och tas upp när undersökanden anser det lämpligt med tanke på exempelvis respondenternas svar eller reaktion på tidigare ställda frågor.

- Ostrukturerad: Strukturen av ett samtal där frågor uppkommer efterhand.

Vi valde att arbeta efter den semistrukturerade metoden, eftersom vi ville ha intervjuer med färdiga frågor, men med öppna diskussioner. Syftet och forskningsfrågorna ligger till grund för de olika intervjufrågor som tagits fram och de har skapats från vår förstudie samt den litteraturstudie som gjorts. Vi anser att det var viktigt att ämnesområdena var desamma på alla intervjuer, men att respondenterna, beroende på sin bakgrund och kunskap, svarade utifrån deras egna arbetserfarenheter. Enligt Holme och Solvang (1997) kan respondenterna vara mer öppna med sina tankar genom intervjuer och detta är något som vi anser vara viktigt då vi vill ha åsikter om hur datoranvändningen är idag, vilken kunskap de hade om den Nationella IT-strategin, projektet SITHS samt vilken slags förbättring de ville ha i framtiden.

3.3.3 Utformning av intervju- samt enkätfrågor

Vid utformning av frågor och ämnesområden, som legat till grund för enkäten samt de nio intervjuerna, har vi utgått från våra forskningsfrågor. De fyra forskningsfrågorna behandlar olika ämnesområden för att tillsammans uppfylla det syfte vi har med denna studie. När det gäller intervjuerna har vi, som tidigare nämnts, valt en semistrukturerad form vilket innebär att vi har utgått från ett antal färdiga frågor inom olika ämnesområden (se bilaga 1 och 2) och sedan haft en öppen diskussion med följdfrågor. Vidare har vi skapat två olika intervjuunderlag, vilka är baserade på respondenternas arbetsuppgifter (placering inom landstinget) och förmodad kunskap inom valt område. Som utgångspunkt för diskussionen nedan vill vi nämna att frågorna skapade för enkäten, är de frågor som kan ses i bilaga 3 och det har således inte ställts några följdfrågor och samtliga respondenter har därmed svarat på samma frågor.

Den första forskningsfrågan behandlar informationssäkerhet inom hälso- och sjukvården, då den syftar till att undersöka hur smarta kort, som enligt den Nationella IT-strategin ska vara en del av en total säkerhetslösning, kan bidra till en förbättrad IT-säkerhet. Utifrån denna undran har vi skapat frågor relaterade till informationssäkerhet så som sekretess, spårbarhet, behörighet och till viss del även tillgänglighet. Vi har även utifrån denna fråga behandlat datoranvändningen idag samt vilka önskemål och förväntningar respondenterna har på framtida säkerhet och datoranvändning. Det har även uppkommit utifrån denna forskningsfråga diskussioner kring den Nationella IT-strategin med samtliga intervjuade respondenter. Smarta kort och projektet SITHS är även de ämnen och frågor som är relaterade till denna forskningsfråga. Det som bör nämnas är att IT-Planering och ITC har fått frågor angående smarta kort, SITHS samt om mer ingående detaljer kring hur smarta kort skulle/kan/kommer att användas inom landstinget, medan vi ej har berört dessa ämnen för IT-kontaktpersonerna. Orsaken till detta är respondenternas kunskapsnivå och arbetsuppgifter, samt att det var av intresse för oss att inte påverka användarnas önskemål, behov och problem.

Forskningsfråga två tar upp ämnet mobilitet vilken är en viktig aspekt för vården idag såväl som för framtiden. Den Nationella IT-strategin samt Carelink menar att mobiliteten kommer att öka inom hälso- och sjukvården, och detta måste skapas en förberedelse inför för att kunna ge så bra vård som möjligt. Vi reflekterade därmed över hur smarta kort kan öka mobiliteten bland både vårdgivare och patienter, och tog därför utifrån denna forskningsfråga fram intervju- och enkätfrågor kring hur respondenterna ser på mobilitet inom hälso- och sjukvården idag, men även inför framtiden.

Tredje forskningsfrågan behandlar e-journalers nytta, samt säkerhetsaspekter kring dessa. Denna frågeställning har, som nämnts tidigare, vuxit fram från den Nationella IT-strategin, ökad mobilitet samt vikten av att ha tillgång till information för att kunna ge patienter bra och rätt vård och behandling. Forskningsfrågan har lett till intervju- och enkätfrågor, vilka behandlar synen på lagring av information elektroniskt och mer specifikt e-journaler, samt säkerhetsaspekter kring dessa.

Vi har utgått från forskningsfråga nummer fyra när vi skapat frågor kring attityder till datoranvändning, säkerhet samt förändringsarbete. Detta med anledning av att vi är intresserade av att se vilken attityd användarna och organisationen har inför ett eventuellt införande och brukande av smarta kort.

3.3.4 Genomförandet av intervjuerna

De intervjuer som genomfördes gjordes på plats med närhet till respondenterna och deras egen miljö. För att respondenterna skulle känna sig så bekväma som möjligt, inleddes intervjuerna med att respondenterna fick förklara sina egna arbetsuppgifter och hur länge de arbetat inom organisationen. Enligt Lundahl och Skärvad (1991) är detta en av grundreglerna för att underlätta en intervju. Eftersom vi valde att göra intervjuerna strukturerade samt semistrukturerade, fick vi tillfällen att ställa följdfrågor samt nya frågor under intervjuerna för att få djupare förståelse.

För att vara säkra på att inte missa något i intervjuerna, valde vi att spela in samtalen med en bandspelare. Detta är något som Holme och Solvang (1997) tillsammans med Lundahl och Skärvad (1991) rekommenderar, då sammanställningen kan bli så komplett som möjligt och allt som respondenten säger kommer med. Nackdel kan dock vara att det kan bli något tidskrävande, men vi anser att vi ökar uppsatsen pålitlighet genom att spela in intervjuerna.

Intervjuerna har dock snabbt renskrivits efter varje intervjutillfälle, då vi ville vara säkra på att inte glömma bort varför vissa diskussioner eller följdfrågor uppkom.

Enligt Lundahl och Skärvad (1991) är det även viktigt att respondenterna får läsa igenom den transkriberade intervjun, då de ska få chansen att rätta eller kommentera det som skrivits. Det kan vara så att de ibland ångrar vissa uttalanden och inte vill ha med dessa. Detta kan dock vara en nackdel om det är så att respondenten vill ta bort något som kan vara en viktig del i uppsatsen. Efter att intervjuerna transkriberats rakt av gick vi igenom dem och ändrade från talspråk till skriftspråk samt lät ta bort data som inte alls var relevant för studien. Därefter har samtliga respondenter fått möjlighet att läsa igenom materialet samt ändra eller lägga till text vid behov. Detta hjälper oss också att säkerhetsställa det resultat vi får, och inte dra några felaktiga slutsatser från intervjuerna. I samband med detta bad vi även om vissa förtydliganden av texten eller uttryck. I vissa fall e-mailade vi även följdfrågor, då vi kände att vi saknade svar från första tillfället. När vi fått svar från respondenterna sammanställde vi intervjuerna med utgångspunkt från följande enheter; ITC, IT-Planering, IT-kontaktpersonerna samt användarna och strukturerade upp intervjumaterialet under respektive grupp i enlighet med forskningsfrågorna och det nuvarande utseendet.

3.3.5 Genomförandet av enkätundersökning

Som tidigare nämnt var det IT-kontaktpersonerna på Länssjukhuset Ryhov som delade ut enkäten på respektive klinik och sammanlagt delades 50 enkäter ut. Detta skedde innan våra intervjuer genomfördes och vi kunde därför samla in enkäterna vid dessa tillfällen. Enkäten bestod av 27 frågor med olika alternativ, så att det skulle underlätta svarstiden av den. Enkätsvaren har sedan sammanställs i ett Excel dokument för att vi lättare ska kunna analysera svaren, se bilaga 4 och 5.

3.3.6 Analysmetod

I kapitel 6 kommer den data som vi har samlat in genom intervjuer och enkäter att analyseras tillsammans med informationen och teorierna i kapitel 2 och 4. Vi har valt att använda oss av forskningsfrågorna som en röd tråd under arbetets gång och utifrån dessa strukturerat teori, empiri och slutligen även analysen. Vi anser att detta ökar förståelsen för läsaren men viktigast av allt underlättar det analysen av datan. Vi har utifrån vårt sammanställda material försökt hitta mönster, likheter och olikheter som sedan analyserats. Repstad (1999) påpekar vikten av att det analytiska arbetet är strukturerat och utförs på ett systematiskt sätt. Genom att strukturera upp ämnesområdena och informationen på ett genomgående likartat sätt anser vi oss underlätta analysarbetet och hitta olika mönster men även minska risken för att utelämna viktig information.

Som nämnts ovan har vi valt att strukturera analysen utifrån de fyra forskningsfrågorna vi använder oss av för att uppfylla syftet med uppsatsen. Frågorna kommer att användas som rubriker, dock i en förkortat version. Rubrikerna som används, både huvudrubrik samt underrubriker är som sagt kopplade till resterande delar av uppsatsen. Rubriken för forskningsfråga nummer ett är följande:

- Hur kan smarta kort förbättra IT-säkerheten inom hälso- och sjukvården?

Under denna forskningsfråga kommer sedan underrubriker relaterade till informationssäkerhet samt smarta kort att användas. Detta då forskningsfrågan hanterar informationssäkerhet, IT-säkerhet samt smarta kort.

Analysen relaterad till forskningsfråga nummer två som inriktar sig på mobilitet och hur smarta kort kan öka mobiliteten bland vårdgivare och patienter kommer att inledas med följande rubrik:

- Hur kan smarta kort öka mobiliteten?

Forskningsfråga nummer två skiljer sig dock från övriga delar då den inte är förankrad i teorin på samma sätt, det vill säga inte har en egen rubrik utan istället diskuteras under kapitel **Fel! Hittar inte referenskälla.** i förundersökningen. Vi anser dock att den är förankrad i flera delar av teorin.

Forskningsfråga nummer tre behandlas därefter och vi har här för avsikt att diskutera elektroniska journaler, behovet av dem samt säkerheten kring dem. Trots att frågan även täcker in pappersjournaler anser vi att vikten ligger på e-journaler och dess användningsområde och vi anser därmed att följande rubrik reflekterar forskningsfråga nummer tre.

- Hur ser behovet och säkerheten ut gällande e-journaler?

I den sista analysdelen, kopplad till forskningsfråga nummer fyra, diskuterar vi förändringar och förändringsarbete inom hälso- och sjukvården och kommer att använda följande rubrik:

- Hur ser attityderna ut gällande datoranvändningen samt säkerheten?

Vi har även valt att använd underrubrikerna; attityder till förändringar samt diffusionsteori i samband med denna forskningsfråga. Detta för att underlätta läsandet samt analysarbetet. Attityder är en central del av forskningsfråga nummer fyra, då det för oss är av stort intresse att se hur attityderna ser ut idag bland användarna och om smarta kort därmed kan vara en lämplig teknik att införa inom hälso- och sjukvården. Diffusionsteori används då det tar upp spridning av en idé eller innovation. Det är enligt oss av intresse att se hur spridningar av ny teknik kan förhålla sig inom hälso- och sjukvården.

3.4 Trovärdighet

För att kunna vara kritiska till vårt egna tillvägagångssätt i uppsatsen, kommer vi här nedan att diskutera olika faktorer som kan ha inverkat på uppsatsen. Vi anser att de viktigaste delarna är reliabiliteten, validiteten och generaliserbarheten. Enligt Holme och Solvang (1997) bestäms reliabiliteten av hur våra mätningar som uträttas och hur exakta vi är vid behandlingen av informationen. Validiteten fastställs däremot av vad vi mäter och om detta är förklarat i frågeställningen.

3.4.1 Reliabilitet

Reliabilitet innebär, enligt Holme och Solvang (1997) hur pålitligt någonting är. Vi anser att vårt resultat blir mer pålitligt genom att göra flera intervjuer samt dela ut enkäten till en större grupp användare. Hansagi och Allebeck (1994) tillsammans med Holme och Solvang (1997) anser att reliabiliteten på en undersökning kan testas genom att göra samma undersökning på samma urval mer än en gång. Då vårt uppsatsarbete är tidsbegränsat har vi ingen möjlighet att göra om samma undersökning på urvalsgruppen, men anser ändå att reliabiliteten ökar genom att göra fler än en intervju samt utföra enkätundersökningen på olika klinikerna runt om på Ryhov.

Intervju
Vi anser att vi får en hög reliabilitet på uppsatsen genom att göra många intervjuer och att de sammanställs på ett pålitligt sätt. Som tidigare nämnt spelade vi in samtliga intervjuer med hjälp av en bandspelare och genom att göra detta anser vi att reliabiliteten ökar. Vi kan lyssna av intervjuerna i flera olika omgångar och kan på så sätt säkerhetsställa respondenternas svar. Vi har även haft möjligheten att höra av oss till respondenterna om förklaringar varit nödvändiga eller om ytterligare frågor dykt upp under arbetets gång. Detta i samband med att respondenterna dessutom fått möjligheten att läsa igenom intervjuerna och ge oss ett godkännande efter transkriberingen har enligt oss lett till högre reliabilitet.

Enkät
Vi delade ut 50 stycken enkäter på Länssjukhuset Ryhov och av dessa har vi fått tillbaka samtliga som vi kunnat sammanställa. Vi anser att reliabilitet är hög, då vi inte haft något bortfall. Vid sammanställningen av enkätsvaren var vi noga med att inte göra några inmatningsfel och dubbelkollade den aktuella enkäten innan vi gick vidare med nästa. Holme och Solvang (1997) menar att ett resultat är representativt då urvalet kan ge en riktig bild av ett fenomen i förhållande till hela populationen.

För att nå ut till användarna på Länssjukhuset Ryhov, till vilka enkäten utfärdades, skedde detta via vår kontaktperson samt de IT-kontaktpersoner som vi intervjuade. Detta kan ha påverkat reliabilitet och vårt resultat, då användarna kan ha valts med hänsyn till datorvana och position på klinikerna och inte valts ut av slumpen. Då vi inte heller har varit på plats när enkäten besvarats på de olika klinikerna, kan vi inte heller säga med säkerhet att det är just de personer som enkäten var ämnad för som har svarat på den. Detta kan också ha påverkat reliabiliteten. Vi påpekade dock vikten, av att urvalet av respondenter blev fördelat mellan yrkeskategorier, ålder, kön och datorvana, för vår kontaktperson. Vid insamlandet av enkäterna nämnde dock några av respondenterna att de hade fördelat enkäterna mellan de olika kategorierna ovan, men det är som sagt svårt för oss att kontrollera.

3.4.2 Validitet

Som tidigare nämnt är validiteten beroende av vad vi mäter och om detta är förklarat i frågeställningen. Eftersom vi inte träffat personerna innan intervju- och enkät tillfällena, var det svårt att veta om vi ställde rätt frågor till rätt personer. Vi anser dock att då vi tagit hänsyn till forskningsfrågorna samt syftet vid utformningen av frågorna har vi hög validitet.

Intervju
Problemet med att få giltig (valid) information är enligt Holme & Solvang (1997) i grundregel mindre i kvalitativa undersökningar än kvantitativa av den orsaken att vi har närhet till studieobjektet. Vid kvantitativa metoder blir däremot urvalet bara giltigt under premissen att vi som undersökare mäter det vi vill mäta. För att få så hög giltighet som möjligt har vi utgått från syftet och teorier vid utformandet av intervju- och enkätfrågorna. Då vi använt oss av vårt syfte samt teori för att utforma intervjufrågorna, anser vi att vi har mätt det vi avser att mäta. Vi har också intervjuat de personer som ansett sig vara kunniga inom det område vi studerar och vi ställde hela tiden olika följdfrågor för att få en djupare förståelse i de svar de gav oss. För att respondenterna skulle generera genomtänkta svar valde vi att skicka ut ett e-mail innan intervjutillfället med information om de ämnesområden som intervjun skulle behandla

Enkät
Enligt Andersen (1998) är det svårt att mäta hur hög vår validitet är vid kvantitativa studier, men det bör vara någon slags överensstämmelse mellan våra teoretiska studier och empiris-

ka studier. I enkäten har vi inte ställt några frågor om just IT-lösningen med smarta kort, då vi inte kan utgå från att alla vet vad detta är. Istället har vi koncentrerats oss på att titta på hur de uppfattar den nuvarande dataanvändningen och vad som skulle kunna blir bättre i framtiden. På så sätt har vi sett till att frågorna är utformade efter vad användarna kan tänkas ha information om och inte behöva svara på något som de inte har stor kunskap om. Det vi har velat få fram om smarta kort har vi istället tagit vid intervjutillfällena, då dessa har genomförts på kunniga personer inom ämnet smarta kort samt projektet SITHS.

3.4.3 Generaliserbarhet

Enligt Holme och Solvang (1997) innebär generalisering att allmänna slutsatser ska kunna dras från ett antal observationer. Det är lättare att mäta generaliserbarhet i kvantitativa studier än med kvalitativa studier, då informationen i kvantitativa studier är mer strukturerade och formaliserade.

Då vi ser på IT-säkerheten kan vår studie vara möjlig att applicera även på andra sjukhus, trots olikheter i organisationen. De flesta sjukhus har sin egen specialitet och specifika kunskap och kan därmed skilja sig mellan varandra i arbetssätt, rutiner och uppbyggnad. Länssjukhuset Ryhovs olika kliniker skiljer sig mycket åt i hur de arbetar och hur långt de kommit i användning av IT-stöd och i och med att skillnaden är stor även inom sjukhuset kan vi påstå att skillnaden på så sätt inte bör blir större gentemot andra sjukhus. Då vi kan applicera vår studie på hela Länssjukhuset Ryhov, anser vi det därmed vara möjligt att i relativt stor utsträckning applicera vårt resultat även nationellt sett. Carelink har som utgångspunkt att anpassa alla säkerhetsdelar nationellt och därav anser vi att vår studie i viss mån kan generaliseras.

Intervju
Målet med våra intervjuer var att skapa en förståelse för hur Landstinget fungerar och hur den nuvarande säkerhetsaspekten påverkade deras arbetssituation. Det är enligt Holme och Solvang (1997) svårt att från kvalitativa metoder generalisera, men det är inte heller syftet med våra intervjuer. Vi vill med intervjuerna istället få en helhetsbild, men även en djupare förståelse över den situation som råder på Länssjukhuset Ryhov idag och vad som kan förbättras i framtiden.

Enkät
Enligt Holme och Solvang (1997) går det att med statistiska undersökningar dra genrealiseringar genom att ställa våra teorier mot de empiriska studierna vi samlat in. Vi kan med våra enkätsvar dra vissa generaliseringar gällande den situation som råder på Länssjukhuset Ryhov, men inte med säkerhet på hälso- och sjukvården i allmänhet. Det finns dock, som diskuterats ovan, möjlighet att se likheter nationellt sätt.

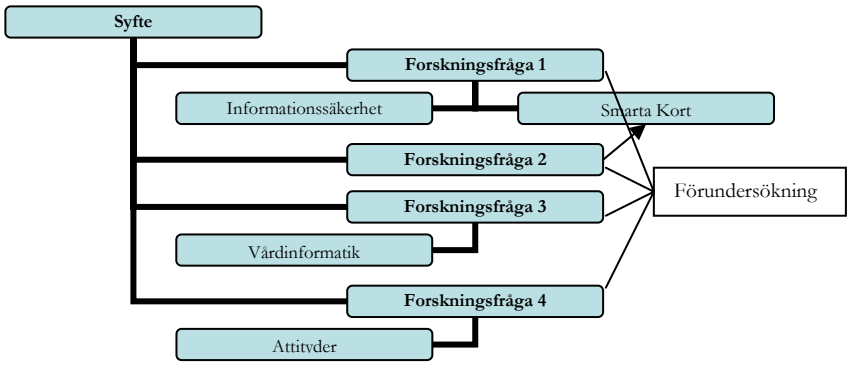
För att hanteringen av våra insamlande data inte skulle bli för svår och allt för tidskrävande, valde vi ett bestämt antal intervjuer och enkäter. Detta kan ha påverkat vår generaliserbarhet, då bortfall av enkätsvar kan bli väsentligt vid ett bestämt antal enkäter. Vi anser dock att 9 intervjuer och 50 enkäter, varav inget bortfall av enkätsvar, ger oss bra grund för uppsatsens pålitlighet, giltighet samt generaliserbarhet.

4 Referensram

I referensramen kommer vi att redovisa de kunskaper och teorier som vi har införskaffat oss genom vår genomförda litteraturstudie. Teorierna syftar till att ge en bättre förståelse kring ämnet informationssäkerhet, hälso- och sjukvården samt bakgrund och information om smarta kort. I samband med varje huvudrubrik kommer vi att inleda med en förklaring till vad det efterföljande teoriavsnittet bidrar med till vår studie.

4.1 Samband mellan forskningsfrågor och avsnitt

Vi vill inleda det här kapitlet med en figur (Figur 4-1) samt en förklaring till hur följande rubrikstycken hör ihop med våra forskningsfrågor. Vi hoppas på så sätt skapa en större förståelse för sambandet mellan avsnitten och forskningsfrågorna. Vi vill påpeka att det finns ytterligare kopplingar mellan ämnena men detta är utgångspunkten för hur teorin har tagits fram utifrån forskningsfrågorna och syftet. Kopplingarna visar därmed grundstrukturen mellan forskningsfrågorna och de olika teoriavsnitten.



Figur 4-1 Samband mellan forskningsfrågor och val av avsnitt

- I första avsnittet kommer vi att behandla ämnet informationssäkerhet, då detta område ligger till grund för forskningsfråga nummer ett. Informationssäkerhet rymmer många olika delar som, enligt oss, är viktigt att förstå i samband med vår studie, då syftet är att undersöka förutsättningarna för hur smarta kort som en del av en total säkerhetslösning kan förbättra säkerheten inom hälso- och sjukvården.

- Under avsnittet Smarta kort vill vi ge en bakgrund till smarta korts uppkomst samt redovisa för vad ett smart kort är och hur det kan användas. Detta för att öka förståelsen för smarta kort som är en central del av vårt syfte. Smarta kort hjälper oss att svara på forskningsfråga ett och två. Även förundersökningen ligger till grund för att skapa förståelse för forskningsfråga två och tre.

- Då vår studie fokuserar på förutsättningarna för hur användandet av smarta kort inom hälso- och sjukvården kan förbättra IT-säkerheten är det enligt oss också viktigt att studera informationssäkerhet ur ett vårdperspektiv. Vi har därmed valt att beskriva vad som menas med vårdinformatik och hur tekniken kan öka tillgängligheten till viktig information. Informationen om journaler samt lagar ses som en vik-

tig grund för vår tredje forskningsfråga som fokuserar på hur säkerheten ser ut kring e-journaler i jämförelse med pappersjournaler.

- Med vår fjärde forskningsfråga vill vi undersöka hur attityder till datoranvändning, förändringar samt säkerheten ser ut. Detta för att se om det finns ett behov av smarta kort och om det därmed kan vara lämpligt att implementera, framförallt på Länssjukhuset Ryhov. Därmed kommer vi i följande avsnitt att diskutera förändringsarbete, attityder samt diffusionsteori.

4.2 Informationssäkerhet

Enligt Mitrović (2005) handlar informationssäkerhet om att skydda sina informationstillgångar. Organisationer hanterar idag stora mängder värdefull information och genom datatekniska och administrativa åtgärder måste de hålla en optimal nivå gällande tillgänglighet, modifierbarhet, sekretess och spårbarhet. Som tidigare nämnt ingår IT-säkerhet som en del av informationssäkerhet och är ett samlingsnamn för den teknik som ska stödja processen att skydda information elektroniskt. Medan informationssäkerhet, enligt Mitrović (2005), syftar till att skapa policys, riktlinjer, etc., för att skydda informationstillgången i en organisation, syftar IT-säkerhet till att bevara tillgänglighet, modifierbarhet, sekretess och spårbarhet i informationssystemet.

4.2.1 IT-säkerhet

Sekretess (Confidentiality), menas att innehållet i ett informationsobjekt inte får göras tillgänglig eller avslöjas för obehöriga. Sekretess innebär enligt Bishop (2003) alltså att en organisation vill dölja information eller resurser från obehöriga. Inom exempelvis hälso- och sjukvården samlas det dagligen in och bearbetas mycket information om enskilda människor. Information som många gånger är känslig att delge någon annan än vårdtagaren själv. Det är av stor vikt att denna information skyddas och att patientens integritet kan bibehållas för patienten själv samt för förtroendet mellan både vårdgivare och vårdtagare (Ruland, 2002). Personal inom hälso- och sjukvården är bundna till tystnadsplikt genom sekretesslagen och ska inte delge känslig information till utomstående part. Samtidigt är det ofta av stor vikt att insamlad information delas med andra vårdgivare eller annan vårdpersonal för att kunna ge patienten bästa möjliga vård. Genom att information om patienter ändå sprids mer eller mindre är det viktigt att vårdgivare tar sitt ansvar.

Spårbarhet (accountability), syftar till möjligheten att kunna spåra processer som skett i systemet och vem som har utfört dem (Mitrović, 2005). Spårbarhet kallas även loggning och innebär att varje användare som har behörighet till systemet ska kunna ställas till svar för sina handlingar om dessa är allvarliga. Systemet måste därför innehålla vissa mekanismer för loggning som kan bevisa att användaren exempelvis mottagit ett viss e-mail eller inte.

Tillgänglighet (availability), avser möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid (Bishop, 2003). Tillgängligheten är en viktig del i systemets pålitlighet, för ett system som inte fungerar är lika illa som att inte ha ett datasystem över huvudtaget. Aspekten tillgänglighet är också relevant i IT-säkerhet då någon obehörig medvetet ser till att användarna nekas tillträde till systemet genom att manipulera data.

Modifierbarhet (integrity), syftar till hur trovärdig data eller resurserna är och innefattar innehållet av informationen samt kontroll av uppgiven identitet av användare, autentisering. Detta innebär att systemet ska skydda obehöriga från insyn, påverkan samt oönskad för-

ändring. Enligt Bishop (2003) skiljer sig det att jobba med modifierbarhet och sekretess. Med sekretess är data antingen kompromitterad eller inte, medan modifierbarhet inkluderar både korrigering och trovärdighet av data, det vill säga att källan till informationen kan stödjas genom noggrannhet och trovärdighet från de ansvariga som från början lagt in informationen i systemet.

4.2.2 Hot och risker

Effektiv IT-säkerhet kan endast införas då organisationen är medveten om vilka hot och risker som kan inträffa och vilka svagheter det finns inom organisationen (Mitrović, 2005 och Carelink, 2006e). Hot kan vara någon form av händelse eller handling som kan skada de IT-resurser som finns inom företaget. Svaghet syftar till den tekniska utformningen av en IT-resurs med eventuella brister. Detta kan vara dåliga rutiner eller den interna kontrollen (kvalitetssäkring). Sårbarhet avser svaghet i systemet eller i verksamheten, som har någon bristande förmåga att motstå hot. Genom att titta på hot, svagheter och spårbarhet kan organisationen skapa sig en hotbild. Det kan vara möjligt att titta en hotbild för enskilda IT-resurser, men vanligast identifieras flera IT-resurser som är berörda.

4.2.3 Auktorisering

För att ett företag ska få en så bra IT-säkerhet som möjligt är en viktigt dela att hantera auktoriseringen till datasystemen så effektivt som möjligt (Mitrović, 2005). Det är viktigt att användaren får rätt behörighet och tillstånd till de system som ska användas. Det är också angeläget att organisationen har med i beredskap att användare slutar på arbetsplatsen och inte längre ska ha behörighet till datasystemet. Här måste det finnas ett effektivt sätt att stoppa behörigheten, så att användaren inte längre har tillgång till den information som finns inom organisationen. Enligt Bishop (2003) kommer det största hotet från människorna inom en organisation och inte utanför. Det är oftast missnöjda anställda eller andra inom organisationen som har kunskap om systemet och kan komma igenom de säkerhetsrutiner som annars hade stoppat en obehörig person.

Autentisering
Enligt Bishop (2004) är autentisering i ett system när en identitet kan bindas till en enhet. Om detta är en extern enhet, måste den innehålla sådan information att systemet kan bekräfta identiteten av användaren. Det huvudsakliga målet med en autentisering är att försäkra att alla enheter är korrekt identifierade. Autentiseringen går igenom tre steg, då en användare ska identifieras. Det första är att få information från användaren, det andra blir sedan att analysera informationen och det tredje är att bestämma om denna information hör ihop med användaren.

Information i ett system som måste bekräfta en identitet kan utföras på olika sätt (Bishop, 2004);

- **Något som användaren vet** (lösenord eller någon annan hemlig information)

Lösenord är den mest grundläggande autentisering mekanismen och baseras på vad användaren vet (Bishop, 2004). Författaren definierar lösenord som information som är associerad med en enhet och som konfirmerar enhetens identitet. Användaren skriver in sitt lösenord och om lösenordet stämmer överens med användarens identitet godkänner systemet användaren. Skulle lösenordet vara fel avslår systemet användaren och inloggningen misslyckas.

Enligt Bishop (2004) är den vanligaste attacken mot lösenordsbaserade system att gissa lösenorden. Oftast börjar gissningen på korta lösenord eftersom det finns färre av dem och detta gör det möjligt att pröva dem alla. Det är därför viktigt att det finns regler på hur många tecken ett lösenord bör innehålla. Människor kan komma ihåg upp till åtta tecken utan problem, men det kan bli svårt att komma ihåg mer än ett sådant. Om användaren måste komma ihåg flera långa lösenord, blir de oftast nerskrivna. Beroende på vart dessa nerskrivna lösenord bevaras kan dock utgöra en säkerhetsrisk. Att bevara ett lösenord i sin plånbok anses säkrare än att skriva ner det på en papperslapp och ha det vid tangentbordet.

- **Något som användaren är** (fingeravtryck, ögonavläsning)

Biometri är ett mer avancerat sätt att identifiera en användare. Biometri är ett mer avancerat sätt att identifiera en användare. Enligt Bidgoli (2002) scannas delar på människokroppen för att säkerhetsställa en identitet i biometri och bygger på att människokroppen är unik för varje person. Dessa delar kan inte bli stulen, förlorad eller kopierad på samma sätt som ett lösenord eller ett kort. Olika sätt att säkerhetsställa en identitet hos en användare kan vara;

  - Fingeravtryck: Användaren måste scanna sitt fingeravtryck för att kunna bli verifierad och få tillåtelse att använda systemet.
  - Handgeometri: Mäter längden på fingrarna, avstånden mellan fingertopparna samt huden mellan fingrarna på båda händerna.
  - Näthinnan: Näthinnan scannas med hjälp av ögonkamera och identifierar användaren med hjälp av data som redan är lagrad i systemet. Är en av de mest framgångsrika metoderna i biometrin.
  - Röstigenkännande: Översätter ord till digitala mönster och överför detta till en server. Mönstret i rösten är registrerad och undersöks bland annat per ton.

De här olika sätten har enligt Bidgoli (2002) varit ett framgångsrikt sätt att skydda obehöriga från datasystem, men är fortfarande en dyr IT-säkerhetslösning.

- **Något som användaren har** (smarta kort, bricka)

Beskrivs närmare i följande stycke.

4.3 Smarta kort

Enligt Bidgoli (2002) är smarta kort ett sätt att öka säkerheten i en organisation. Som en behörighetskontroll och autentisering används idag smarta kort på olika sätt inom en organisation för att på ett säkert sätt identifiera en användare. Smarta kort kan bland annat användas som passerkort och vid inloggning till ett datasystem.

4.3.1 Smarta korts historia

Den första användningen av plastkort tog sin början i USA under 1950-talet. Korten användes då som betalkort och var utfärdade av Diners Club (Rankl och Effing, 2001). Betalkorten var då endast till för exklusiva medlemmar som egentligen betalade med sitt goda namn än med kontanter.

Enligt Rankl och Effing (2001) var kortets funktioner i början mycket enkla, men utgjorde ändå sitt syfte med att förvara data på kortet från förfalskning och manipulation. Information såsom användarens namn var tryckt på framsidan medan personlig data och kortnumret var ett relieftryck, det vill säga, de buktade ut från kortet. För att ytterliggare öka säkerheten med att förhindra förfalskning krävdes ett synligt kännetecken som godkände transaktionen och detta kunde antingen vara en signatur eller ett säkerhetstryck.

Då användningen av korten började öka kraftigt, fick affärer och banker börja införskaffa maskinavläsning för korten istället för att göra allt manuellt (Rankl och Effing, 2001). Samtidigt började även bedrägerierna för korten att öka kraftigt och det stod klart att säkerheten på korten måste utökas mer och förbättras. Den första förbättringen som gjordes var att sätta en magnetremsa på kortets baksida, vilket gjorde det möjligt att nu förvara digital data i en läsbarform. Användarens signatur behövdes dock fortfarande för att identifiera rätt korthållare. I och med den nya magnetremsan minskade pappersarbetet avsevärt, även om pappersnotor med signaturerna måste sparas. Nya applikationer idag gör det möjligt att även utesluta pappers nota som en säkerhets del. Identifikationen av korthållaren kan idag göras med hjälp av en så kallad PIN (Personal Identification Number) kod. PIN koden jämförs med ett referens nummer som är kopplat till kortet och godkänner transaktionen.

Betalkortet med en magnetremsa är fortfarande idag det mest användbara, men har dock några starka nackdelar. Data som är lagrad på magnetremsan kan avläsas, bli borttagen samt ändrad av personer med rätt utrustning. Uppdaterad teknik måste hela tiden appliceras för att skydda mot bedrägerierna, men detta har med åren blivit mycket kostsamt. För att minska dessa kostnader behövdes lösningar tillämpas där transaktionerna inte behövde stå i direktkontakt med banken, men ändå kunde utföras säkert (Rankl och Effing, 2001).

Framställningen av smarta kort skapade nya möjligheter för att lösa det här problemet. De första smarta kort som kom under 1970-talet innehöll ett chip som gjorde det möjligt att integrera data som var lagrad på kortet med matematisk logik, och på så sätt förbättra säkerheten. Det var dock inte förrän under 1980-talet som smarta kort fick sitt riktiga genombrott. Då beslöt sig French PTT (postal och telecommunication services) att använda sig av smarta kort som telefonkort. Även om smarta kort ännu inte användes på de områden där redan existerande plastkorten användes, uppfylldes ändå de förväntningarna som fanns för att minska bedrägerier och öka pålitligheten (Rankl och Effing, 2001).

Smarta kort är flexibla och dess höga funktionalitet gör det möjligt att korten hela tiden kan bli omprogrammerade med nya applikationer. Transaktioner med smarta kort genomförs offline, det vill säga, att de som är inblandade i transaktionerna inte behöver vara i kontakt med en huvuddator för att köpet ska godkännas. Detta har resulterat att det har öppnats helt nya områden, förbi de traditionella kortapplikationer, med smarta kort.

Enligt Rankl och Effing (2001) kan smarta kort delas in i två stycken grupper;

- Minneskort
- Kort med mikroprocessor

4.3.2 Minneskort

De första smarta korten som kom ut på marknaden var så kallade minneskort och användes som tidigare nämnt mest som telefonkort (Rankl och Effing, 2001). Kortens användes som ett ”kontantkort” och var förbetalda eftersom värdet förvarades elektroniskt i ett chip på kortet. Varje gång kortet användes minskade värdet med den summa som det kostade

att nyttja kortet. För att förhindra att kortet manipulerades, var chipet förprogrammerat med en matematik logik som gjorde det omöjligt att bort minnet när det väl var skrivet. Nackdel med kortet var dock att när det redan var tomt gick det inte att fylla på det igen. Det blev ett onödigt kortslöseri, då dessa bara fick slängas. Minneskorten hade bara begränsade funktioner, med dess säkerhet på chipet gjorde det möjligt att skydda data mot fiffel och bedrägerier.

4.3.3 Kort med mikroprocessor

De första smarta korten med en mikroprocessor var ett bankkort som användes i Frankrike (Rankl och Effing, 2001). Kortets möjlighet att förvara privata nycklar och utföra modern kryptografi gjorde det möjligt att göra säkra transaktioner utan att behöva stå i direktkontakt med banken. Mikroprocessorn gör det möjligt att programmera och utöka applikationer allteftersom. Ett stort användningsområde av dessa smarta kort är korten i mobiltelefoner, men används också som identifikationskort, accesskontroll för känsliga områden, skydda lagrad data, elektroniska signaturer och elektroniska köp. Enligt O'Mahony, Pierce och Tewari, (2001) kan kort med mikroprocessor även delas in i följande;

Kontaktkort: Chipet på kortet kräver en extern enhet, exempelvis en kortläsare, för att kunna importera och exportera data. Det smarta korten utför dessa operationer genom en direkt kontakt med enheten.

Kontaktlösa kort: Den här typen av smarta kort är enligt O'Mahony et al. (2001) mer flexibla än de kort som kräver kontakt med en extern enhet. Kortet behöver inte komma i direkt kontakt med exempelvis en kortläsare utan använder istället någon typ av elektronisk koppling för att kommunicera med kortläsarenheten. Det kontaktlösa kortet bör dock placeras nära enheten för att kunna utföra sina operationer. Nu finns det dock även smarta kort som använder sig av radiovågor för att klara av längre distanser.

4.3.4 Smarta kort och säkerhet

Det finns två olika säkerheter associerat med ett smart kort (O'Mahony et al, 2001);

Logisk säkerhet: Här är chipet på kortet designat så att inga enskilda funktioner eller kombinationer kan utföras och avslöjas på kortet förutom det som korten tillåter. Detta kan uppfyllas genom att en intern övervakning, så som operativsystem, applikationer och loggning bevakar de operationer som utförs.

Fysisk säkerhet: Förutom den logiska säkerheten har korten också en fysisk säkerhet. Speciella lager med oxid över chipet skyddar innehållet på kortet från att bli analyserat. Även om lagret skulle tas bort, går det ändå inte att avläsa några data.

Vanligtvis är föremålet för smarta kort att rätt användare använder kortet (Wettergren, 1997). Därför innehåller kortet både en hemlig nyckel och ett certifikat som tillsammans identifierar rätt data. Det är vanligt att det inte finns någon mekanism implementerad på kortet som tillåter att tillåta rätt mottagare att öppna meddelandet. Ett smart kort har heller inte vanligtvis en publik nyckel av utfärdaren eller en kod som använder det. När en gemensam autentisering är utförd, så är det oftast terminalen själv som utför den på kortens begäran.

Kortet själv går igenom olika faser innan det kan användas. Först är det programmerat för att klara ett visst antal operationer och sedan blir det ”personaliserat”, för att kunna knytas

till ett viss användare. När detta sedan är klart får användaren själv välja Pinkod för att sedan kunna börja använda det (Wettergren, 1997).

Genom att begära att användaren har ett lösenord, vanligtvis i form av en Pinkod, kan det smarta kortet identifiera rätt användare med korten innan det utför den begära operationen (O'Mahony et al., 2001). Enligt Wettergren (1997) var en tidig tillämpning av smarta kort att ha en symmetrisk nyckel lagrad på kortet. Nyckeln används i kombination av rätt Pinkod för att utföra önskade åtgärder. Om fel Pinkod slagits in ett antal gånger, låser sig det smarta kortet sig själv. Dock innehåller kortet en andra nivå med Pinkod som gör det möjligt att låsa upp kortet igen. Om denna Pinkod dock matas in fel, har kortet låst sig själv för evigt.

4.3.5 Smarta kort som identifikationskort

Roland Moreno, smarta kortets uppfinnare, anser att den garanterade identitetssäkerheten är den mest intressanta egenskapen med smarta kort. Enligt Höynä (1997) var Sverige ett av de först länderna med att använda smarta kort som en elektronisk Identitetskort, EID. Det första kortet var ett tjänstekort som nyttjades av Rikspolisstyrelsen, Riksskatteverket och Riksförsäkringsverket.

Enligt Finkenzeller (2004) är smarta kort den yngsta medlemmen i familjen av identifikationskort i det så kallade ID-1 formatet. Den karaktäriseras av vissa egenskaper som är inbäddat i kortet. Dessa egenskaper gör det möjligt att överföra, förvara och processa data med kortet. Data överföringen kan ta plats antingen via kontakt med kortet eller via elektromagnetiska fält utan kontakt. Smarta kort erbjuder många möjligheter jämfört med ett vanligt kort med magnetremsa. Bara förvaringsmöjligheten är många gånger större än vanliga kort. Den viktigaste fördelen är dock att data på kortet kan skyddas mot obehöriga och manipulation. Eftersom korten är kopplat till ett operativsystem skapas möjligheten att skriva konfidentiell data till kortet så att det inte kan läsas utifrån. Minnesfunktionerna på kortet som att lägga till, ta bort och avläsa data kan länkas ihop på vissa villkor från både hårdvara och mjukvara.

4.3.6 Smarta kort i hälso- och sjukvården

Enligt Höynä (1997) är hälsoområdet det tredje största området till att använda smarta kort efter bankkort och telefonkort. Utvecklingen har dock gått långsamt framåt, eftersom hälsokortet varit en känslig fråga för myndigheterna på grund av dess innehåll och funktion. Målet är dock att kortet ska användas för att patienten ska kunna identifiera sig samt innehålla information så som patientens medicinska historia och akut medicinska uppgifter. Även personal inom hälso- och sjukvården kan använda smarta kort för att identifiera sig samt bli mer mobila (Höynä, 1997). Korten kan innehålla information som namn, yrke, sjukhusets namn, tidigare praktiker, expertutdrag och annan tekniks data så som vilken behörighet den anställde har vid sin arbetsplats.

4.4 Vårdinformatik

Med informatik menas, enligt Petersson och Rydmark (1996), läran om informationsbehandling, vilket betyder att genom utnyttjandet av olika metoder försöka automatisera insamling, lagring, bearbetning, användning, presentation, överföring samt kommunikation av data. Petersson och Rydmark (1996) menar att när IT används i kombination med en ämnesdisciplin så som medicinsk informatik (MI) innebär detta att organisationer ägnar sig

åt informationsbehandling och kommunikation inom det aktuella området och i detta fall i hälso- och sjukvårdens verksamhet, utredning och forskning.

Att använda IT inom hälso- och sjukvården har inte varit av prioritet under många år och utvecklingen har gått långsamt. Detta beror enligt Regeringen (2006) bland annat på att hälso- och sjukvården är en komplex organisation med mycket integritetskänslig information som måste skyddas. Under senare år har dock kraven på sjukvården ökat både gällande bättre vårdkvalitet samt ökad effektivisering av de resurser som finns att tillgå. Enligt den Nationella IT-strategin för vård och omsorg kommer medborgarna i framtiden att ställa högre krav samt vilja ha en mer anpassad vård där de som individer har möjlighet till egna val. Detta på grund av bland annat längre vårdköer och mindre resurser inom hälso- och sjukvården (Regeringen, 2006).

Även Ruland (2002) menar att IT kan utgöra en avgörande roll för effektivisering och bättre kvalitet då hälso- och sjukvården är en informationsintensiv organisation där integration mellan verksamhetsområden är nödvändig. Det har även fastställts i den Nationella IT-strategin för vård och omsorg att vårdkvalitet, tillgänglighet samt patientsäkerhet kan nämnvärt förbättras med hjälp av IT-stöd. Det är, som nämns ovan, av stor vikt att relevant information finns att tillgå för att säkerställa vårdkvaliteten, vilket kan realiseras med hjälp av informationsteknologi och mer specifikt med hjälp av elektroniska journaler (Regeringen, 2006)

4.4.1 Elektronisk journal

Enligt Ruland (2002) är patientinformation en av de viktigaste byggstenarna vid vård av patienter. Patientjournalen är det arbetsredskap som kan tillhandahålla denna information. All vård av patienter skall enligt Johnsson (2002) dokumenteras i en journal och ska inte ses som enbart en administrativ uppgift utan även som en del av vården av patienten. En patientjournal menar Gratte (1996) och Ruland (2002) kan ses som det mest centrala kommunikationsmedium för vårdpersonal när de undersöker, behandlar och vårdar patienter. Det är därmed av stor vikt för att kunna göra rätt bedömningar vid vårdtillfället att patientjournalen finns till handa. En journal kan ge vårdgivaren en överblick över en patients sjukdomshistoria, vilket kan vara avgörande för att ge rätt typ av behandling. Patientjournalen ska enligt Gratte (1996) och Ruland (2002) inte bara vara lättillgänglig utan även vara välskriven så att den på ett snabbt och lätt sätt ska kunna användas av flera olika vårdgivare. Problem och i viss grad förhinder vid användandet av patientjournaler är de lagar och förordningar som måste följas för att säkerställa patienters integritet (Regeringen, 2006). Journalen ska vara tillgänglig för vårdpersonal, men de måste samtidigt följa de lagar som finns vid förvaring och arkivering av dessa. Förandet av journaler regleras genom patientjournallagen (Riksdagen, 2003).

Enligt Gratte (1996) är en patientjournal ett juridiskt dokument som i efterhand ska kunna användas som utredningsmaterial om misstag har begåtts etc. En journal bidrar även enligt Johnsson (2002) till kvalitetsutveckling samt en enhetlighet inom vården. En journal kan sparas på olika typer av medium och fortfarande vara en journal och i och med det är journaler enlig Johnsson (2002) teknik neutrala. I en patientjournal ingår alla typer av anteckningar, remisser, laboratoriesvar, röntgenbilder, rapporter etc. som tillhör den patienten vare sig det är en pappersjournal eller en elektroniskt lagrad journal.

4.4.2 Patientjournallagen

Enligt patientjournallagen skall en patientjournal föras vid vård av patient inom hälso- och sjukvården samt tandvården och journalen skall vara individuell. Med patientjournal avses enligt Socialstyrelsen (1994) alla uppgifter så som anteckningar och handlingar som innehåller uppgifter om de åtgärder som genomförts eller planeras samt information om patientens tillstånd. Patientjournalen skall utgöra ett stöd och arbetsverktyg för vårdgivaren samt verka som ett beslutsunderlag för eventuella åtgärder. Patientjournalen är även viktig för att säkerställa kvalitet och säkerhet inom hälso- och sjukvården samt ses som ett viktigt instrument vid uppföljning och utvärderingsarbetet inom vården. Vidare kan journalen även vara av stor betydelse vid legala sammanhang och vid forskning. (Socialstyrelsen, 1994 och Johnsson, 2002).

Patientjournalerna skall enligt Socialstyrelsen (1994) vara skrivna på svenska och så tydliga som möjligt för att underlätta för annan behandlande personal. Journalen skall skrivas så att patientens integritet respekteras. Enligt särskilda föreskrifter av socialstyrelsen skall överkänslighet som kan leda till allvarliga eller livshotande tillstånd markeras i journalen (Socialstyrelsen, 1994).

I enlighet med patientjournallagen är den som är legitimerad eller har särskilt förordnande att utöva vissa yrken enligt Socialstyrelsen (1994) skyldig att föra en patientjournal. Det skall vid varje anteckning i journalen finnas uppgift om vem som har gjort den och när den gjordes det vill sägas den skall signeras av den som ansvarar för uppgiften. Det är inte heller tillåtet (med vissa undantag) att ta bort eller göra uppgifter i journalen oläsliga (Socialstyrelsen, 1994).

Patientjournaler är teknikneutrala, vilket innebär att de kan lagras på samt innehålla olika medium, men vid journaler förda med ADB gäller även datalagen (Socialstyrelsen, 1994). Det är dock samma regler utöver datalagen som gäller för ADB- förda journaler som för manuellt förda journaler. Det är därmed viktigt enligt Socialstyrelsen (1994) att bland annat tänka på följande:

- Det skall framgå vem som tillfört anteckningar etc. till journalen.
- Signering skall upprätthållas på motsvarande sätt som för manuella journaler
- Vi rättelse av tidigare uppgift får inte den felaktiga uppgiften förstöras.
- Oss det behövs skall journalerna kunna ges ut som både kopia och original.
- Behörighetsnivåer för tillgång till journaler ska finnas som tillgodoser patienternas rätt till sekretesskydd och integritet.
- Patientjournalerna skall bevaras, gallras och arkiveras enligt de bestämmelser som finns i patientjournallagen. (socialstyrelsen, 1994)

4.4.3 Sekretesslagen

Sekretesslagen samt sekretessförordningen innehåller enligt Rättsnätet (2006) tillsammans de riktlinjer och bestämmelser för vad som ska hållas hemligt i statens och kommunernas verksamheter. För hälso- och sjukvården gäller huvudregeln i 7kap 1 och 4 § i sekretesslagen av vilken framgår att enskilds persons hälsotillstånd eller andra personliga förhållanden inte får röjas om det inte står klart att den enskilde eller någon honom närstående inte lider, men av det agerandet (Rättsnätet, 2006). I regel har varje svensk medborgare enligt offent-

lighetsprincipen rätt att ta del av de allmänna handlingar som finns hos en myndighet, men i vissa fall är det dock nödvändigt enligt riksdagen att göra inskränkningar i denna rättighet. Detta enligt Rättsnätet (2006) för att skydda enskild persons ekonomiska och personliga förhållanden. De sekretessregler som finns inbegriper både muntliga och skriftliga uppgifter och med sekretess innebär därav att varken muntliga eller skriftliga uppgifter får röjas. Skyldiga att följa sekretess är alla de som arbetar eller deltar i en myndighets verksamhet. Inom hälso- och sjukvården får personal ta del av sekretessbelagda uppgifter i den mån det är nödvändigt för behandling och vård av en patient, det vill säga att personer utan vårdrelation till patient inte får, enligt inre sekretes, ta del av dess uppgifter. Sekretessen gäller även i vissa fall gentemot patienten själv inom hälso- och sjukvården (Rättsnätet, 2006)

4.4.4 Hälso- och sjukvårdslagen

Enligt Socialstyrelsen skall hälso- och sjukvårdslagen se till att en god vård ges till hela befolkningen på lika villkor. Enligt lagen innebär hälso- och sjukvård *"… åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador. Till hälso- och sjukvården hör även sjuktransporter samt att ta hand om avlidna."* (Rättsnätet, 2006 och Regeringskansliet, 2005)

Enligt Regeringskansliet (2005) är några av de viktigaste målen uppsatta inom hälso- och sjukvården och som hälso- och sjukvårdslagen stödjer är:

- Att ge den som har störst behov av hälso- och sjukvård företräde till vård och att ge vården med respekt för alla människors lika värde.
- Att vården som ges skall vara av god kvalitet samt tillgodose patientens behov av trygghet.
- Att vården skall vara lätt tillgänglig.
- Att vården bygger på respekt för patientens integritet och självbestämmande.
- Att främja goda kontakter mellan personal och patient.
- Att arbeta för att förebygga ohälsa.

4.4.5 Personuppgiftslagen

Personuppgiftslagen, PUL, har enligt Riksdagen (2003) skapats för att skydda människor och dess personliga integritet från att kränkas vid behandling av dess personuppgifter. PUL reglerar hur personuppgifter, i synnerhet känsliga sådana får behandlas och lagras i register, databaser etc. Med personuppgifter menas enligt lagen *"all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet".* (Riksdagen, 2003).

Det finns vissa undantag från personuppgiftslagen som enligt Riksdagen (2003) bör beaktas. PUL gäller exempelvis inte då en person helt privat utför behandling av personuppgifter eller då det finns lagar eller förordningar som strider mot PUL. När detta inträffar ska dessa bestämmelser gälla och inte PUL. Exempel på detta är enligt Riksdagen (2003) att bestämmelserna i PUL inte gäller om det strider mot tryck- och yttrandefriheten eller offentlighetsprincipen. PUL kan inte heller hindra myndigheter från att arkivera eller bevara allmänna handlingar. Personuppgifter får i viss mån även sparas för historiska, vetenskapliga eller statistiska ändamål. Vid behandling av personuppgifter måste dock den ansvarige vidta *"… lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas"* (Riksdagen, 2003).

I PUL redogörs vidare krav på hur behandling av personuppgifter skall skötas, vilket skall varas enligt lagen och på ett korrekt och sätt *"… i enlighet med sed"* (Riksdagen, 2003). För behandling av personuppgifter som är känsliga är reglerna stränga och det finns bara vissa undantag. Ett undantag är hälso- och sjukvården där känslig information om den är nödvändig för följande, får lagras (Riksdagen, 2003).*:*

- Förebyggande hälso- och sjukvård
- Medicinska diagnoser
- Vård eller behandling
- Administration av hälso- och sjukvård

PUL påpekar även att personal som omfattas av tystnadsplikten får behandla känslig information som omfattas av just tystnadsplikten (Riksdagen, 2003).

Vid lagrandet av personuppgifter har den personuppgiftsansvarige enligt Riksdagen (2003) en informationsskyldighet. Detta innebär att han/hon har skyldighet att lämna, vid begäran en gång per år, besked om hur personuppgifter gällande den sökande använts. Informationsskyldigheten är dock undantagen vid tystnadsplikt och sekretess (Riksdagen, 2003).

4.5 Attityder till förändringar och spridning av ny teknik

Då en organisation bestämmer sig för att genomföra förändringar, kan detta ibland leda till känslor som rädsla, osäkerhet och upprördhet bland de anställda. Enligt Goldkuhl och Röstlinger (1988) arbetar människor i en verksamhet oftast på rutin och det tas för givet att sådant som sker idag kommer även att ske i framtiden. Rutinerna är inrotade och är så vanliga att de längre inte ifrågasätts och en förändring innebär oftast ett nytt sätt att arbeta på. Då ett förändringsarbete ska genomföras måste dessa nuvarande arbetssätt värderas och detta kan ha en inverkan på människor som är inblandade, både positivt och negativt.

En förändring i en verksamhet innebär enligt Goldkuhl och Röstlinger (1988) vanligtvis att det finns ett problem som bör åtgärdas. Förändringsarbete innebär någon slags omstrukturering i verksamheten och detta kan skapa problem och svårigheter för de inblandade. Enligt författarna kan det ibland skapa mer problem än lösningar, då ett förändringsarbete oftast sker på ett ostrukturerat sätt och kommunikationen inte riktigt når fram till de olika intressenterna. Beroende på hur människor kan se en verksamhet på olika sätt innebär också att de tolkar situationer på olika sätt. Hur förändringsarbetet kommer att uppfattas av exempelvis de anställda beror på hur mycket förståelse och kunskap de har om den särskilda situationen.

Enligt Preece, Sharp and Rogers (2002) känner många människor också en viss osäkerhet inför datorer. Det kan i många sammanhang vara praktiskt att ta reda på datorns arbetssätt, för att på så sätt lättare förstå hur en dator kan underlätta till exempelvis det dagliga arbetet. Ett av de första och fortfarande största användningsområdet med datorer är att administrera stora datamängder och all den data som samlas in i en organisation används som information. Enligt Hallerström (1995) är det viktigt att en organisation hittar applikationer och hjälpmedel som överensstämmer med det egna behovet. Då ständiga förändringar sker kommer ett datasystem som känns bra nu att kännas bristfälligt i framtiden. Det är därför viktigt att omsorg läggs på säkra framtidsbedömningar vid en ny utformning, så att systemet snabbt kan fungera i verksamheten.

Om de applikationer som används i verksamheten är användarvänliga är också en viktig del för att få användarna att trivas med datorer (Preece et al. 2002). Applikationerna bör vara utformade efter vilka som ska använda programmen samt var de kommer användas. Därför bör användarna uppleva att applikationerna är lätta att lära sig samt effektiva för deras arbetsuppgifter. Enligt Arbetslivsinstitutet (2006) är det viktigt att alla användare och andra vederbörande får information och undervisning om bra datoranvändning och hur datorn kan underlätta det dagliga arbetet. Det har, enligt Linthicum (1999 återgiven i Mantanza och Themistocleous, 2005), motiverat hälso- och sjukvården att på senare år söka efter mer avancerade applikationer för att underlätta arbetet för vårdgivarna. Det är sedan själva implementationen av en applikation och hur användarna vill ta till sig den nya informationen som kan leda till problem. Hur olika organisationer kan vinna över dessa problem, då de vill introducera nya applikationer, diskuteras vidare i ämnet diffusionsteori (se 4.5.1).

4.5.1 Spridning av teknik

Diffusion, eller spridning, är enligt Rogers (1995) den process där en innovation eller idé överförs från en person till en annan över ett område. En innovation är en nyhet som kan erbjuda en bättre lösning än det som redan finns, men kan vara svårt att sprida snabbt. På vilket sätt informationen sprids mellan en sändare och mottagare gällande en innovation, är beroende på kommunikationskanalen. Själva spridningsprocessen kan delas upp i två processer, där den ena är beroende av att individen flyttar, medan den andra är beroende av exempelvis massmedia eller individer som redan anammat en innovation. Enligt Rogers (1995) anses massmedians kommunikationskanal vara den mest effektiva att sprida kunskap om innovationer, medan sociala kontakter är effektivast då det handlar om att skapa och förändra attityder gentemot en innovation. En person som bestämt sig för att anamma en innovation kan berätta för två andra personer, som då bestämmer sig för att också anamma innovationen. Dessa två personer diskuterar sedan innovationen med ytterliggare två personer och spridningen är igång.

Rogers (1995) anser att en spridning kan analyseras med hjälp av något som kallas diffusionsteori, då en innovation kan undersökas för att se hur sannolik en spridning är. Diffusion är en särskild typ av kommunikation där meddelandet ämnar en ny idé, men vid brist på information om den nya idén kan detta leda till osäkerhet hos individen. Processen att anamma en innovation är något som Rogers (1995) kallar för ”the innovation-process” och delas in i fyra olika faser.

- Kunskapsstadiet - Här får individen kännedom om att innovationen existerar. Det är lättare att individen får kännedom om en innovation om det finns ett behov av att använda den. Behovet kan skapas av att individen upplever att han saknar något, till exempel ett datorprogram.

- Övertygelsestadiet - Här upplever individen antingen en positiv eller negativ inställning till innovationen. Här är det känslorna som avgör om individen kan ta till sig innovationen eller inte.

- Beslutstadiet - I beslutstadiet tar individen sig tid att komma fram till ett beslut där han antingen bestämmer sig för att anamma eller avfärda innovationen. Här vill oftast individen prova på innovationen för att minska sin osäkerhet.

- Implementationsstadiet - Implementationsstadiet följer oftast direkt efter beslutsstadiet och här bestämmer sig individen för att använda innovationen och då på ett konkret sätt.

Enligt Rogers (1995) anammar inte alla automatiskt en innovation enligt denna process, då varje stadium innehåller ett antal steg som kan påverka beslutet att ta till sig och nyttja en innovation. Olika individer till sig en innovation olika snabbt och det kan också ha betydelse för vilken slags innovation som sprids. Alla innovationer skiljer sig åt, men enligt Rogers (1995) går det att utskilja olika grunddrag hos innovationer som kan påverka farten på spridningen.

- Kompatibilitet: Hur innovationen uppfattas jämfört med tidigare erfarenheter och de behov som finns.
- Komparativa fördelar: Hur innovationen uppfattas bättre än den som kan tänkas kunna efterträda.
- Komplexitet: Hur svår är innovationen att använda eller bilda kunskap om.
- Observerbarhet: Hur påtagliga är resultaten av innovationen för potentiella användare.
- Testmöjlighet: Om en innovation går att få pröva på, tenderar den att anammas snabbare.

Sammanfattningsvis kan innovationer som har låg komplexitet, är observerbara, möjliga att testa, har komparativa fördelar och är kompatibla, spridas snabbare än innovationen som saknar dessa grunddrag.

5 Empiri

I följande kapitel kommer vårt studieobjekt Länssjukhuset Ryhov att beskrivas närmare. Vi kommer även att redovisa resultatet vi fått genom de intervjuer och den enkät som genomfördes på Länssjukhuset Ryhov. För att få en gemensam struktur kommer empirin att redovisas i enlighet med de fyra forskningsfrågorna samt referensramen.

5.1 Länssjukhuset Ryhov

Länssjukhuset Ryhov i Jönköping är ett av Sveriges nyaste sjukhus och där utövas varje dag både planerad och akut specialistvård (Ryhov, 2006a). Sjukhuset har idag 25 basenheter som bland annat består av kliniker, medicinteknisk service samt hjälpmedelscentral. De arbetar dessutom tillsammans med 12 vårdcentraler i de tre kommunerna Jönköping, Habo och Mullsjö. Tillsammans bildar de till Jönköpings sjukvårdsområde, som är en förvaltning inom Landstinget i Jönköpings län. På Länssjukhuset Ryhov arbetar idag cirka 3300 personer och inom primärvården cirka 700 personer.

5.2 Sammanställning av intervjuer

Tillsammans med vår kontaktperson på Länssjukhuset Ryhov togs ett antal respondenter fram till intervjuerna. För att dessa personer skulle hjälpa oss att uppfylla vårt syfte, begränsades respondenterna till inom vilket område på sjukhuset de arbetade. Det bestämdes att intervjuerna skulle utföras på ITC, IT-Planering samt IT-kontaktpersoner runt om på sjukhuset.

ITC ansvar för Landstingets datorer samt nätverk och har monopol på IT-tekniken. Detta innebär att de har hand om bland annat datasäkerhet, utbildning, övervakning samt kundservice inom hela landstinget. IT-Planering finns på Länssjukhuset Ryhov där de ansvarar för planering, policys, säkerhet, etc. På IT-Planering finns en person som är IT-samordnare, men som innehar titeln IT-planeringschef.

Inom landstinget finns det även en IT-samordnare per förvaltning och de har ett övergripande IT-ansvar inom de olika förvaltningarna (Jönköping, Eksjö, Fastighet, Tandvård, Kansliet, med flera). I princip kommer alla uppdrag till ITC från basenheternas IT-samordnare, men förmedlas av IT-Planering. IT-Planering kan även lägga egna uppdrag på ITC. I de olika fastighetsdistrikten (kliniker, vårdcentraler, etc.) finns det även IT-kontaktpersoner som ska kunna lite mer om IT än övriga användare för att hantera vardagssituationer. De ska se till att användarna lär sig använda IT-stöden fullt ut.

Intervjuer har genomförts med nio respondenter inom Jönköpings Läns Landsting. Dessa är fördelade som följer; Två respondenter från ITC, två respondenter från IT-Planering samt fem respondenter ute på klinikerna, det vill säga fem IT-kontaktpersoner. Intervjumaterialet har skrivits samman och redovisas med utgångspunkt från dessa tre grupper. Först kommer intervjuerna från ITC att redovisas, därefter IT-Planering och till sist redovisar vi de fem intervjuerna med IT-kontaktpersonerna. Orsaken till detta är att respondenterna har olika erfarenheter och uppgifter inom organisationen och därför hade det blivit svårt att sammanställa alla tillsammans.

Samtliga intervjuer har utifrån det transkriberade resultatet, vilket finns sparat och kan visas vid behov, omarbetats från talspråk samt skrivits samman med övriga intervjuer inom det, som nämnts ovan, aktuella området. Vi har även sållat i det transkriberade materialet och

uteslutit uttalanden eller ämnen som ej varit aktuella för denna studie. Respondenterna har alla fått tagit del av sina respektive intervjuer och godkänt materialet.

Enkätundersökningen som utförts i samband med studien kommer att redovisas sist, efter intervjuerna. Enkäterna har delats ut till användare inom Länssjukhuset Ryhov, vilket innebär läkare, sjuksköterskor, undersköterskor etc. I kap 5.6 har vi valt att lyfta fram de svarsresultat från enkätundersökningen som vi anser svara på våra forskningsfrågor samt syfte. Dock redovisas alla enkätsvar i bilaga 4 och 5.

5.3 IT- Centrum

Följande intervju är gjort på IT-Centrum (ITC) den 18 april 2006 med Anders Jacobsson, IT-konsult i konsultgruppen, och Jan Svensson, IT-säkerhetsansvarig i Jönköping landsting samt säkerhetshandläggare och personuppgiftsombud.

ITC består av sju delar där produktion, konsult, administration och teknik (Rosenlund, Eksjö, Värnamo och Ryhov) ingår. Sammanlagt har de ca 80 anställda på ITC. ITC har monopol på IT-tekniken i landstinget Jönköping och ansvarar för ca 6000 PC: s och 9000 användare.

5.3.1 Informationssäkerhet

Som det ser ut idag måste samtliga användare först logga in på sitt Novellkonto för att kunna använda sin dator. Därefter måste de även logga in på de olika dataprogrammen som de vill använda för att kunna lösa sina arbetsuppgifter. Enligt Jacobsson skiljer det sig på sjukhuset och primärvården här i Jönköping. Primärvården Jönköping har separata system som är lokala och är uppbyggda av olika databaser och en patient som besöker två olika vårdcentraler blir därför lagrad i två olika databaser. En anledning till att primärvården ligger före med sin dataanvändning jämfört med sjukhuset tror Jacobsson beror på att de är små enheter med ett bestämt sätt hur de jobbar med patienter. Ett sjukhus däremot har flera olika kliniker och det ansågs tidigare vara svårt med ett gemensamt datasystem för alla. Tankarna är i dagsläget att nästa system som ska införas ska ersätta de nuvarande primärvårdssystemen och det ska bli ett gemensamt system mellan primärvård och sjukhus. Enligt Svensson kommer ett pilotsystem för detta snart att testas och fungerar pilotsystemet hoppas ITC att detta kan införas år 2008-2009.

5.3.2 Smarta Kort

Enligt Svensson kommer ITC den närmaste tiden att testa hur smarta kort kan användas för att underlätta arbetet med att identifiera användarna samt signering och kryptering av meddelanden. Kravet kommer från verksamheten där de vill öka säkerheten med dataöverföringar och genom korten ska även en garanti säkras att informationen även kommer får landstinget Jönköping och inte bara från användaren. Detta sker med så kallade mjuka certifikat som ingår i organisationen och genom att använda sig av detta kan landstinget minska risken med till exempelvis förfalskning av recept som skickas till apoteken. För att få erfarenhet kommer ITC under hösten 2006 att testa smarta kort i sin egen verksamhet.

Det smarta kort som ska användas i testet kommer att identifiera användaren på två olika. Dels talar kortet om vem användaren är genom autentisering och det andra är en signerings- och krypteringsdel där det är en applikation verifierar användaren. Kortet kommer däremot i dagsläget inte att lösa den inloggningsprocess som användarna idag måste gå ige-

nom för att använda systemet. Jacobsson anser dock att det finns möjlighet att i framtiden lösa även den här delen. Anledningen till att det inte kommer lösas just nu är för att Landstingets ledning inte ser något behov av detta här i Jönköping och ITC har därför inte fått i uppdrag tittat på några andra användningsområden än att kortet ska identifiera användaren och signera samt kryptera den information som sänds från användaren. De dataöverföringar som kommer att ske över det egna nätverket kommer inte att krypteras, medan det som skickas utanför nätverket ska krypters.

Smarta kort i verksamheten

Enligt Svensson kommer det att finnas två certifikat som ska laddas ner till kortet, så att det kan nyttjas av användaren. Det ena certifikatet ska användas för att tala om vem användaren är på ett säkert sätt och det andra tillåter användaren att sända information krypterat och signerat över systemet. Rättigheterna sen, det vill säga det användaren får göra i systemet, läggs upp i HSA-katalogen och det kommer vara den lokala HSA administrationen som bestämmer vilka rättigheter de olika användarna ska ha. I HSA-katalogen identifierar användaren sig via kortet och sedan får rätt till vissa behörigheter och kortet i sig paketerar en informationsmängd som användaren signerar och krypterar. Smarta kort och HSA-katalogen hänger samman på grund av att användaren måste identifiera sig för att få tillgång till sina rättigheter. Då certifikaten laddas ner, har de en tidsbegränsning på 5 år. Dessa kan enligt Jacobsson ändras beroende på hur länge en användare till exempelvis ska vara anställd på arbetsplatsen. Varje gång ett kort används jämförs det i en återkallningslista, för att försäkra sig om att användaren är en behörig användare. I återkallningslistan kollas det om certifikaten fortfarande är aktiva och den här listan uppdateras flera gånger per dag. Om en användare glömmer sitt kort hemma, kan denne få ett tillfälligt kort, ett så kallat reservkort. Ett reservkort med reservdata kan skapas enkelt för användaren eftersom certifikaten redan är knutna till den specifike användaren. Om kortet däremot skulle vara borttappat eller stulet, får användaren ett reservkort tills ett nytt kort skickats hem till användaren. Det gamla kortet blir då också spärrat.

Det kommer att finnas en viss loggning på korten. Då kan ansvariga titta i den publika delen av certifikatet och ser om just denna användare har de rättigheter att göra vissa utföranden. Idag är loggningen däremot applikationsberoende, det vill säga loggningen sker i varje enskild applikation. Det finns en portal som användaren loggar in sig på för att få tillgång till uppgifter via HSA-katalogen. Här får användaren tillgång till tre delsystem, Patientöversikt (PÖS), labbsystemet och läkemedelssystemet. Dessa tre system hänger ihop och en användare kan bara jobba med en patient i taget. Byter användaren patient i ett av systemet, ändras det också i de andra två. Här kan loggning därför ske i de här tre systemen samtidigt, men i de övriga applikationerna måste loggningen ske separat. Ett smart kort löser däremot inte detta i dagsläget på Länssjukhuset Ryhov, men i framtiden kan det göra det.

Den typen av smart kort som valts till användning i dagsläget innehåller tre magnetspår, där ett spår kan programmeras av ITC själva. Även om det inte är aktuellt i dagsläget, så anser ändå ITC att det slutliga målet är att använda smarta kort som en del av inloggningsprocessen, passerkort, och ID-kort. ITC har märkt att det finns ett behov ute på klinikerna för detta, men det är ändå upp till ledningen att ta detta beslut. Det är en stor omstrukturering som måste ske för att få detta att fungera och detta kommer att ta mycket lång tid då infrastrukturen och personal får nya arbetsuppgifter.

Detta är ett stort förändringsarbete och det kommer att ta sin tid på grund av olika satsningar och lagar som måste ändras. Gällande den Nationella IT-strategin så tar den IT i

sjukvården i rätt riktning, men även där kommer det att ta tid innan alla beslut är tagna. Bra att ändå ha den i bakhuvudet och följa den, så att ändringar slipper göras senare.

5.3.3 Mobilitet

ITC anser att det idag inte finns någon direkt mobilitet för användarna att röra sig mellan de olika arbetsplatserna inom Landstinget. Enligt Svensson går det att få bättre mobilitet, men det behöver inte lösas med ett smart kort, utan räcker med en personlig profil för användaren. Det som blir säkrare med smarta kort är att användaren måste identifiera sig på ett säkert sätt.

5.3.4 E-journaler

Den Nationella IT-strategin diskuterar också om möjligheten för patienterna att bära runt sin information på smarta kort och detta är något som ITC haft uppe i diskussion för några år sedan. Dock ansågs dessa kostnader bli alltför stora och idén lades på is. Dessutom är smarta kort just nu enligt ITC bra bärare till textfiler, men inte till att förvara exempelvis röntgenfilmer på då korten skulle behöva ha stora minnesutrymmen för detta.

Enligt de lagar som gäller idag för sekretess, patienter, PUL, etc., får en patient inte titta i sin egen journal, men kan däremot få tillstånd att se vissa delar. Enligt Jacobsson säger dock datainspektionen en sak, medan socialstyrelsen och patentlagen en annan. Lagarna står helt enkelt mot varandra och just nu pågår det aktivt hur detta ska lösas. Det handlar också om vem det är som ska läsa journalen. Är det patienten själv som går in som privatperson är det vissa regler som gäller, medan en person som arbetar i vården har andra skyldigheter och lagar.

Som det ser ut idag är det landstinget som myndighet som har ansvaret för journaler. Som privatperson kan du kräva att få se vissa delar ur din journal, men det är landstinget som då ansvarar för detta. Enligt Svensson har patienten rätt att ta del av sin journal efter en så kallad menprövning, det vill säga en läkare skall se att det inte är skadligt för patienten att se sin journal. En patient har i normalfallet en mycket stark rätt att få ta del av allt det material som finns i hans journal. Enda undantaget från denna huvudregel gäller uppgifter om hälsotillståndet, som får undanhållas patienten ”om det med hänsyn till ändamålet med vården eller behandlingen är av synnerlig vikt att uppgifter inte lämnas till honom”. Skyldigheten ligger normalt på ansvarig läkare att bedöma om medicinskt motiverat hinder föreligger. Om patienten ska få möjlighet att titta i sin journal via till exempelvis en patientportal, måste detta ske via en säker förbindelse. Östergötland är ett län som har ett försök med en patientportal, där vissa patienter kan få tillgång att titta på vissa delar ur sin journal.

Enligt Jacobsson är det viktigt med samtycket gällande vad som får lämnas ut vid en elektronisk journal (e-journal) och inte lämnas ut. I dagsläget pågår det en test mellan Östergötland, Uppsala, Norrbotten och Jönköping om en nationell patientöversikt. Innan kunde landstinget inte gå in och titta i varandras patientjournaler, men idag finns det möjlighet att titta, men inte ändra eller skriva till något. ITC anser att det måste ske en ändring i lagen för att få e-journaler att fungera över landstinggränserna. Patienten måste själv lämna sitt samtycke och sedan styr sekretesslagen vad som får lämnas ut mellan myndigheter.

5.3.5 Attityder till förändringar

ITC anser att användarna är osäkra vid förändringar och då speciellt de datoriserade som införs. Användarna är rädda att göra misstag som de kan bli anmälda för. Det är därför viktigt att verksamhetscheferna ger rätt information och utbildning. Ledningen har också centralt ett ansvar, men den juridiska biten är det verksamhetscheferna som ansvarar för.

5.4 IT- Planering

Följande intervju genomfördes på IT-Planering den 11 april 2006 med Jan Günther-Hanssen, IT-planeringschef, och Inger Offenbacher, informationssäkerhets handläggare.

Günther-Hanssen är IT-planeringschef och ansvarar för en grupp av medarbetare där de arbetar med verksamhetsutveckling genom att stödja införandet och användandet av IT-stöd i vården. IT-Planering arbetar också med att utbilda personalen och kan ses som konsulter åt de olika enheterna och klinikerna som finns på sjukhuset.

5.4.1 Informationssäkerhet

IT-Planering tror att den dåliga prioriteringen av IT-säkerhet inom hälso- och sjukvården beror på att det inte funnits så mycket kunskap inom Landstingen. Enligt Offenbacher kan det bero på att Landstinget inte är någon vinstdrivande verksamhet och därför blivit dåligt prioriterade på utvecklingsfronten. I den privata sektorn kan de satsa på IT-system som kan bli rena investeringar, medan inom hälso- och sjukvård kan det rationellt sett bli effektivisering av organisationen, exempelvis operera fler människor, men det kommer istället att kosta mer pengar, då varje operation är dyr. Ett annat problem som har uppstått är att det har lagts gamla rutiner på ny teknik istället för att få in nya rutiner som ska göra det enklare.

Günther-Hanssen tror att den dåliga prioriteringen också beror på att regeringen har velat ge självstyre till landsting, regioner och kommuner och att då varje landsting har fått frihet att själva ta fram sina egna IT-lösningar. Detta har enligt Günther-Hanssen blivit fel från början. Sverige är ett litet land och har samma regler och lagar som måste följas i alla landsting. Det finns även internationella regler att följa, så eftersom Sverige har en homogen struktur borde det ha gett en större samordning på nationell nivå.

Som tidigare nämnt måste samtliga användarna på Länssjukhuset Ryhov idag logga in på ett novellkonto som ligger som bas för att de ska kunna komma åt de olika applikationerna. För att sedan använda applikationerna behöver användarna logga in med nya lösenord, medan användarnamnen är desamma. Enligt Offenbacher är nackdelen med dessa inloggningar att det är tekniskt krångligt för användarna, vilket kan medföra en säkerhetsrisk då flertalet skriver ner sina lösenord på papperslappar. Enligt Günther-Hanssen varierar dessutom antalet datorer. På vissa kliniker har de datorer till samtliga användare, medan andra kliniker har tillgång till tre datorer på 20 anställda. Detta är ett problem som sjukhuset känner till och de behöver skapa en mer effektiv inloggningslösning.

Enligt Offenbacher går de inte att blunda för det faktum att det på vissa kliniker är så att den användare som kommer på morgonen loggar in och sedan står datorn öppen hela dagen för vem som helst att använda. Detta är något som försöks minimeras med gruppinloggningarna, då användarna inte ska behöva logga ut ur hela systemet utan det räcker med att de loggar ut ur applikationen som använts. Detta hjälper också till att behålla spårbarheten.

Enligt Offenbacher måste IT-säkerheten inom Landstinget förbättras snarast och ett sätt skulle vara att börja förenkla de besvärligaste delarna med ett smart kort i centrum. Då skulle användarna kunna logga in på sin egen profil med ett inlogg, vilket är tidsbesparande. Korten skulle användas för en säker verifiering av den anställde.

Sekretess
Användarna ska, enligt Offenbacher, vara medvetna om vilka regler som gäller, då de hantera känslig information. Vi tror gärna att så är fallet, men har kunnat konstatera att de anställda inte är medvetna om alla regler och lagar som existerar. IT-Planering är ofta ute och informerar samt utbildar personal, men som nämndes räcker inte alltid detta. Günther-Hanssen tror att detta kan ha att göra med hur mycket var och en kan ta till sig. Det kan också bero på vem som är säkerhetshandläggare, men detta är något som de på IT-Planering börjar bli bättre på. Informationssäkerhet kan vara lite av ett nödvändigt ont för många och de kan säkert tycka att det känns lite polisiärt. Användarna kan dock hålla sig uppdaterade med information om säkerhet på Intranätet samt genom de IT-kontaktpersoner som finns runt om på klinikerna.

Det är verksamhetschefen som har det yttersta ansvaret för den sekretessbelagda informationen som finns inom dennes område, men ansvaret varierar beroende på ”hur mycket ansvar som vågas ta”. Det är ändå viktigt att den anställde känner att de har förtroende från Landstinget.

Loggning
Fördel med den nuvarande inloggningsprocessen är, enligt Offenbacher, att det finns en spårbarhet, så att det går att följa upp vart användarna har varit inloggade och vad de har gjort och inte gjort. I dagsläget finns det ett påbörjat ett projekt relaterat till detta. IT-Planering har blivit uttagen att arbeta med den landstingsövergripande logghanteringen för där är Länssjukhuset Ryhov inte så bra i dag. IT-Planering vill att det ska komma ut till verksamheten att de själva ska kunna arbeta med det här mot sina anställda. Loggarna ska kontinuerligt kontrolleras för då kan de lättare läsas av och upptäcka om det är något fel. Det kan även göras stickprovskontroller. Som det ser ut idag måste det läggas in en beställning och begära utdrag om loggning och ju mer teknik som kommer in i verksamheten, desto viktigare är det med logghantering.

Enligt Offenbacher räcker det att titta på Anna Lind situationen för att förstå vikten av loggning. Günther-Hanssen anser att det är förvånansvärt få anställda som vet om att de inte får läsa sina egna journaler och det varierar i hur mycket de anställda vet om de rättsliga åtgärder som kan drabba dem. Detta har inte bara att göra med datoriseringen utan också tillgängligheten. Att det är tillgängligt gör det svårt att se vart gränsen går, då vissa saker är klara och andra saker svårare att förstå. Inom detta område finns det fortfarande mycket att arbeta med och det är en otydlighet från landstingsledningen. IT-Planering anser att det borde finnas ännu tydliga riktlinjer och direktiv, men ännu har inget hänt. I dagsläget finns det policys utlagda på intranätet och dessa kan anställda klara sig långt med.

5.4.2 Smarta Kort

Günther-Hanssen anser att smarta kort kan förbättra IT-säkerheten inom Landstinget i Jönköping. Det vore idealiskt att bära runt informationen om sig själv och kunna verifiera att jag är jag. Inloggnings- och utloggningsprocessen skulle också kunna lösas med ett smart kort, samt få ökad mobiliteten och användas som passerkort för att verifiera en anställds identitet. Det kan även bli en bättre struktur i behörighetsträdet med ett smart kort.

Enligt Offenbacher skulle det bästa vara om patienten också fick bära runt sin information på ett smart kort och själv ge sitt samtycke till vem som ska få läsa journalen. Då skulle behandlingar kunna ske snabbare samt även fungera att patienter besöker olika sjukhus. Offenbacher tror också att projektet SITHS är en viktig del i framtiden, då det kan hjälpa olika Landstingen i Sverige att bli enade på en nationell nivå.

5.4.3 Mobilitet

Günther-Hanssen anser att prestandan på systemet idag inte fungerar så bra, vilket gör att det tar lång tid för användarna att både logga in och ut. Att de är mer mobila i vården och behöver göra en sak på en dator och sedan förflytta sig och fortsätta på en annan dator påverkas mycket av detta. Det tar tid att logga in och ur och enligt Günther-Hanssen är just inloggningsprocessen det största användarproblemet och det uppstår frustration då användarna inte kommer åt systemen. Det varierar dessutom mellan kliniker, då vissa behöver vara mer mobila, använda många applikationer och ha tillgång till Internet mer än andra. På vissa ställen är detta löst med så kallade gruppinloggningar, vilket innebär en gemensam inloggning för hela kliniken. Dock behöver varje enskild anställd ändå logga in på de applikationer de sedan vill använda med sina personliga inloggningsuppgifter, vilket inte underlättar så mycket för mobiliteten.

5.4.4 E-journaler

Anställda har idag lättare att läsa patientjournaler, då ledningen har fattat beslut om att hela landstiget är ett så kallat läsrättsområde. I patientöversikten (PÖS) kan den anställde läsa vilken information som helst om alla patienter i landstiget, men det går inte att lägga till information. PÖS används för att exempelvis läkare och sjuksköterskor ska kunna hjälpa patienter snabbare med hjälp av den information som finns sparad om patienten. Den anställde måste dock fortfarande ha vårdrelation till patienten för att få läsa i PÖS.

Günther-Hanssen anser att pappersjournaler kan vara svårare att läsa till skillnad från e-journaler eftersom den anställde då måste gå till ett arkiv och hämta ut dem. Dock går det inte att spåra vilka som har läst en pappersjournal som det går att göra med en datoriserad journal. På Länssjukhuset Ryhov finns det fortfarande pappersjournaler, men i dagsläget håller dessa på att bli inskannade för att de ska kunna bli lästa över PÖS. Vårdcentralerna däremot har använt sig av datoriserade journaler i flera år som kan läsas i PÖS i hela landstinget. Enligt Offenbacher är det värdefullt att komma åt information snabbt och e-journaler öka tillgängligheten och översikten på ett positivt sätt. En nackdel med e-journaler är dock att informationen exponeras på ett nytt sätt och det kan innebära en större risk att någon obehörig kommer åt informationen om en patient.

5.4.5 Attityder till förändringar

När det gäller förändringsarbete i verksamheten tror Offenbacher inte att informationen ska komma ut för tidigt till anställda. Bättre att berätta om förändringar då det finns något konkret att säga och få de anställda att känna sig delaktiga. Enligt Günther-Hanssen skiljer det sig mycket på attityderna mellan användarna. Rent generellt så är medelåldern inom landstinget ganska hög, ca 48 år, vilket innebär att datorvanan bland anställda kan skilja sig. Det ska dock påpekas att det inte bara är äldre användare som har problem med datoranvändningen. På IT-Planering jobbas det mycket med utbildning och det ges även en grundutbildning i datoranvändning när personal nyanställs. När det förs in ett nytt IT-stöd eller nya användare tillkommer så ser vi till att användarna får ytterliggare utbildning. Först be-

hövs en grundkompetens, vilken kan vara svår att avväga i omfattning, då olika människor har olika lätt att ta till sig information. IT-planering undersöker bland annat via enkäter hur datormognaden ser ut, det vill säga vad som krävs i utbildningsväg. Günther-Hanssen anser dock att de håller en bra nivå på utbildningarna, då det är deras ansvar att se till att användarna har den kunskap de behöver gällande IT för att kunna lösa sina arbetsuppgifter.

5.5 IT- Kontaktpersoner

Nedan är en sammanställning av de intervjuer som genomfördes med IT-kontaktpersonerna på fem olika kliniker på Länssjukhuset Ryhov i Jönköping. IT-kontaktpersonerna som intervjuats arbetar på följande kliniker: Ambulansenheten 2006-04-25, Medicinkliniken 2006-04-21, Radiologen 2006-05-09, Rehabiliteringsmedicinska kliniken, samt 2006-04-26, Ögonkliniken 2006-05-09. Nedan följer en kort beskrivning av hur arbetet på de olika klinikerna gällande datoranvändning ser ut.

Ambulansenheten
Ambulansenheten för idag datoriserade journaler i ambulanserna. I det dagliga arbetet med datorer för ambulanspersonalen så ingår det att logga in sig när de kommer till arbetet och tala om vilken bil de kör. Sedan kommer deras uppdrag in i systemet från SOS, vilket i sin tur genererar en patientjournal med ärendets typ, uppdragsnummer, tider etc. De är ålagda att föra dokumentationer på samtliga vård åtgärder de utför. Sedan är det en del knapptryckningar i bilen då de för in vilken tid de är framme på platsen, när de lämnar platsen samt vilka åtgärder och aktiviteter de utför. Även en bedömningskod på patienten registreras i journalen. I dagsläget kan dock ej journalen i ambulansen överföras till akutmottagningen.

Medicinkliniken
Medicinkliniken använder sig idag fortfarande mest av pappersjournaler, då det inte finns godkännande för digital lagring i något av deras huvud system än. Däremot används PÖS.

Radiologen
Radiologen har egna helt datoriserade röntgenjournaler. Övrigt arbete på kliniken är också datoriserat förutom remissen som så småningom kommer att bli digital även den. De skickar även ut alla röntgenbilder till en webbportal till remitenterna. En ortoped kan exempelvis gå in och titta på bilder bara två minuter efter det att de har tagit dem. Även primärvårdsläkare och alla som har behörigheten inom landstinget har tillgång till dessa. De skickar även bilder teleradiologiskt mellan olika sjukhus om de får en begäran på detta.

Rehabiliteringsmedicinska kliniken
Rehabiliteringsmedicinska kliniken är helt datoriserade och använder därmed e-journaler. Kliniken arbetar med Rehabiliteringsprocessen för en patient och fastän kliniken består av fyra olika enheter arbetar personalen tvärs över organisationen och följer patienten i processen. Därmed är IT-stöden väldigt viktiga på kliniken för att underlätta kommunikation och samordning.

Ögonkliniken
Ögonkliniken har idag fortfarande bara pappersjournaler, men de arbetsredskap som de använder i det dagliga arbetet är mycket teknikorienterade.

5.5.1 Informationssäkerhet

En viktig del i att förbättra och bibehålla informationssäkerheten på sjukhuset är, enligt Ögonkliniken, Ambulansenheten samt Rehabiliteringsmedicinska kliniken, att informera och påminna anställda med jämna mellanrum, då information är en färskvara. Klinikerna menar att personalen är väl informerade om informationssäkerheten i allmänhet, men påpekar att det i slutändan är de anställdas ansvar att följa de regler och riktlinjer som gäller. Det är många lagar och riktlinjer inom sjukvården som måste följas så som; patientjournallagen, lagen om personuppgiftslagen (PUL), läkemedelslagen (förordningen), sekretesslagen, etc. Detta tillsammans med det komplexa informationsflödet inom vården med kontakter mellan kommunen, vårdcentraler, privata kliniker och i flödet ingår patienter, personal gör att enligt Medicinkliniken att det inte är helt lätt att uppnå en bra säkerhet. Radiologen har haft problem med sin informationssäkerhet, då deras system ibland legat nere eller inte uppfyllt alla säkerhetskrav, men har då tillfört manuella säkerhetskontroller och utfört riskanalyser.

Samtliga kliniker använder sig idag av datorer i sitt dagliga arbeta men i olika hög grad. Klinikerna innehar arbetsredskap som är datoriserade och de skulle idag inte klara sig utan datorer i sitt arbete, då de anser att IT-stöden är oerhört viktiga för utförandet av deras arbete. Samtliga kliniker ser datorn som ett mycket bra arbetsredskap och Radiologen menar att trots problem som finns så vill de inte tillbaka till en icke datoriserad värld, då det inte skulle fungera med dagens arbetsbörda samt att kvaliteten på arbetet, röntgenbilder och diagnoser till följd av detta skulle bli sämre.

Det finns dock problem med datoranvändningen idag på samtliga kliniker. Enligt Radiologen, Medicinkliniken samt Ögonkliniken är slöa, långsamma system och nätverk ett av problemen. Det tar, enligt dem, alldeles för lång tid att starta upp datorn, logga in eller utföra aktiviteter på datorn eller via nätet.

Driftsäkerheten ett ytterligare ett problem idag, då systemen inte är 100 procentiga och de kan inte lita på att systemen fungerar 24 timmar per dygn. Det är, enligt Radiologen, viktigt att de har tillgång till informationen när de behöver den. Medicinkliniken håller med och menar att driftstopp har hänt ett flertal gånger, vilket inte är bra trots att det finns reservsystem och backup.

IT-tekniken ute på vårdklinikerna är också en brist, då inte alla har tillgång till exempelvis samma system. Det uppstår problem främst gällande kommunikation, då de inte har kommit lika långt i datoriseringen och som sagt att olika system används. Radiologen som i stort sätt är helt datoriserade precis som Rehabiliteringsmedicinska kliniken upplever problem, då de behöver skicka eller ta emot information i pappersform som därmed måste omvandlas till digital information. Radiologen menar att på grund av att alla inte har tillgång till systemet leder detta bland annat till förlängda svarstider. Ambulansenheten anser att mycket av effektiviteten försvinner då system inte kan kommunicera med varandra och anser att det i slutändan är patienten som blir lidande, då viktig tid tas till att fråga ut patienten varje gång den kommer till en ny klinik, skapa en ny journal, etc. Detta leder till att det uppstår svårigheter med att hantera flödet av patienten, speciellt då patienten och personalen inte alltid befinner sig på en enhet.

Ögonkliniken påpekar vikten av att samla ihop den idag spridda informationen så att den går att nå enkelt. De flesta patienter förväntar sig att anställda inom vården kommunicerar med varandra, speciellt inom ett och samma sjukhus. Samtliga kliniker anser också att gemensamma system som kan kommunicera och dela information är en förutsättning i framtiden. Radiologen anser att en bidragande orsak till de olika system som finns idag är att

varje klinik kan välja egen leverantör, vilket bidrar till att system utan möjlighet till kommunikation skapas. Därmed bör detta ändras i framtiden och regleras mer centralt. Det är viktigt att ta reda på vad verksamheten behöver, men även ha den tekniska kunskapen. Detta har dock förbättras något då kontaktpersoner som både har IT-utbildning samt arbetar i vården finns idag. Säkerheten är något som alltid kan förbättras enligt Medicinkliniken och Ambulansenheten och det är viktigt att fortsätta informera och utbilda de anställda. Medicinkliniken samt Rehabiliteringsmedicinska kliniken anser att det vid förändringar i framtiden är viktigt att gamla rutiner inte lever kvar för saks skull utan att de anpassas så att det stämmer överens med den nya tekniken.

Ambulansenheten anser att det är bra med gemensamma standarder så de vet vilka krav de ska ställa mot leverantörerna samt för att underlätta kommunikationen. Rehabiliteringsmedicinska kliniken tror dock det kan bli svårt att enas men tror ändå att viss styrning är att föredra.

Loggning
Samtliga kliniker anser att loggning är bra och nödvändigt på en arbetsmiljö som sjukhuset, då loggningen ökar säkerheten framförallt för patienten. Det är viktigt att det loggas för att bibehålla integriteten hos patienten. Medicinkliniken samt Rehabiliteringsmedicinska kliniken trycker på att det är bättre att ge folk ansvar och större frihet och istället logga det som görs i systemen. Klinikerna menar att de anställd ska vara medvetna om att allt de gör loggas och är synligt. Problemet idag menar Rehabiliteringsmedicinska kliniken och Radiologen är dock att loggen inte gås igenom som den ska och det borde vara enklare. De vill få en bättre struktur på loggen så att de verkligen följer den.

Autentisering
Inloggningsprocessen är något samtliga intervjuade kliniker vill förändra, då detta är krångligt. De är alla överens om att inloggningen måste bli enklare och snabbare, men fortfarande vara säker. Ambulansenheten däremot använder gruppinloggning, då de har få datorer och det annars skulle ta alldeles för lång tid att för dem logga in först i huvudsystemet och sedan i journalsystem. De övriga klinikerna anser att inloggningsförfarandet är krångligt och tar alldeles för lång tid. Ingen av klinikerna ser någon fördel med dagens inloggningsprocess, men Rehabiliteringsmedicinska kliniken förstår att anledningen från början är säkerheten. Även Radiologen och Ambulansenheten nämner att det är mellan åtta och tio system som de behöver logga in på och komma ihåg lösenord till. Det uppstår även problem och datastrul, enligt Ögonkliniken, vid byte av lösenord till samtliga system som ska göras med jämna mellanrum. ITC och IT-Planering arbetar, enligt Medicinkliniken, med att de ska få vårdgivarprofiler, vilket leder till en gemensam första inloggning och som skulle underlätta processen något. Ögonkliniken anser dock att en gruppinloggning inte skulle underlätta för dem då det inte passar deras sätt att arbeta på kliniken.

Ögonkliniken anser att de legitimationshandlingar i form av elektroniska kort som de använder idag även skulle kunna användas vid inloggningen. Även Medicinkliniken nämner kort och mer specifikt smarta kort som det optimala sättet för inloggning. De vill ha en ”smart card inloggning” där de kommer åt samtliga system efter en inloggning. Genom att förbättra inloggningsprocessen kommer även loggningen att förbättras.

5.5.2 Mobilitet

Samtliga kliniker har anställda som rör sig mellan klinikerna. På Ögonkliniken har anställda ett rullande schema där de roterar mellan mottagningen, vårdkliniken, operation samt grå-starrenheten. Rehabiliteringsmedicinska kliniken och Medicinkliniken har ibland läkare ute

på andra kliniker har inte möjlighet att komma åt sina journaler eller sin information från andra kliniker. Medicinkliniken menar att mobiliteten är viktig, men att åtkomsten är varierande och att det beror på vilka system som används. Första gången de kommer till en ny klinik måste deras profil installeras på nytt, vilket tar tid och ofta krånglar. Om det handlar om ett nytt system måste den anställde få tillgång till inloggningsuppgifter vilka beställs från ITC. Detta är, enligt Medicinkliniken, alldeles för långsamt och under den tiden arbetar personen i fråga utan egna inloggningsuppgifter, vilket inte är bra beroende på loggning.

Även mobiliteten inom klinikerna är ett problem. Både Medicinkliniken och Radiologen menar att läkare som går ronder är de som drabbas mest, då det är för att de inte har tillgång till bärbara datorer och därför inte kommer åt den information de behöver medan Medicinkliniken menar att bärbara datorer inte har löst problemet, då de inte har tillgång till journaler, vilket ses som känslig information, via de bärbara datorerna. Därmed måste läkare logga in och ut flertalet gånger på de stationära datorerna för att komma åt aktuell information.

5.5.3 E-journaler

Radiologen, Rehabiliteringsmedicinska kliniken samt Ambulansenheten använder sig idag av e-journaler i sitt arbete och även användandet av PÖS varierar mellan klinikerna. Medicinkliniken använder PÖS frekvent medan Radiologen använder PÖS för att få uppgifter om labbsvar. Ambulansenheten i sin tur använder inte PÖS alls, då de har sitt eget journalsystem. Vare sig klinikerna använder sig av PÖS idag eller inte så ser de fördelarna med den och menar att det är en mycket bra början, men den behöver spridas, innehålla mer information och deras önskemål är att de i slutändan får en ren e-journal. Samtliga kliniker anser att e-journaler är en förutsättning och nödvändiga i framtiden.

Problemet med pappersjournaler är att de skapas en ny journal på varje ny klinik patienten kommer till. Rehabiliteringsmedicinska kliniken säger att innan införandet av e-journaler hade de åtta olika pappersjournaler bara inom kliniken. Detta ledde till att de olika klinikerna inte läste varandras journaler samt att samma information dokumenterades på ett flertal olika ställen.

Att få tillgång till e-journaler kommer enligt Radiologen, Rehabiliteringsmedicinska kliniken samt Ambulansenheten att leda till bättre vård för patienterna, då vårdgivaren får tillgång till samtlig information om patienten oberoende av vilken klinik de varit på innan. Tillgängligheten kommer också, enligt Medicinkliniken, vara en av de största fördelarna med införandet av e-journaler. Ambulansenheten anser att omhändertagandet av patienten kommer att förbättras och effektiviseras genom att de med hjälp av e-journaler kommer att kunna skicka över journalen till akutmottagningen och således ge akutmottagningen möjlighet att på förhand sätta sig in i situationen bättre samt förbereda ankomsten.

Ingen av klinikerna ser några större risker med införandet av e-journaler utan menar att den tekniken som finns (dock inte på sjukhuset idag) är tillförlitlig. Det är dock viktigt, enligt Rehabiliteringsmedicinska kliniken, att informationen är på sin rätta, då det inte bör finnas massa papperskopior liggande överallt som ändå kan läsas utan. Sammanfattningsvis är samtliga kliniker positiva till e-journaler och ser det som en nödvändighet i framtiden som kommer att förbättra deras arbete.

Samtliga kliniker anser att den Nationella IT-strategins tanke om en gemensam plattform är mycket tilltalande. Klinikerna ser behovet av en gemensam information och journalsystem då patienter idag blivit mer mobila. En positiv aspekt med en nationell plattform är enligt

Ögonkliniken att system kan ändras/byggas om utan att de påverkar andra system och de kommunicerar sedan genom plattformen.

Det är dock av stor vikt, enligt Rehabiliteringsmedicinska kliniken och Radiologen att patientens integritet skyddas och att säkerheten kring den nationella plattformen och informationsutbytet är tillräckligt. Radiologen anser att viss känslig information kanske inte ska finnas tillgänglig nationellt och Rehabiliteringsmedicinska kliniken tillägger att det är en viktig diskussion om vilken information vi ska kunna ta del av och inte, men det måste i de flesta fall vara till nytta för patienten att synliggöra vilka problem/sjukdomar de tidigare haft och därmed kanske underlätta diagnoser och behandling.

Det är blandade känslor gällande den Nationella IT-strategins förslag av användandet av smarta kort. Medicinkliniken och Ögonkliniken anser att smarta kort är mycket bra, medan Rehabiliteringsmedicinska kliniken och Ambulansenheten menar att det skulle vara lätt att tappa ett sådant kort samt svårigheter kan uppstå när de ska se till att alla i Sverige ska får ett sådant kort. Den fördel som Rehabiliteringsmedicinska kliniken kan se är att informationen då följer patienten genom hela vårdkedjan. Medicinkliniken anser också att patienternas krav idag är högre än tidigare och att de vill ha tillgång till sin egen information.

5.5.4 Attityder till förändringar

Radiologen, Ambulansenheten samt Ögonkliniken anser att kommunikationen med IT-Planering har fungerat bra och att de fått gensvar på problem och önskemål. Dock menar både Ögonkliniken och Rehabiliteringsmedicinska kliniken att IT inom sjukhuset och landstinget är en trög och ”knölig” process. Rehabiliteringsmedicinska kliniken anser att de inte får besluta så mycket själva utan det mesta styrs uppifrån och de blir ofta tilldelade system att arbetar med som egentligen inte är bra och de egentligen vet att det finns bättre och effektivare system för att stödja deras arbete.

Rehabiliteringsmedicinska kliniken tillägger att det är viktigt att Landstinget tar hänsyn till varje kliniks specifika behov och menar att de kan skapa ramverket, men sedan måste klinikerna själva få hjälpa till att fylla upp det och beskriva vilka behov de har.

På flertalet kliniker har stora förändringar skett de senaste åren och det har till och från varit jobbigt för de anställda med all förändring. De största förändringarna har varit datarelaterade och Rehabiliteringsmedicinska kliniken menar att det fanns en oerhörd rädsla bland de anställda vid och innan införandet av e-journaler, men när de ”kom över tröskeln” och de kunde se nyttan med förändringen så har de blivit mer öppna för förändringar i allmänhet.

Samtliga kliniker bedriver säkerhetsutbildning och utbildning av de nya systemen själva eller med hjälp av IT-Planering. Radiologen, Medicinkliniken samt Ögonkliniken anser att de har bra utbildning i informationssäkerhet. Radiologen och Medicinkliniken har fått väldigt mycket utbildning och Ögonkliniken har ett ganska omfattande introduktionsprogram, men de menar precis som de övriga klinikerna att det alltid kan bli bättre. Enligt Rehabiliteringsmedicinska kliniken är det svårt att veta om utbildningen är tillräcklig och de försöker informera så mycket som möjligt, men precis som Ögonkliniken menar de att vi är enskilda individer och för vissa är det tillräckligt med information medan andra behöver mer utbildning och förevisning. Information är dessutom färskvara som behöver uppdateras, läras ut på nytt och påminnas om.

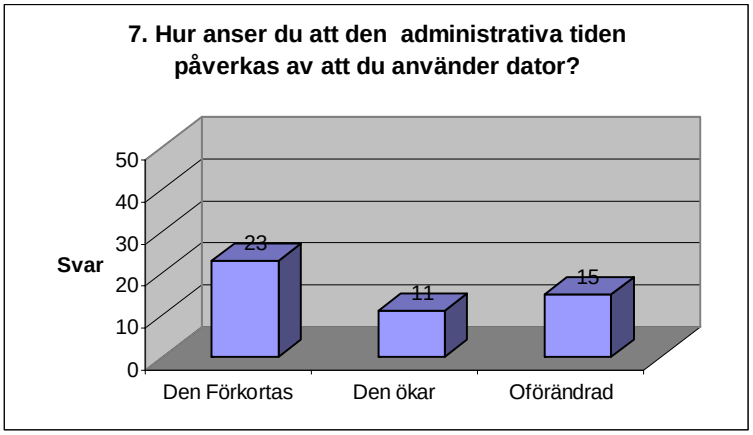
Ett av de största problemen vid förändringar har varit bristfälligheten i systemen. Det har enligt Medicinkliniken, Ambulansenheten samt Radiologen uppstått driftstopp, buggar och andra fel som påverkat de anställdas attityder negativt. När detta blivit åtgärdat har således också attityden blivit positivare. För att förhindra oro vid förändring menar klinikerna att information och utbildning är viktigt. Rehabiliteringsmedicinska kliniken tillägger att desto mer delaktiga de anställda är i förändringsarbetet desto enklare blir det att genomföra och för dem att acceptera.

5.6 Användarna

Från början ville vi att enkäten skulle delas ut både på sjukhuset och inom primärvården, men tyvärr fick vår kontaktperson inget gensvar från någon av de IT-kontaktpersoner som finns på de olika vårdcentralerna. Istället delades sammanlagt 50 enkäter ut på de fem olika klinikerna vid Länssjukhuset Ryhov som vi tidigare intervjuat. Vi fick tillbaka alla enkäter med svar och slapp därför eventuella bortfall. Enkäterna kommer dock redovisas tillsammans, då vi inte bett respondenterna att redovisa var på sjukhuset de arbetar, detta för att behålla anonymiteten.

5.6.1 Informationssäkerhet

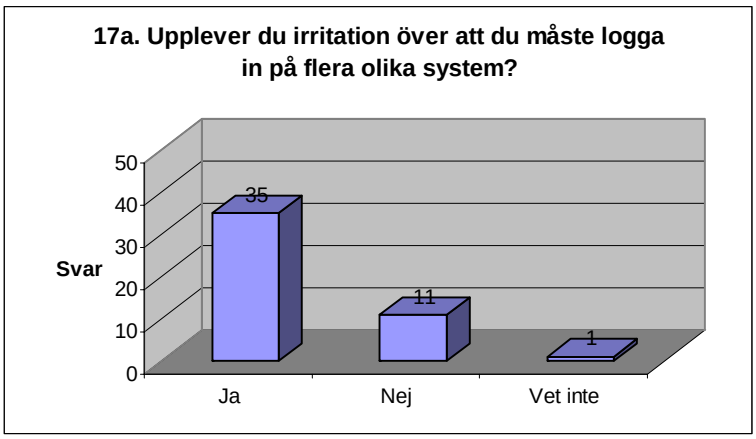
Av de 50 personer som deltog i enkäten (se Bilaga 4 och 5), så var det 14 män och 36 kvinnor och majoriteten i de båda grupperna var över 40 år. Hur länge de jobbat på sina respektive arbetsplatser var dock spritt mellan de olika tidsalternativ som fanns att välja på. 48 anställda använder datorn i det dagliga arbete och majoritet av dessa anser att datorn hjälper dem att lösa uppgifterna på ett bra sätt (se Figur 5-6-1). 23 anställda anser dessutom att datorn förkortar den administrativa tiden och av dessa är majoriteten över 40 år. Ett par anställda tycker det inte känns bra att lagra information elektroniskt, då systemet anses vara för sårbart. De menar att systemet inte är tillförlitligt och fungerar bara lite då och då. Det är också få personer som använder datorn till att söka annan information som kan hjälpa dem vid diagnosställningar.



Figur 5-6-1 Påverkning av den adminstrativa tiden

42 personer betraktar att det nuvarande datasystem som finns på Länssjukhuset Ryhov tillräckligt säkert för att skydda känslig information från obehöriga. Dock anser många att dagens inloggningsprocess är krånglig. Det anses vara för många inloggningar med olika lö-

senord för att komma åt olika applikationen. Systemet är dessutom långsamt och de anställda arbetar inte vid samma dator hela tiden. Majoritet loggar in på fler än en dator per dag och upplever irritation (se Figur 5-6-2) över att dessutom behöva logga in på varje applikation som ska användas.



Figur 5-6-2 Inloggning på flera olika system

Hälften av de tillfrågade väljer att inte logga av datorn när den lämna obevakad, eftersom detta bland annat tar för lång tid. Anställda känner att de inte hinner logga av eller så glöms det helt enkelt bort. På vissa kliniker används oftast en dator av två personer och skulle båda hålla på att logga ut och in på datorn vid användning skulle detta stjäla tid från patienten. De anser inte att detta är en bra orsak, men känner att det är nödvändigt. En anställd anser dessutom att informationen på datorn inte är hemlig för kollegor. Många anställda väljer också att låsa sin dator istället för att logga ur, då de kan efter att ha låst upp datorn fortsätta med det de höll på med utan att behöva logga in på alla program igen. Mer än hälften av de tillfrågade anser att andra anställda inte kan använda sin inloggade dator och skulle välja att säga till personen eller ansvarig på kliniken om detta skedde. En anställd skulle dessutom begära loggningsuppgifter för att få reda på vad som använts i systemet. En annan anställd anser dock att andra anställda kan använda den inloggade datorn om det gäller grundsystemet, men inte i enskilda system.

Loggning

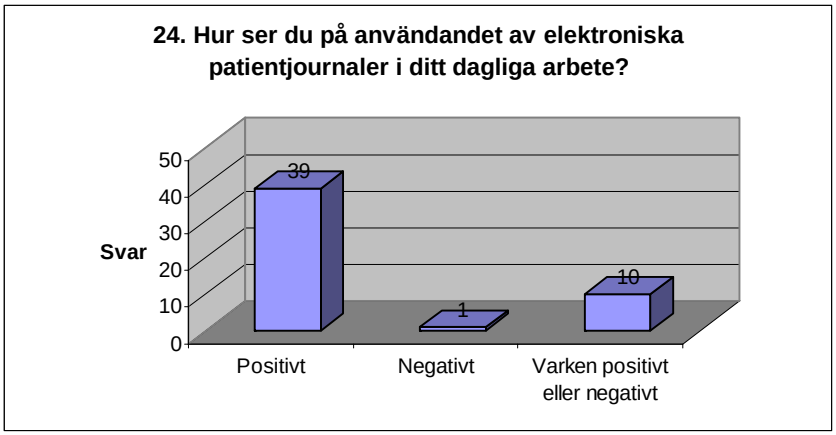
Av alla anställda har hälften av de anställda någon gång skrivit ner sitt lösenord på till exempel en papperslapp för att kunna komma ihåg alla de olika lösenorden. 15 anställda har dessutom lånat ut sina inloggningsuppgifter till någon annan och då vanligast en kollega eller vikarie. En tredjedel av samtliga respondenter är inte medvetna om hur ofta de ska byta lösenord och så många som 25 anställda känner inte till de regler som gäller då en dator lämnas obevakad och känslig information kan ses av obehöriga. På frågan om de känner till de hot och risker som kan uppstå om en dator lämnas obevakad var det bara ett litet antal som visste detta. Bland annat kan det leda till sekretessbrott och användarkontot kan bli avstängt, men en anställd känner ändå att det är ologiskt att varje gång behöva logga ur och in på datorn för att förhindra detta. Av de tillfrågade vet majoriteten att allt de gör i systemet loggas och kan ses av ansvariga. Flertalet tycker dock detta är bra samt är medvetna att de inte kan dölja det som sker i systemet på deras inloggning.

5.6.2 Mobilitet

Mobiliteten existerar endast på den egna kliniken, då de anställda kan komma åt sin profil på de olika datorerna. Dock blir det problem om de ska lånas ut till andra kliniker och enligt undersökningen känner majoriteten frustration över att behöva använda flera olika datorer i sitt dagliga arbete.

5.6.3 E-journaler

En tredje del av de tillfrågade är negativa till den nuvarande säkerheten kring de patientjournaler (majoriteten använder fortfarande pappersjournaler) som används, men flertalet är positiva till användning av elektroniska patientjournaler (se Figur 5-6-3). De som är negativa till den nuvarande säkerheten anser att patientjournalerna i pappersform är för lättillgängliga för alla att läsa. På en klinik sparar anställda remisser som skannats in till datasystemet i kartonger och dessa är inte låsta. En anställd som använder sig av e-journaler anser att IT-säkerheten just nu är under all kritik på kliniken.

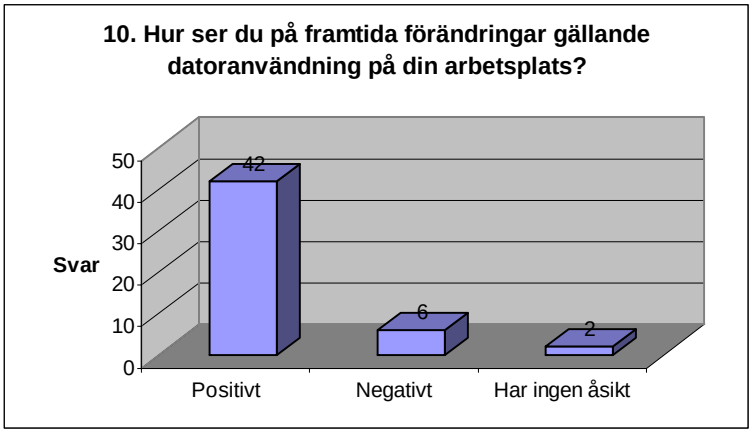


Figur 5-6-3 E-journaler

48 respondenterna känner till vilket ansvar de har som anställda då de varje dag hanterar känslig information. Av dessa vet sex anställda dock inte om de rättliga åtgärder som kan drabba dem om de till exempelvis läser en journal till en patient som de inte har någon vårdrelation till. Endast två anställda känner emellertid att arbetsplatsen varit dålig på att informera vad som gäller vid hantering av känslig information.

5.6.4 Attityder till förändringar

Majoriteten, enligt Figur 5-6-4, av de tillfrågade anser att det är positivt med förändringar och de som inte är positiva anser att de redan har ett välfungerande datajournalsystem som känns bra som det är. En ytterligare åsikt är att de system som ska införas inte är tillräckligt anpassade för just den kliniken. Programmen trycks vara uppbyggda på det sättet att de anställda sitter vid en och samma dator under ett helt arbetspass, men så är inte verkligheten. De nya förändringarna anses också stjäla mer tid av personalen och det blir mindre tid med patienterna.



Figur 5-6-4 Framtida förändringar

6 Analys

I den här delen har vi använt oss av de referenser som vi byggt upp vår uppsats kring samt de intervjuer och den enkät som redovisats i den empiriska delen av uppsatsen. Intervjuerna har i huvudsak försett oss med information om hur IT-säkerheten fungerar på Länssjukhuset Ryhov idag, medan enkäten mestadels har gett oss information om vad användarna anser om den nuvarande datoranvändningen samt säkerheten kring den. I analysdelen kommer insamlad data att kopplas ihop med information samt teorier från kapitel ***Fel! Hittar inte referenskälla.*** *och 4 då vi försöker besvara våra forskningsfrågor.*

6.1 Hur kan smarta kort förbättra IT-säkerheten inom hälso- och sjukvården?

Enligt Mitrović (2005) hanterar organisationer idag stora mängder värdefull information och genom datatekniska och administrativa åtgärder måste de hålla en optimal nivå gällande tillgänglighet, modifierbarhet, sekretess och spårbarhet. Enligt vår insamlade data använder sig samtliga kliniker på Länssjukhuset Ryhov av datorer i sitt dagliga arbete, men i olika stor omfattning. Enkätundersökningen visar att majoriteten uppskattar datorn i det administrativa arbetet och att datorn även hjälper till att förkorta den. Radiologen samt Ögonkliniken äger idag arbetsredskap som är mycket teknikbaserade och samtliga IT-kontaktpersoner anser att de inte skulle klara sig utan datorer i sitt arbete (se 5.5.1). Radiologen menar att trots problemen som finns och har funnits, så vill de inte tillbaka till en icke datoriserad värld då det inte skulle fungera med dagens arbetsbörda. De menar även att tekniken i allmänhet hjälper till att diagnostisera samt behandla fler människor.

Trots alla positiva uttalanden om datorer på Länssjukhuset Ryhov har vi kunnat identifiera ett flertal problem inom Landstinget. Landstinget och sjukhusets miljö, komplexa informationsflöde samt lagar och restriktioner är, enligt respondenter från IT-Planering ITC samt IT-kontaktpersonerna, några av anledningarna till de problem som uppstått. Även den Nationella IT-strategin har konstaterat att hälso- och sjukvården är en komplex organisation med mycket integritetskänslig information (Regeringen, 2006). Detta har varit en anledning till att utvecklingen av IT-stöd inom vården gått långsamt och att det fortfarande, enligt vår uppfattning, är i någon slags utvecklingsfas där många fel, problem och brister ofta uppstår.

Informationssäkerhet syftar bland annat till att skapa policys och riktlinjer, för att skydda den informationstillgång som finns i en organisation (Mitrović, 2005). Enligt IT-Planering finns det fortfarande mycket att arbeta med inom det här området, då det existerar en viss otydlighet från landstingsledningens sida. Günther-Hanssen (personlig kommunikation 2006-04-11) anser att det borde finnas tydligare riktlinjer och direktiv inom Landstinget, då han menar att trots Länssjukhusets olika policys ligger ute på Intranätet är det nödvändigt att påminna de anställda om det (se 5.4.1). Även flertalet av klinikerna påpekar att det finns ett behov av att ständigt informera de anställda om policys och riktlinjer, då information är en färskvara. Det är skilda meningar om hur medvetna de anställda är om den information som finns och enligt enkätundersökningen är det så många som hälften av de tillfrågade som inte känner till de regler som gäller då exempelvis en dator med eventuellt känslig information lämnas obevakad. Informationen bör även vara tydlig, då det påpekas från IT-Planering att det är svårt att veta vart gränserna går mellan rätt och orätt när det gäller datorer och den lättillgängliga information de erbjuder. Detta påpekas uppstå speciellt på de klinikerna med öppen behörighet.

6.1.1 Loggning

Hos flertalet av de intervjuade respondenterna fanns det en diskussion om öppenhet av system och det ansvar som läggs på den anställde i förhållande till att införa hårdare åtkomstmöjligheter/behörighetskrav och viss låsning av system. Då det inom hälso- och sjukvården finns integritetskänslig information är det av stor vikt enligt Ruland (2002) att den skyddas och att patienternas integritet bibehålls samt att det värnas om förtroendet mellan patient och vårdgivare. Medicinkliniken, Rehabiliteringsmedicinska kliniken samt IT-Planering anser att det är bättre att ge de anställda mer ansvar och därmed större frihet, men att istället logga det som görs i systemen. Den Nationella IT strategin anser också att användandet av IT-stöd i vården ger ett bättre skydd för patienters integritet, då det går att spåra och förebygga intrång av olika slag (Regeringen, 2006). Loggning är som Mitrović (2005) diskuterar i kapitel 4.2.1 ett annat ord för spårbarhet och används för att kunna ställa användare till svars för felaktiga eller förbjudna handlingar utförda i systemet. En av användarna anser att ett stort säkerhetsansvar ska ligga på den enskilde, men det är viktigt att de anställda är informerade om vad som gäller och tar eget ansvar och följer de regler och riktlinjer som finns.

Trots att elektroniskt lagrad data kan bli mer tillgänglig för vårdgivarna menar vi att de i slutändan ändå omfattas av lagar så som PUL (se 4.4.5) och sekretesslagen (se 4.4.3) som reglerar precis som nu vad användarna får och inte får göra. Om vi ska spekulera i detta så torde det inte bli fler som bryter mot lagen bara för att mediet byts ut även om det i vissa fall kan bli mer frestande. Att dessutom använda sig av loggning menar majoriteten av samtliga respondenter vara mycket positivt och kan verka i förebyggande syfte. Av användarna är majoriteten dessutom medveten om att allt de gör i systemet loggas och kan ses av ansvariga. Kanske kan det till och med vara mer avskräckande att allt loggas i förhållande till att läsa en pappersjournal i vilken det är svårare att kontrollera vem som har läst vad. IT-Planering, Radiologen samt Rehabiliteringsmedicinska kliniken menar att loggningen idag är bristfällig inom sjukhuset och bör förbättras (se 5.5.1). Klinikerna vill ha bättre och enklare rutiner för hur loggarna ska skötas och kontrolleras. De kliniker som idag arbetar med pappersjournaler har inte haft samma behov av loggning, vilket antagligen är en orsak till att det har blivit eftersatt och en naturlig orsak till att alla inte använder sig av loggar idag. Ytterligare en orsak till bristfällig loggning kan vara problemet med inloggningsprocessen, så sammanfattningsvis anser vi att Länssjukhuset Ryhov först behöver lösa problemet med in- och utloggningsprocessen innan loggningen kommer att fungera tillfredsställande.

6.1.2 Tillgänglighet

Günther-Hanssen (personlig kommunikation, 2006-04-11) tillsammans med tre av IT-kontaktpersonerna anser att prestandan på systemen inte är tillfredsställande. Systemen är slöa och det tar enligt dem alldeles för lång tid att starta upp datorn, logga in och/eller att utföra aktiviteter på datorn eller via nätet. Detta leder enligt undersökningen i viss mån till frustration bland användarna då de inte kommer åt systemen. Enligt Bishop (2003) är tillgängligheten en viktig del i systemets pålitlighet, då ett system som inte fungerar bra är lika illa som att inte ha ett datasystem över huvudtaget. Driftsäkerheten på Sjukhuset Ryhov är enligt Radiologen, Medicinkliniken samt Ögonkliniken inte heller tillfredsställande (se 5.5.1). De anser att de inte kan lita på att systemen finns tillgängliga och Radiologen har dessutom drabbats av att system legat nere och anser att kliniken inte kunnat uppfylla de säkerhetskrav som finns. Antalet datorer varierar mellan klinikerna och på vissa ställen är

detta löst med så kallade gruppinloggningar, vilket innebär en gemensam första inloggning för hela kliniken. Ambulansenheten anser detta vara en nödvändighet hos dem trots att det bara tar bort ett inloggningsförfarande. Vi förstår att detta är en praktisk lösning från sjukhusets sida, men anser ändå att den information som dagligen hanteras i organisationen måste skyddas bättre och vara mer lättlillgänglig.

6.1.3 Modifierbarhet

Enligt Günther-Hanssen (personlig kommunikation, 2006-04-11) och Radiologen är ett problem på Länssjukhuset Ryhov att flera anställda ibland måste dela på de datorer som finns, vilket kan utgöra en säkerhetsrisk då informationen kan göras tillgänglig för obehöriga. På vissa kliniker blir det så att den anställde som först anländer till arbetet på morgonen och loggar in på datorn är också den som är inloggad resten av dagen, medan andra använder samma dator. Vi anser att detta kan påverka både modifierbarheten och sekretessen, eftersom det blir svårare att skydda informationen från obehöriga, samt oönskad förändring av informationen. Enligt Bishop (2003) syftar modifierbarheten just till hur trovärdig informationen är och detta kontrolleras av uppgiven identitet av användaren. IT-kontaktpersonerna anser att de anställda hela tiden måste påminnas om hur viktigt det är med informationssäkerhet, för att kunna behålla den.

6.1.4 Sekretess

Majoriteten av de tillfrågade i enkätundersökningen anser att systemet idag är tillräckligt säkert för att skydda informationen från obehöriga, men då majoriteten av användarna är missnöjda med inloggningsprocessen väljer hälften av respondenterna att helt enkelt inte logga ut på grund av tidsbrist eller glömska (se 5.6.1). Detta menar vi leder till en ökad säkerhetsrisk och gör systemet osäkert trots flertalet lösenord för att skydda informationen. Enligt Ruland (2002) samlas det dagligen in information inom hälso- och sjukvården om enskilda personer som är känslig för obehöriga och därför måste det läggas stor vikt på sekretessen. Enligt Bishop (2003) innebär sekretess att en organisation vill dölja information för obehöriga, vilket enligt oss berör sjukvården i allra högsta grad. Günther-Hanssen (personlig kommunikation, 2006-04-11) menar att det är förvånansvärt få anställda som inte vet att de inte ens får läsa sin egen journal, vilket visar att det måste tryckas ännu mer på sekretessen. En anställd från enkätundersökningen anser dessutom att informationen inte är hemlig för andra anställda, men enligt Bishop (2003) kommer det största hotet mot säkerheten just från människorna inom en organisation och inte utanför. Offenbacher (personlig kommunikation, 2006-04-11) påpekar att det måste finnas en vårdrelation till patienten, för att den anställde ska få läsa journalen, men eftersom information om patienter tyvärr ändå sprids i mer eller mindre omfattning är det viktigt att vårdgivare tar sitt ansvar och tänker på sekretessen. När det gäller vårdrelation är detta inget som regleras i systemet så som en behörighet utan om en anställd har tillgång till journalsystemet kan hon se samtliga journaler. Det enda som hindrar personen i fråga är en förfrågan om den anställde har en vårdrelation till patienten där användaren bara ska svara ja eller nej. Mycket ansvar läggs därmed på vårdgivarna. Det är dock viktigt att det finns en bra avvägning mellan spridning/tillgänglighet av information och restriktioner för de anställda då patientdata, enligt Regeringen (2006) och den Nationella IT-strategin samt Ruland (2002), kan vara livsavgörande. Det får inte uppstå problem att nå information då det är nödvändigt och därav måste ansvaret ligga på vårdgivaren. Det stöd som patienten har mot olovlig spridning av data anser vi i slutändan vara lagen samt väl skötta loggar, personers samvete och konsekvenser för de som missköter sig.

6.1.5 Autentisering

Inloggningsprocessen på Länssjukhuset Ryhov är enligt majoriteten av de tillfrågade idag en omfattande process där användarna måste inneha många olika lösenord för att komma åt de olika applikationerna i ett system. Enligt Mitrović (2005) är det viktigt att en organisation hanterar auktoriseringen till datasystemen så effektivt som möjligt och att användarna har behörighet till de system som de ska använda. Samtliga kliniker med undantag för Ambulansenheten är missnöjda med inloggningsprocessen (se 5.5.1). Anledningen till detta är sannolikt att Ambulansenheten inte behöver logga in i lika många system och har dessutom ett gruppinlogg medan övriga kliniker antingen har för få datorer och/eller mellan åtta och tio lösenord att memorera. Majoriteten av respondenterna i enkätundersökningen upplever idag irritation över att hela tiden behöva logga in och ut på de olika applikationerna (se 5.6.1). Även IT-Planering påpekar att problemet med inloggningsprocessen existerar och menar att det är en av de största anledningarna, som de uppfattat det, till missnöje bland användarna. Personligen har varken IT-Planering eller ITC samma problem, då de alla har tillgång till en egen dator och inte samma typ av arbetsuppgifter. Dock påpekar IT-Planering att även de har ett flertal lösenord att memorera, men då de har egen dator behöver de inte logga in och ut flera gånger per dag (se 5.4.1).

Enligt Bishop (2004) är lösenord den mest grundläggande autentiseringsmekanismen och baseras på vad användaren vet. Människor kan komma ihåg upp till åtta tecken utan problem, men det kan bli svårt att komma ihåg mer än ett sådant. På Länssjukhuset Ryhov anses alla dessa inloggningar teknikiskt krångliga och Offenbacher (personlig kommunikation, 2006-04-11) menar att detta kan medföra en säkerhets risk, då många användare väljer att skriva ner sina lösenord på papper för att komma ihåg dem. Även Bishop (2004) berör detta och menar att lösenord lätt blir nerskrivna om användaren måste komma ihåg flera långa lösenord. Beroende på vart dessa nerskrivna lösenord förvaras kan de utgöra en säkerhetsrisk. Detta kan vi se i vår undersökning, vilken visar att utav samtliga användare i enkätundersökningen har hälften någon gång skrivit ner sitt/sina lösenord på till exempel en papperslapp för att kunna komma ihåg det/dem (se 5.6.1). 15 anställda har dessutom lånat ut sina inloggningsuppgifter till någon annan och då vanligast en kollega eller vikarie. På frågan om de känner till de hot och risker som kan uppstå om en dator lämnas obevakad var det bara ett litet antal som visste detta. Bland annat kan det leda till sekretessbrott och användarkontot kan bli avstängt, men en användare känner ändå att det är ologiskt att varje gång behöva logga ut och in på datorn för att förhindra detta. Vi tror dock inte att de anställda skulle logga ut oftare om de var mer medvetna om riskerna i den situation som råder nu. Vi anser att konsekvenserna av för få datorer, långsamma system och för många lösenord tyvärr resulterar i slarv, både medvetet och omedvetet, med in och utloggningar.

6.1.6 Smarta Kort

Bidgoli (2002) anser att smarta kort kan vara ett sätt att öka säkerheten i en organisation. Som en behörighetskontroll och autentisering används idag smarta kort på olika sätt inom en organisation för att på ett säkert sätt identifiera en användare. Enligt intresseorganisationen Carelink är kraven så höga på säkerheten inom vården att smarta kort skulle vara den bästa lösningen. IT-planering anser att IT-säkerheten måste förbättras med ett smart kort i centrum och med utgångspunkt från projektet SITHS samt den Nationella IT-strategin (Regeringen, 2006).

På det smarta kortet ska det finnas en PKI, som bland annat möjliggör singel sign on, säkra överföringar av medicinsk information samt digitalt signerade journalhandlingar och recept. Carelink anser att ett vanligt tjänstekort med ett tjänstecertifikat inte är tillräckligt för att lösa de säkerhetskrav som ställs inom hälso- och sjukvården. Då vi intervjuade ITC visade det sig att enheten under hösten 2006 kommer testa hur smarta kort kan användas för att underlättar arbetet i verksamheten. Här ska smarta kort identifiera användaren på två olika sätt, först talar kortet om vem användaren är genom autentisering och det andra är en signerings- och krypteringsdel där det är en applikation som verifierar användaren.

Enligt smarta kortets uppfinnare, Roland Moreno, är den garanterade identitetssäkerheten den mest intressanta egenskapen med smarta kort (Höynä, 1997). Det smarta kortet karaktäriseras av vissa egenskaper som är inbäddat i kortet och den typen av smarta kort som valts till användning i dagsläget hos ITC är ett kort med en mikroprocessor som gör det möjligt att programmera och utöka applikationer allt eftersom (Rankl och Effing, 2001). Dessa egenskaper gör det möjligt att överföra, förvara och processa data och kortet skyddas mot obehöriga och manipulation (Finkenzeller, 2004). Kortet som ITC ska nyttja innehåller tre magnetspår, där ett spår kan programmeras av ITC själva och har möjlighet att förvara privata nycklar samt utföra modern kryptografi.

Eftersom de smarta korten är kopplade till ett operativsystem skapas möjligheten att skriva konfidentiell data till kortet så att det inte kan läsas utifrån (Finkenzeller, 2004). Minnesfunktionerna på kortet som att lägga till, ta bort och avläsa data kan länkas ihop på vissa villkor från både hårdvara och mjukvara. Enligt Wettergren (1997) går ett smart kort igenom olika faser där det först är det programmerat för att klara ett visst antal operationer och sedan blir det ”personaliserat”, för att kunna knytas till ett viss användare. Enligt ITC kommer det att finnas två certifikat som ska laddas ner till kortet, så att det kan nyttjas av användaren. Det ena certifikatet ska användas för att tala om vem användaren är på ett säkert sätt och det andra tillåter användaren att sända information krypterat och signerat över systemet. Rättigheterna sedan, det vill säga det användaren får göra i systemet, kommer att läggs upp i HSA-katalogen. Enligt Carelink (2006d) är HSA-katalogen en viktig basenhet för att kunna skapa infrastruktur på en nationell nivå. Smarta kort och HSA-katalogen hänger samman på grund av att användaren måste identifiera sig för att få tillgång till sina rättigheter. Kortet kommer också vara kopplat till användaren med en pinkod. Enligt Wettergren (1997) och O’Mahony et al. (2001) kan det smarta kortet med en Pinkod identifiera rätt användare med korten innan det utför den begära operationen.

Då certifikaten laddas ner, har de, enligt ITC, en tidsbegränsning på 5 år. Dessa kan dock ändras beroende på hur länge en användare till exempelvis ska vara anställd på arbetsplatsen. Detta är något som Bishop (2003) påpekar som viktigt då en organisation måste ha med i beredskap att användare slutar på arbetsplatsen och inte längre ska ha behörighet till datasystemet. Här måste det finnas ett effektivt sätt att stoppa behörigheten, så att användaren inte längre har tillgång till den information som finns inom organisationen. Hos ITC kommer det att fungera så att varje gång ett smart kort används, jämförs det i en återkallningslista, så att de kan försäkra sig om att användaren är en behörig användare. I återkallningslistan kollas det om certifikaten fortfarande är aktiva och den här listan uppdateras flera gånger per dag. Vi anser detta vara ett mycket bra tillvägagångssätt för att skydda information och det skapar en bra struktur och kontroll av de kort som använda inom Landstinget.

Enligt vår undersökning, ska dock det smarta kortet i dagsläget inte användas till inloggning vid Länssjukhuset Ryhov. ITC menar att de inte fått något uppdrag av ledningen, som i sin tur inte ser något sådant behov ute i verksamheten. Vi anser dock att enkätundersökningen

samt intervjuerna med kontaktpersonerna visar på något annat. Vi har identifierat ett behov av en bättre arbetssituation främst gällande in- och utloggningen som enligt oss till viss del kan lösas med hjälp av ett smart kort. Även om många i enkätundersökningen känner att dagens inloggning är säker, så är den ändå krånglig och tidskrävande. Det händer också att användarna väljer att inte logga ur sin profil, utan låter andra använda datorn på den egna inloggningen. Vi tror att detta kan ha en betydande inverkan på IT-säkerheten och hur den konfidentiella informationen skyddas. Antalet lösenord kan ha invaggat ledningen i en falsk säkerhet enligt oss, men om de ser att det inte ”bara” är ett problem i det dagliga arbetet utan även påverkar säkerheten negativt torde det läggas relativt högt på prioriteringslistan enligt oss.

Enligt Bishop (2004) är autentisering i ett system när en identitet kan bindas till en enhet och vi anser att autentiseringen hos Länssjukhuset Ryhov kan bli bättre om det sker via ett smart kort. Om användaren istället har ett smart kort, måste detta sättas i en kortläsare och användaren kan inte lämna dator utan att ta bort det. På så sätt kan rätt användare identifiera sig på ett säkrare sätt än med vanlig inloggning. ITC hoppas ändå i framtiden att använda smarta kort som en del av inloggningsprocessen, passerkort, och ID-kort (se 5.3.2). Som Carelink (2006e) också diskuterar är det en stor omstrukturering som måste ske för att få detta att fungera och detta kommer att ta mycket lång tid då infrastrukturen och personal får nya arbetsuppgifter.

Som vi ser det skulle ett smart kort kunna lösa vissa av Länssjukhuset Ryhovs problem idag. Först inloggningsprocessen som vi fått erfara genom våra studier är krånglig och tidsödande, men även en säkerhetsrisk. Det vi ser som ett önskemål från de anställda är att slippa att logga in i varje applikation för sig och använda sig av upp till tio olika lösenord. De vill ha ett inloggningsförfarande med endast ett inlogg för att nå samtliga applikationer. Ett gruppinlogg som varit uppskattat hos Ambulansenheten tror vi bara är en övergångslösning som inte kommer att förändra mycket i det stora hela. Vi anser att denna lösning som sagt inte är hållbar i längden då användarna fortfarande har cirka nio applikationer att logga in i, men visst ett steg på vägen till en säkrare och bättre arbetsmiljö. Klinikerna menar att det kan vara bra med en gruppinlogg, men att det är en inlogg det vill ha i slutändan.

Vi är medvetna om att detta kan lösas utan smarta kort genom att förändra systemen och skapa nya profiler till användarna. Problemet är säkerheten som kan påverkas negativt genom detta, då det som sagt endast krävs en inloggning för att nå all känslig information och glömmer eller orkar inte användaren då logga ur finns detta mycket lättillgängligt för obehöriga. Slarvet med utloggning behöver inte upphöra för att inloggningsförfarandet ändras, men det kommer enligt oss troligtvis att minska. Att använda ett smart kort i samband med ett nytt inloggningsförfarande ser vi som en bättre och säkrare lösning. Då sjukvården är en organisation med mycket integritetskänslig information är det av stor vikt att denna hanteras så säkert som möjligt. Kortet medför att säkerheten höjs enligt (Bidgoli, 2002) då det ger en säker identifiering av personen i fråga. Om kortet dessutom används som passerkort, vilket är tänkt på ITC kommer de anställda troligtvis att ta det med sig när det lämnar datorn och därmed logga ut i större utsträckning. Självklart är tillgången till datorer en faktor som påverkar hur rutinerna kommer att se ut med ett smart kort, precis som det gör nu. Om inte antalet datorer ökar kan problemet kvarstå, men som tidigare nämnts kommer inloggningsprocessen att förenklas och gå snabbare, vilket sannolikt underlättar och möjliggör ”delade” datorer på arbetsplatsen. Respondenterna på Ögonkliniken samt Medicinkliniken nämner själva smarta kort som ett önskat redskap för inloggning, passerkort, etc. och menar att det skulle underlätta klinikernas arbete (se 5.5.1).

När det gäller spårbarhet så löses loggningen i sig inte enbart av ett smart kort, men som nämnts innan, kommer loggningen att bli mer trovärdig och användbar om de anställda använder sin egen profil i arbetet. Det sker även viss loggning på kortet och det är möjligt att i den publika delen av certifikatet se vad personen i fråga använt kortet till (se 5.3.1). Detta leder även till en större säkerhet för användarna själva, vilket vi anser är viktigt att informera om. Inte heller det stora ansvaret som ligger på en vårdgivare kommer att försvinna, men även det kan i vår uppfattning kontrolleras i större grad med en säker och smidig inloggning genom smarta kort.

6.2 Hur kan smarta kort öka mobiliteten?

Carelink arbetar, enligt Björner (2001) för att vårdgivarna och informationen ska bli lika mobila som dagens patienter är. Det är därför särskilt viktigt att ha en öppen PKI i större regioner, då det är stor rörlighet bland personalen och antalet dubbelanställningar är stort. I den Nationella IT-strategin framgår att information om patienter skall följa patienten samt att vårdgivarna skall ha tillgång till denna information för att kunna bedriva en säker och bra vård (Regeringen, 2006). I Hälso- och sjukvårdslagen framgår dessutom att vården som ges skall vara av god kvalitet samt tillgodose patientens behov och trygghet och dessutom vara lättillgänglig (se 4.4.4). För att hälso- och sjukvården ska kunna leva upp till dessa krav framöver, måste de se över sin mobilitet. HSA-katalogen är ett sätt att skapa mobilitet eller rättare sagt uppfylla de krav som finns för mobila patienter (Carelink, 2006d). Katalogens huvudsyfte är att alltid ge vårdgivare tillträde till aktuell information oavsett var patienten eller vårdgivaren befinner sig. Enligt den Nationella IT-strategin är HSA-katalogen en viktig grund för arbetet med en nationell infrastruktur (Regeringen, 2006).

Vi har i vår studie kunnat konstatera att det idag inte finns någon direkt mobilitet för användarna att röra sig mellan de olika arbetsplatserna inom Landstinget, vilket även ITC påpekar. Detta kan, enligt ITC, lösas med en bättre architektur/infrastruktur och personliga profiler till användarna som kan användas överallt (se 5.3.3). Detta behöver enligt respondenten inte innebära att smarta kort måste användas, men de påpekar att det skulle bidra till en högre säkerhet då användarna kan identifiera sig på ett säkert sätt.

Majoriteten av klinikerna ser behovet av gemensam information och infrastruktur, då de märkt att patienter blivit mer mobila. PÖS har till viss del underlättat patientens mobilitet, men bara inom Landstinget i Jönköping och inte på nationell nivå. Dessutom har inte alla kliniker och enheter tillgång till PÖS idag, då de kommit olika långt i datoriseringsprocessen. Läkare kan i PÖS se vilka behandlingar/åtgärder vårdcentraler eller andra kliniker gjort, vilket enligt dem underlättar vidare behandling.

IT-Planering anser också att brist på teknik som stödjer mobilitet på klinikerna är ett problem, då de flesta är mycket rörliga i sitt arbete. Samtliga kliniker har anställda som rör sig mellan kliniker, enheter eller andra delar inom Landstinget i Jönköping och Medicinkliniken menar att mobiliteten är viktig och att åtkomsten av system (när de kommer till en annan arbetsplats) är mycket varierande, vilket påverkar deras arbete negativt. De som drabbas hårdast av bristen av teknik som stödjer mobilitet menar Medicinkliniken och Radiologen är läkarna som går ronder och i slutändan patienten (se 5.5.2). De har till viss del bärbara datorer, men kommer dock inte åt känslig information då säkerheten på dessa inte är fullgod.

Mobiliteten kan främst lösas genom en gemensam infrastruktur som ger sjukhus och primärvård tillgång till information om patienter vart de än befinner sig. Detta är också vad

den Nationella IT-strategin vill uppnå (Regeringen, 2006). Hur kan då smarta kort underlätta mobiliteten och skapandet av denna gemensamma information? Vi anser att de smarta korten kommer att tillåta de anställda att skicka och ta emot krypterad information både nationellt och inom landsting. Det kan även ge en säker identifikation av en vårdgivare så han eller hon kan få tillgång till den gemensamma informationen. Vidare kan ett smart kort underlätta in- och utloggningsprocessen, vilket bidrar till ett säkrare system, men även underlättar det dagliga arbetet genom att spara tid och förenkla. IT-Planering anser att ett smart kort skulle leda till ökad mobilitet. Enligt undersökningen har vi sett att den interna mobiliteten är bristfällig och speciellt utsatta som nämnts ovan är läkarna när de exempelvis går ronder (se 5.5.2). Deras mobilitet kunde därmed enligt oss bli bättre genom användandet av ett smart kort som ger en snabb inloggning eller höjer säkerheten på de bärbara datorerna så de kommer åt den information de behöver.

Ett annat alternativ är att ge patienten ett smart kort att förvara sin data på, vilket leder till att informationen följer patienten vart hon än befinner sig. Enligt Offenbacher och Ögonkliniken skulle det bästa vara om patienten fick bära runt sin information på ett smart kort och själv ge sitt samtycke till vem som ska få läsa journalen. Då skulle behandlingar kunna ske snabbare och även fungera när patienter besöker olika sjukhus. Det här är även något som Höynä (1997) samt Regeringen (2006) i den Nationella IT-strategin diskuterar. Det är då tänkt att patienter ska kunna använda smarta kort till att identifiera sig samt innehålla information så som patientens medicinska historia och akut medicinska uppgifter. Ambulansenheten kan se fördelar med detta men nämner samtidigt tillsammans med ITC att det skulle bli mycket dyrt och risken för att patienten tappar eller glömmer sitt kort är stort. Smarta kort för patienter kommer att diskuteras mer under avsnitt 6.3.

6.3 Hur ser behovet och säkerheten ut gällande e-journaler?

Ett identifierat problem bland respondenterna är tekniken på och mellan klinikerna och andra enheter mellan och inom Landstinget i Jönköping. Majoriteten av de intervjuade IT-kontaktpersonerna menar att tekniken är ett stort problem då det leder till dålig kommunikation och samarbete. De påpekar vikten av att kunna kommunicera mellan enheter för att skapa tillgänglighet av information samt för att effektivisera vården. Ambulansenheten menar att effektivitet försvinner då system inte kan kommunicera med varandra, vilket i slutändan går ut över patienten. Det komplicerar helt enkelt möjligheten att följa patienten i vårdkedjan och hantera flödet av patienter.

Möjlighet till integrerade system och gemensam infrastruktur är en av hörnstenarna i den Nationella IT-strategin, vilken menar att detta är ett måste för att bedriva säker och bra vård (Regeringen, 2006). De anser att vårdkvaliteten kan förbättras vid ökad kunskap om patienten genom en gemensam patientjournal. Även Ruland (2002) menar att patientinformation är en av de viktigaste tillgångarna vid vård av patienter. All information om en patient så som bilder och text samlas i journaler som kan lagras på olika sätt. Journaler är teknikneutrala, vilket innebär att de kan sparas på olika typ av medier och fortfarande vara en journal.

För tillfället menar Regeringen (2006) i den Nationella IT-strategin att det är få system som kommunicerar med varandra över gränserna, vilket vi även kunnat konstatera på Länssjukhuset Ryhov där de olika klinikerna kommit olika långt i sin utveckling mot införandet av IT-stöd och därmed har problem med kommunikation. Idag används mestadels slutna system inom kliniker och trots detta eller kanske på grund av detta har vi sett en del problem. Om vi ser på tekniken i sig har den varit bristfällig och vi undrar hur de ska lyckas få det

driftsäkert och stabilt i ett större sammanhang. Detta måste lösas, inte bara för hälso- och sjukvården själva utan det är dessutom reglerat i personuppgiftslagen.

Samtliga kliniker anser att tanken om en gemensam plattform med gemensamma standarder, smarta kort samt gemensamma e-journaler som presenteras i den Nationella IT-strategin är mycket tilltalande.

Svårigheter kommer troligen ändå att uppstå vid införandet av gemensamma och integrerade system. Den Nationella IT-strategin (se 2.1.2) påpekar att den gemensamma infrastrukturen och informationen måste byggas på en enad struktur och regelverk och därmed bli enhetlig (Regeringen, 2006). Rehabiliteringsmedicinska kliniken menar att det finns mycket prestige inom framförallt läkarkåren, vilket skapat problem för dem bara genom att slå ihop åtta tidigare pappersjournalsystem till ett datoriserat system. Det största problemet är termer och yttryck som de menar är skiftande och att kompromissa ihop ett regelverk antas ta tid och skapa motsättningar.

Tre av klinikerna använder sig idag av olika sorters e-journaler, en klinik har både pappersjournaler och e-journaler medan den femte kliniken bara använder pappersjournaler. Det är, enligt Ögonkliniken, viktigt att samla ihop den idag spridda informationen till ett ställe där den enkelt går att nå. De e- journaler som används idag är knutna till klinikerna och ej gemensamma för sjukhuset. PÖS kan till en viss del ses som e-journal då den lagrar data om patienter, men användarna kan bara gå in och läsa den informationen och har inte möjlighet att ändra eller lägga till något. Trots att PÖS idag är begränsad anser samtliga kliniker att det är en bra början, men den behöver nå ut till fler och innehålla mer information. Därför har samtliga kliniker önskemål om en e-journal som är gemensam för hela sjukhuset och är nödvändiga i framtiden då dessa kommer att förbättra det dagliga arbetet.

Problemet med pappersjournalerna är, enligt Rehabiliteringskliniken och Ambulansenheten, att det skapas en ny journal för varje sjukhus, klinik, etc., vilket leder till dubbellagring av information och dessutom försämrad effektivitet. Klinikerna menar att tillgängligheten är och kommer att vara den största fördelen med e-journaler. Rehabiliteringskliniken och Ambulansenheten menar vidare att gemensam lagring av information kommer att leda till bättre och effektivare vård för patienterna. Även Offenbacher på IT-Planering håller med och tillägger att det är viktigt att komma åt information snabbt och enkelt, vilket e-journaler kan bidra till. Sammanfattningsvis anser hon att e-journaler bidrar till en ökad tillgänglighet och bättre översikt. Vårdgivarna behöver informationen för att kunna ge bästa behandlingen, vilket även Ruland (2002) håller med om.

IT-Planering och ITC anser båda att utvecklingen mot e-journaler är mycket positivt, men ITC tillägger att en lagändring måste ske för att e-journaler skall fungera nationellt, över landstingsgränserna. De tillägger att lagarna ”står mot varandra” i dagsläget, vilket gör situationen komplicerad. Regeringen (2006) genom den Nationella IT-strategin tar upp att harmonisera lagar och regelverk med en ökad IT-användning som ett av sina arbetsområden. Problemet är enligt dem att lagarna inte har utvecklats i takt med tekniken inom hälso- och sjukvården. Detta har resulterat i att lagar och regelverk idag inte stödjer verksamhetens alla behov av IT-stöd etc. Så för att få en fungerande nationell e-journal så måste detta åtgärdas, men även IT-stöden som lagarna ska harmonisera med måste ses över. Som IT-Planering nämner innebär e-journaler användandet av ett ”nytt” medie att exponera integritetskänslig information i, vilket kan innebära en större risk för intrång.

Klinikerna ser ingen större risk med införandet av e-journaler utan anser att den tekniken som finns att tillgå idag, dock inte på sjukhuset än, är tillförlitlig. De tillägger dock att det är

mycket viktigt att informationen skyddas och att säkerheten kring den nationella plattformen är tillräcklig. Radiologen samt Rehabiliteringsmedicinska kliniken diskuterar dessutom om det är nödvändigt att all information finns tillgänglig, det vill säga viss information som är extra integritetskänslig så som sexuellt överförbara sjukdomar eller HIV. Detta skulle enligt oss kunna lösas med visst behörighetskrav. Lämplig teknik finns förmodligen att tillgå problemet vi kan se är att teknik åldras fort och måste underhållas och uppdateras för att fortsätta vara en säker lösning. Dessutom finns det människor som ser tjusningen i att lyckas överlista systemen, vilket i detta fall kan få stora konsekvenser. Vi menar inte att e-journaler är en dålig lösning i sig utan att hälso- och sjukvården bör se över den kunskap som finns, då vi sett tendenser till brister inom detta område viket bland annat Ambulansenheten påpekar. Vissa delar av utvecklingen bör dessutom styras centralt, då vi ser vilka problem lokalt bestämmande lett till. IT-Planering anser att det uppstått fel från början när Landstingen fick stort självstyre. De fortsätter och menar att Sverige är ett litet land och har samma regler och lagar som måste följas i alla landsting och eftersom Sverige har en homogen struktur borde det ha resulterat i en större samordning på nationell nivå. Här menar vi, som även vissa av respondenterna lyfter fram, att den Nationella IT-strategin brister. Bohlin (2006) och Hellbom (2006) påpekade vikten av en konkret strategi tidigare i år, vilket vi anser att den Nationella IT-strategin kanske inte har levt upp till. Det kommer krävas fler riktlinjer för att få igång processen att skapa exempelvis en nationell e-journal.

Som nämnts ser klinikerna ingen nackdel med e-journaler gällande säkerhet utan snarare tvärtom. Trots att informationen kommer vara mer lättillgänglig blir det enligt respondenterna även säkrare då e-journaler bidrar till en ökad spårbarhet med förutsättning att in- och utloggningsprocessen fungerar. Ögonkliniken menar att pappersjournaler kan vara svåra att lokalisera och de kan inte se vem som har läst dem, då detta inte registreras. Bland användarna är en tredjedel negativa till den nuvarande säkerheten kring patientjournaler, men som nämnt tidigare är majoriteten positiva till e-journaler. Anledningen till dagens missnöje grundas i användandet av pappersjournaler och att det enligt respondenterna är alldeles för lätt att läsa en journal utan.

En ytterligare positiv aspekt med e-journaler är mobiliteten, vilken enligt oss och Regeringen (2006) genom den Nationella IT-strategin, kommer att förbättras både för vårdgivaren och patienten. Nationella e-journaler kan tillhandahålla vårdgivaren information om en patient oberoende av vilken vårdcentral, sjukhus etc. han eller hon besöker. Det finns dessutom önskemål från Ögonkliniken och IT-Planering om att lagra e-journaler på smarta kort som sedan patienten själv får ta ansvar för. Idag äger sjukhuset informationen, vilket Ögonkliniker anser vara ologiskt då det handlar om patienten själv. Det skulle även enligt dem lyfta en stor säkerhetsbörda från vårdgivarna om patienten själv ansvarar för informationen. Önskan om mobilitet skulle kunna tillgodoses även den med ett smart kort tillhörande patienten och Offenbacher tillägger att det skulle kunna ge snabbare vård. Ambulansenheten och Rehabiliteringsmedicinska kliniken menar att det finns nackdelar med att patienten skulle ha ett eget kort. Det är lätt att tappa samt svårt att administrera ett smart kort för patienten.

Vi anser också att det skulle bli ett dyrt och svårt uppdrag rent administrativt att ge samtliga svenska medborgare ett smart kort. Som klinikerna också nämner är det lätt att tappa eller glömma kortet, då det inte är självklart att alltid bära med sig kortet. Informationen skulle dessutom behöva lagras på något mer ställe än bara på kortet för att kunna återskapas vid borttappat kort eller liknande. Att patienten själv hemma skulle lagra informationen säkert ses inte som ett alternativ enligt oss, då alla inte har tillgång till en dator, inte har ordentliga brandväggar, virus skydd och backupper. Lagring på en extern hårddisk eller ett USB-

minne ser vi inte som säkrare, då det kan försvinna, gå sönder eller utsättas för yttre hot så som brand, vattenskada eller inbrott.

För att följa den Nationella IT-strategin där tillgänglighet är en av grundpelarna och där Regeringen (2006) nämner att en säker och bra vård inte kan ges utan patientinformation vore det riskabelt att inte förvara den information som finns säkert. Vi anser att landsting har en större förmåga att förvara informationen på ett bra och säkert sätt. Att inte ha tillgång till patientinformation på sjukhus eller vårdcentraler skulle dessutom enligt oss försvåra forskning och utveckling inom hälso- och sjukvården. Mycket av den lagrade informationen som finns om oss och många led bakåt i tiden är ett värdefullt bidrag till dagens forskare.

Sammanfattningsvis anser vi precis som majoriteten av respondenterna att e-journaler är ett mycket tilltalande sätt att hantera data om patienter. Det skulle dessutom underlätta och effektivisera arbetet för vårdgivarna samt öka mobiliteten och i slutändan ser vi samt många av respondenterna att det skulle bidra till en bättre vård för patienten.

6.4 Hur ser attityderna ut gällande datoranvändningen samt säkerheten?

Enligt Goldkuhl och Röstlinger (1988) kan förändringar i en organisation röra upp känslor så som osäkerhet och rädsla hos personalen och bör därför genomföras med stor kunskap om den nuvarande arbetssituationen. Både ITC och IT-Planering tror att användarna vid Länssjukhuset Ryhov känner osäkerhet vid förändringar och Offenbacher (personlig kommunikation 2006-04) anser också att informationen om förändringar inte bör komma ut för tidigt, då de anställda blir irriterade om det tar för lång tid. Istället vill de få reda på förändringar när de är mer konkreta och på sätt bli delaktiga i det som ska hända.

Vår enkätundersökning visar dock att majoriteten av användarna faktiskt är positiva till förändringar, men vill samtidigt inte att framtida förändringar ska stjäla tid från varken personalen eller patienterna. Vi anser att detta är ett bra sätt att se på förändringarna inom sjukvården, då den blir mer och mer datoriserad. Som Goldkuhl och Röstlinger (1988) också diskuterar, handlar förändringar oftast om att det finns problem som måste åtgärdas och därför är nödvändiga. Detta är något som vi känner att de anställda också är medvetna om, då det krävs vissa datoriserade förändringar för att underlätta det dagliga arbetet. Vi håller också med författarna om att förändringar kan skapa mer problem än lösningar om det inte sker på rätt sätt, då det hela tiden är viktigt att kommunicera med de olika parterna och arbeta på ett strukturerat sätt. En klinik menar att beslut om vissa förändringar ibland tas på en sådan hög nivå att de program som sedan implementeras inte passar kliniken i alla fall. Vi anser därför att det är viktigt att framtida förändringar arbetas fram utifrån kliniken och de anställdas behov, så att det inte går åt onödig tid och resurser. Vi förstår samtidigt att det är svårt att få ett enhetligt datasystem som ska passa alla kliniker, men anser ändå att det ska gå att kommunicera på något sätt mellan dem samt att inloggningsprocessen ska kunna gå till på samma sätt på alla kliniker.

6.4.1 Attityder till förändringar

Majoriteten av respondenterna känner att osäkerhet inför förändringar dämpas om det är tydlig information och utbildning. Som tidigare nämnt känner en del anställda att vissa applikationer som implementeras inte riktigt anpassas efter kliniken behov, utan istället byggs utifrån någon standard som inte fungerar helt i deras dagliga arbete. Som Preece et al.

(2002) diskuterar tillsammans med Hallerström (1995), känner många människor en osäkerhet inför användandet av datorer och ett sätt att komma över denna osäkerhet är att ta reda på hur datorn kan hjälpa till vid det dagliga arbetet. Vi anser att majoriteten av användarna är nöjda med att använda datorer i det dagliga arbetet och undersökningen visar heller ingen skillnad i ålder. ITC beskriver tillsammans med IT-Planering att det är viktigt med olika utbildningar, såsom säkerhet och användningen av datorer, för att hela tiden hålla användarna uppdaterade med aktuell information. Detta är något som även Arbetslivsinstitutet (2006) trycker på, då det just är viktigt att få ut rätt information och utbildning som användarna kan ta till sig. Efter att ha varit ute i verksamheten håller vi med om att utbildningar är ett bra sätt att hjälpa användarna, då varje klinik jobbar olika och har sina egna applikationer. Det som generellt sett är samma mellan klinikerna är inloggningsprocessen och säkerheten kring denna, och samtliga IT-kontaktpersoner anser att det bedrivs bra säkerhetsutbildningar tillsammans med IT-Planering. Dock är det viktigt att hela tiden påminna användarna om att hålla sig uppdaterade, för att på så sätt undvika att känslig information kommer i orätta händer. Ibland utför IT-Planering olika enkätundersökningar för att undersöka hur datormognaden ser ut och kan på så sätt se om det krävs mer utbildning eller om användarna känner sig trygga med den information de fått. Vi anser att det är bra att IT-Planering arbetar på det här sättet, då det enligt Preece et al. (2002) är viktigt att få användarna att känna sig trygga med datorn, applikationerna samt säkerheten.

6.4.2 Diffusionsteori

Enligt ITC kommer ett införande av smarta kort innebära stora omstruktureringar och förändringar som kan komma att påverka användarna både positivt och negativt. Vi anser därför att det är viktigt att denna omstrukturering sker på ett sådant sätt att användarna inte känner rädsla för det nya som ska införas. Rogers (1995) använder termen diffusionsteori, då det handlar om att sprida kunskap om något nytt och då bäst genom individer i mellan. Författaren menar också att en spridning även kan analyseras, för att se hur sannolik en spridning är, vilket vi menar skulle kunna anammas även på Länssjukhuset Ryhov. IT-Planering har diskuterat innan att de gärna gör enkätundersökningar för att titta på hur datormognaden är och vi anser att de även kan använda Rogers analys för att titta på hur nyheten om användandet av smarta kort kan spridas på bästa sätt och inte skapa oro bland användarna. En sådan analys på Länssjukhuset Ryhov skulle kunna se ut så här;

- Kunskapsstadiet: Stadiet då individen får kännedom om att innovationen existerar. Många användare på Länssjukhuset Ryhov känner sig missnöjda med just inloggningsprocessen, så en nyhet om att smarta kort skulle kunna underlätta detta anser vi vara viktigt att det kommer ut till användarna. Informationen kan komma antingen via Intranätet, men kanske ännu bättre via IT-kontaktpersonerna. Det är de som har den närmaste kontakten med IT-Planering och klinikerna, så därför anser vi att användarna lättare kommer lyssna på dessa personer.

- Övertygelsestadiet: Här upplever individen antingen en positiv eller negativ inställning till innovationen. Här anser vi att det är viktigt att ITC tillsammans med IT-Planering framför informationen om smarta kort på ett sådant sätt att användarna får positiva känslor om korten och lättare kan anamma dem. Visa på vilka fördelar smarta kort har och hur det kommer att påverka användarnas dagliga arbetssituation.

- Beslutstadiet: Här bestämmer sig individen för att anamma eller avfärda innovationen. Då det gäller införandet av smarta kort på Länssjukhuset Ryhov är det svårt

för individen att ta det beslutet att inte använda smarta kort, då detta kommer att göras på en högre nivå. Dock kommer smarta kort nu under hösten 2006 att testas i verksamheten, vilket vi anser ger användarna en chans att testa korten för att minska sin osäkerhet. På det här sättet kan ITC visa ännu tydligare vad smarta kort kan göra för verksamheten.

- Implementationsstadiet: Här bestämmer sig individen för att använda innovationen och då på ett konkret sätt. Även här kommer beslutet om att använda smarta kort tas på en högre nivå och användarna får rätta sig efter beslutet. Åter igen anser vi att det kommer ha en stor påverkan på hur detta beslut läggs fram till användarna. Viktigt att kommunikationen hela tiden fungerar och att klinikerna får känna sig delaktiga.

Som både Rogers (1995) och Günther-Hanssen (personlig kommunikation 2006-04-11) diskuterar varierar det dock hur användarna tar till sig en innovation och det är angeläget utbildningar som underlättar införandet när nya IT-stöd ska implementeras. Vi anser att detta är något som användarna är nöjda med idag och därför bör IT-Planering fortsätta med att hålla utbildningar.

.

7 Slutsatser

De slutsatser som kommer att presenteras nedan har framkommit från analysen av insamlad data samt teori. Studien är utförd tillsammans med Länssjukhuset Ryhov, vilket leder till att slutsatserna främst är kopplade till dem. Slutsatserna presenteras i enlighet med forskningsfrågornas upplägg.

- *Hur kan smarta kort förbättra IT-säkerheten inom hälso- och sjukvården i enlighet med den Nationella IT-strategin och Carelink?*

  Smarta kort kan enligt vår studie förbättra IT-säkerheten inom hälso- och sjukvården genom att skapa en säker identifiering vid användning av IT-stöd. Smarta kort kan även bidra till en förenklad in- och utloggningsprocess, vilket i sin tur leder till bättre spårbarhet.

- *Hur kan smarta kort öka mobiliteten bland vårdgivare och patienter?*

  Enligt undersökningen är det idag en brist i mobiliteten för både vårdgivare och patienter. Studien visar att ett smart kort med säker identifiering leder till säkrare system och enklare in- och utloggningsprocess, vilket i sin tur bidrar till mobilitet inom och mellan kliniker. Vidare kan den säkra identifieringen med hjälp av ett smart kort bidra till den säkerhet som krävs för en gemensam plattform och således öka mobiliteten för både vårdgivare och patienter.

- *Hur ser behovet samt säkerheten ut kring e-journaler i förhållande till pappersjournaler?*

  Enligt undersökningen är behovet av e-journaler stort, men säkerheten gällande dem bör ses över. Genom användandet av e-journaler kan vi konstatera att tillgänglighet av information ökar, vilket studien visar är av stor betydelse inom hälso- och sjukvården.

- *Hur ser attityderna ut till datoranvändningen samt säkerhetsaspekterna som idag finns inom hälso- och sjukvården bland vårdgivarna?*

  Enligt studien är attityderna hos majoriteten av vårdgivarna positiva till förändringar gällande en förbättrad arbetssituation och mer specifikt en förbättrad in- och utloggningsprocess, som kan underlättas av smarta kort. Studien visar att vårdgivarna anser att en förbättring gällande dagens säkerhet- och arbetssituation är nödvändig, vilket smarta kort även kan bidra till. Då vårdgivarna är positiva till dessa typer av förändringar möjliggör detta därmed ett smidigt införande av smarta kort inom hälso- och sjukvården.

8 Avslutande diskussion

I det följande kapitlet redogör vi våra reflektioner över uppsatsen samt de erfarenheter vi fått. Vi diskuterar även studiens applicerbarhet och generaliseringsmöjligheter samt ger förslag på fortsatta studier inom ämnet.

8.1 Egna reflektioner och erfarenheter

Arbetet med denna studie har varit mycket intressant och givande för oss, då vi lärt oss mycket nytt under arbetets gång. Det har som nämns nedan inte varit en helt problemfri process, men vi anser dock att vi slutligen har lyckats besvara de forskningsfrågor som vi arbetat med för att uppfylla vårt syfte.

Genom vår studie har vi förstått att studera IT i hälso- och sjukvård är mer komplicerat än vad vi tidigare trott. I början var vi mer fokuserad på att titta på hur lösningen smarta kort kunde användas i sjukvården, men insåg snart att vi även måste titta på de lagar som gäller för att sekretess och behörighet ska gälla även vid användandet av smarta kort. Vi hade i början därför svårt att begränsa oss, då vi ville täcka in så många områden som möjligt. Detta resulterade att vi först fick ett frågeunderlag som var för omfattande för studien. Dock granskades och ändrades detta innan intervjutillfällena och vi ansåg då att frågorna täckte våra forskningsfrågor. Nu i efterhand har vi trots detta insett att en del av frågorna inte hade behövt vara med, då de inte hjälpte oss att svara på vårt syfte eller forskningsfrågor. Vi ville från början även studera ett sjukhus som infört smarta kort i sin verksamhet, vilket vi tror hade varit givande för studien. Dock ansåg vi att vår egen studie var för omfattande vid det laget för att kunna dra in en andra part i undersökningen.

Vid insamlandet av den empiriska data använde vi oss av både kvalitativ och kvantitativ studie, vilket vi fortfarande anser vara nödvändigt för studien. Vi valde att använda oss av semistrukturerade intervjuer, då vi ville ha möjligheten att ställa följdfrågor samt hålla diskussioner kring ämnet. Dock kan vi nu i efterhand känna att det ibland var svårt att få raka svar från våra respondenter, eftersom de gärna svävande ut i egna funderingar och då kom bort från ämnet. Detta resulterade i att vissa svar inte användes i analysen eller resultatet. Det positiva med att använda öppna frågor anser vi ändå vara att vi fått tillgång till intressant information som hjälpt oss vidare i arbetet och gett oss en klarare bild av hur ett sjukhus som en organisation fungerar. Vi har tidigare erfarenheter av att enkätundersökningar kan leda till stora bortfall och detta var något som vi ville undvika. IT-kontaktpersonerna var till en stor hjälp vid undersökningen då enkäterna lämnades ut och samlades in inom rimlig tid. Vi anser att arbetet också underlättades genom att hålla sig till ett antal kliniker samt användare och inte svävande ut i att undersöka alla användare på de kliniker som Länssjukhuset Ryhov har. Då tror vi att det hade blivit för omfattande samt svårt att få in en hög svarsfrekvens.

Tid är alltid en bristvara och gäller även för denna uppsats. Då vi var på det klara med vad vi ville skriva om, hade vi till en början svårt att hitta en organisation att studera. Istället för att börja studera litteraturen i tid, lades det ner mycket tid och energi på att övertala Länssjukhuset Ryhov att ingå i studien. Lite tur hade vi dock när det senare visade sig att de jobbade tillsammans med Carelink och hade funderingar på att testa smarta kort i sin verksamhet. Sedan skulle då vår planering passa ihop med respondenternas planering och detta gjorde att det lätt försvann ett par veckor till att bara vänta. Här kunde vi istället ha fokuserat mer på vad vi egentligen behövde ha med i uppsatsen för att svara på syftet, istället för att sitta med det i slutet då mycket annat ändå skulle genomföras. I och med att arbetet ökade i omfång, var det ibland även svårt att hålla den röda tråd som vi försökt skapa. En

riktig loggbok hade dessutom varit bra att använda istället för lösa papper som lätt försvinner för att komma ihåg olika diskussioner vi fört under arbetes gång.

Vi är medvetna om att det är många delar som kunde diskuteras inom ramen för ämnet, men vi har medvetet valt bort diskussionen om exempelvis biometri och som nämndes i avgränsningar, djupare tekniska eller ekonomiska diskussioner. När det gäller biometri är vi medvetna om att det kunde vara ett tillfredsställande, om inte mer säkert, komplement till smarta kort, men vi valde bort funderingar kring biometri som ett alternativ är för att vår studie inriktar sig på smarta kort och dess lämplighet inom hälso- och sjukvården.

Som nämnts ovan har det varit svårt att begränsa sig, men det är självklart även problematiskt att från början se vart studien leder och vad exempelvis de olika forskningsfrågorna kommer att resultera i. Vi har under studiens gång blivit medvetna om att problemfråga två och tre överlappar varandra i viss mån då vi insett att mobilitet kan skapas av e-journaler vars säkerhet kan möjliggöras av ett smart kort. Trots detta har vi valt att behålla uppdelningen av dessa två områden och låtit redovisa samt analysera dem var för sig, men samtidigt låtit vissa delar tas upp på nytt dock ur ett annat perspektiv. Anledningen till detta är att vi ser på mobilitet och e-journaler som två viktiga delar inom hälso- och sjukvården och att samtlig information inte är gemensam eller överlappar den frågan andra.

Sammanfattningsvis känner vi, trots en omfattande studie, att det varit en mycket intressant tid, där vi lärt oss mycket nytt gällande sjukvården i Sverige samt hur IT fungerar inom denna organisation.

8.1.1 Studiens applicerbarhet

Som vi tagit upp tidigare har arbetet med uppsatsen utförts tillsammans med Länssjukhuset Ryhov som studieobjekt och slutsatserna vi kommit fram till utifrån forskningsfrågor och syfte är främst relaterade till dem. Däremot ser vi att det finns möjlighet att applicera de slutsatser vi arbetat fram på andra sjukhus inom Sverige. Vi ser detta som troligt då vi fått erfara att klinikerna och enheterna inom ett sjukhus skiljer sig oerhört mycket gentemot varandra både gällande arbetssätt, teknik, kunskap och utveckling och anser därför att skillnaderna inte är större mellan sjukhus än vad de är inom en organisation. Då studien är utförd på Länssjukhuset Ryhov och resultaten kan appliceras på hela sjukhuset ser vi det även som troligt att vi kan applicera vårt resultat på andra sjukhus i Sverige. På Länssjukhuset Ryhov verkar attityderna gentemot smarta korttekniken vara gynnsamma och behovet av en förändrad arbetssituation stort, vilket vi anser torde vara fallet även på andra sjukhus. Så sammanfattningsvis ser vi att våra slutsatser från denna studie troligen kan appliceras på en nationell nivå, det vill säga på andra sjukhus runt om i Sverige.

8.2 Förslag till fortsatt arbete

En intressant studie skulle vara att följa upp det kommande pilotprojekt som ITC ska testa med smarta kort i sin egen verksamhet. Hur kommer smarta kort användas i organisationen och kommer behovet av smarta kort vid in- och utloggning att ses över närmare? Studien skulle kunna jämföras med andra sjukhus som samtidigt testar smarta kort och se om resultaten skiljer sig. De nya resultaten skulle också kunna analyseras och jämföras med denna uppsats resultat, för att se om bland annat användarnas attityd har ändrats med tiden.

En annan infallsvinkel för en studie kan vara att följa den tekniska biten vid införandet av smarta kort. Här skulle studien kunna fokusera på program och kostnader, som faktiskt har

en stor påverkan vid införande av nya IT-system. Något som ITC också diskuterade var den stora omstrukturering av bland annat personal som måste ske vid införandet av smarta kort och en studie skulle kunna fokusera djupare på vilka fördelar respektive nackdelar denna omstrukturering för med sig.

Referenslista

Beekman, G. & Rathswhol E.J. (2003). *Computer Confluence – Exploring Tomorrow's Technology*. New Jersey: Prentice Hall

Bidgoli, H. (2002). *Electronic Commerce, Principles and Practice*. San Diego: Academic Press

Bishop, M. (2003). *Computer security: art and science*. Boston: Addison-Wesley.

Bishop, M. (2004). *Introduction to computer security*. Boston: Pearson education.

Björner, O. (2001). *Varför SITHS*. Hämtad 2006-04-21 från http://www.carelink.se/pages/newsbill.asp?VersionID=1&Pages=1,246,37

ComputerSweden. (2004). *Fritt fram kolla patientjournaler*. Hämtad 2006-03-17 från http://computersweden.idg.se/ArticlePages/200404/15/20040415164730_CS327/20040415164730_CS327.dbp.asp

Carelink. (2006a). *Carelinks Organisation*. Hämtad 2006-04-20 från http://www.carelink.se/pages/oneRightPicture.asp?VersionID=1&Pages=1,2,24

Carelink. (2006b). *Så arbetar vi*. Hämtad 2006-04-20 från http://www.carelink.se/pages/oneRightPicture.asp?VersionID=1&Pages=1,2,277

Carelink. (2006c). *SITHS – En PKI för vård och omsorg i Sverige*. Hämtad 2006-04-21 från http://www.carelink.se/pages/newsbill.asp?VersionID=1&Pages=1,246,37

Carelink. (2006d). *HSA – Hälso- och Sjukvårds Adressregister*. Hämtad 2006-04-12 från http://www.carelink.se/files/doc_20051123132131.pdf

Carelink. (2006e). *Informationssäkerhet i vårdprocessen - Krav beskrivna i generella användningsfall utifrån vårdscenarion*. Hämtad 2006-04-18 från http://www.carelink.se/files/doc_2002126110411.pdf

Dagens Nyheter. (2004a). *Sjukhusanställd brottsmisstänkt för läst Lindhjournal*. Hämtad 2006-03-16 från http://www.dn.se/DNet/jsp/polopoly.jsp?d=147&a=261447

Dagens Nyheter. (2004b). *Böter för att ha läst Lindhs journal*. Hämtad 2006-03-16 från http://www.dn.se/DNet/jsp/polopoly.jsp?d=147&a=290413&previousRenderType=1

eEurope. (2005). *Ett informationssamhälle för alla*. Hämtad 2006-04-18 från http://europa.eu/scadplus/leg/sv/lvb/l24221.htm

Finkenzeller, K. (2004). *RFID Handbook – Fundamentals and Applications in Contactless Smart Cards and Identifications*. Chichester: John Wiley & Sons Ltd

Goldkuhl, G. & Cronholm, S. (2003). *Multi-grounded theory – Adding theoretical grounding to grounded theory*. Linköping

Goldkuhl, G. & Röstlinger, A. (1988). *Förändringsanalys – Arbetsmetodik och förhållningssätt för goda förändringsbeslut*. Lund: Studentlitteratur

Hallerström, M. (1995). *Informationsstrategi och ADB-upphandling* – en praktisk arbetsmetodik. Stockholm: Printgraf

Hansagi, H. & Allebeck, P. (1994*). Enkät och intervju inom hälso- och sjukvård*. Lund: Studentlitteratur

Holme, I.M. & Solvang, B.K. (1997). *Forskningsmetodik – Om kvalitativa och kvantitativa metoder*. Lund: Studentlitteratur

Johnsson, L-Å. (2002). *Patientsäkerhet och vårdkvalitet i hälso- och sjukvården*. Stockholm: Thomson Fakta.

Järvinen, P.H. (1999). *Research question guiding selection of an appropriate research method. Department of computer and information sciences:* University of Tampere, Finland.

Höynä, U-K. (1997). *Smarta kort – den smartaste lösningen?* Teledok Info nr 17. Stockholm: Teldok

Länssjukhuset Ryhov. (2006). *Om Länssjukhuset Ryhov*. Hämtad 2006-04-12 från http://www.lj.se/extweb/index.jsp?nodeId=24481&nodeType=13

Lundahl, U. & Skärvad, P-H. (1991). *Forskningsmetodik – Om kvalitativa och kvantitativa metoder*. Lund: Studentlitteratur

Mitrović, P. (2005). *Handbok i IT-säkerhet*. Pagina Förlags AB. Sundbyberg.

O'Mahony, D., Pierce, M. & Tewari, H,. (2001). *Electronic Payment Systems for E-commerce*. Norwood; Artech House Inc.

Preece, J., Sharp, H. & Rogers, Y. (2002). *Interaction Design - Beyond Human-Computer Interaction*. New York: John Wiley & Sons, Inc.

Rankl, W. & Effing, W. (2003). *Smart Card – Handbook*. Chichester: John Wiley & Sons ltd

Regeringen. (2006). *Nationell IT-strategi för vård och omsorg*. Hämtad 2006-04-03 från http://www.regeringen.se/content/1/c6/05/96/62/abac6cb0.pdf

Regeringskansliet. (2005). *Hälso- och sjukvård på lika villkor*. Hämtad 2006-04-03 från http://www.regeringen.se/sb/d/2717

Repstad, P. (1991). *Närhet och Distans: Kvalitativa metoder i samhällsvetenskap*. Lund: Studentlitteratur

Riksdagen, (2003). *Personuppgiftslag (1998:204)*. Hämtad 2006-04-03 från http://rixlex.riksdagen.se/htbin/thw?%24%7BOOHTML%7D=SFST_DOK&%24%7BSNHTML%7D=SFSR_ERR&%24%7BBASE%7D=SFST&BET=1998%3A204&%24%7BTRIPSHOW%7D=format%3DTHW

Ruland, C.M, (2002). *Vårdinformatik, hur användning av informations- och kommunikationsteknologi kan utveckla vård och omvårdnad*. Stockholm: Bokförlaget natur och Kultur.

Rättsnätet. (2006). *Hälso- och sjukvårdslagen*. Hämtad 2006-04-02 från http://www.notisum.se/rnp/SLS/LAG/19820763.HTM

Rättsnätet (2006). *Sekretesslagen*. Hämtad 2006-04-09 från http://www.notisum.se/rnp/SLS/LAG/19800100.HTM

Socialstyrelsen, (1994). *Patientjournallagen*. Hämtad 2006-04-10 från http://www.sos.se/sosfs/1993_20/1993_20.htm

Wettergren, C. (1997). *Security of smart card usage – exploring their logical security*. Stockholm; KTH

Wiedersheim-Paul, F. & Eriksson, L.T. (1991). *Att utreda, forska och rapportera*. Malmö: Liber-Hermods.

Bilaga 1 – Intervjuunderlag IT-Centrum och IT-Planering

- Vad är dina arbetsuppgifter?
- Varför tror du sjukvården har prioriterats så dåligt av regeringen gällande IT-användningen?
- Hur ser inloggningprocessen ut idag hos er?
    - Vilka fördelar respektive nackdelar anser du att dagens inloggningsprocess har?
- Hur hanteras informationssäkerheten hos er idag, gällande;

    Sekretess

    Spårbarhet

    Tillgänglighet

    Behörighet
- Kan datasystemet idag utföra någon loggning?
    - Vad tittar ni efter i så fall?
- Hur väl informerade är anställda om den informationssäkerhet som krävs?
- Har de anställda möjlighet att läsa de patientjournaler som finns i datasystemet?
    - Förklara PÖS i relation till e-journaler
- Tror du anställda inom sjukvården vet vilka rättsliga åtgärder som kan drabba dem om de exempelvis läser patientjournaler som den anställde ej har någon vårdrelation till?
- Vilka fördelar respektive nackdelar ser du med e-journaler?
- Vad anser du bör förbättras i framtiden gällande datoranvändningen hos er?
- Hur ser du på projektet SITHS? Fördelar/ nackdelar?
- Anser du att smarta kort kan förbättra säkerheten och informationshanteringen hos er?
    - Hur kan den i så fall förbättras?
- Hur skulle smarta kort användas hos er?
    - Certifikat/nycklar/lösenord?
- Behörighet, hur skapas vårdrelation?
- Kommer användarna genom att använda smarta kort bara behöva logga in en gång för att komma åt alla system?

- Tror du att smarta kort att öka mobiliteten bland de anställda och i så fall på vilket sätt? Fördelar/nackdelar?
- Hur upplever du attityderna till datoranvändningen bland de anställda på arbetsplatsen?
- Får användarna någon utbildning i datoranvändning hos er?
- Hur tror du de anställda känner inför ett förändringsarbete?
- Hur väl informerade är anställda om framtida projekt?

Bilaga 2 – Intervjuunderlag IT-kontaktpersoner

1. Vad är dina arbetsuppgifter?

Datoranvändningen

2. Tycker du att datorn är ett bra verktyg för att lösa dina arbetsuppgifter?
3. Använder du datorn vid informationssökning för att exempelvis kunna ställa diagnoser?
4. Hur upplever du den nuvarande situationen gällande datoranvändning och informationssäkerhet?
5. Hur upplever du attityderna till datoranvändning bland de andra i personalen på din arbetsplats?
6. Anser du att utbildningar som ges inom datoranvändning och säkerhet är tillräcklig?

IT-säkerhet

6. Vilka fördelar respektive nackdelar anser du att dagens inloggningsprocess har?
7. Tycker du det är bra att allt som sker i systemet loggas?
8. Hur väl informerade är ni anställda om den informationssäkerhet som krävs?
9. Anser du att den utbildning ni har fått gällande säkerhetsinformation varit tillräcklig?
10. Tror du anställda inom sjukvården vet vilka rättsliga åtgärder som kan drabba dem om de exempelvis läser patientjournaler som den anställde ej har någon vårdrelation till?

E-journaler

11. Tycker du att det är bra att lagra information elektroniskt?
12. Hur tycker du PÖS fungerar? Fördelar respektive nackdelar?
13. Vilka fördelar respektive nackdelar ser du med e-journaler?
14. Hur ser du på användandet av e-journaler inom ert landsting?

Framtiden

15. Vad anser du bör förbättras i framtiden gällande datoranvändningen hos er?
16. Hur tror du de anställda känner inför ett förändringsarbete?

Bilaga 3 – Enkätfrågor om informationssäkerhet

Denna enkät består av 27 frågor och är en del av en magisteruppsats vid Internationella handelshögskolan i Jönköping inom området informatik vilken syftar till att undersöka hur anställda ser på informationssäkerheten inom hälso- och sjukvården.

Instruktioner:

Enkätfrågorna bygger på bestämda svarsalternativ samt öppna frågor. För att välja ett svarsalternativ kryssar du i under respektive fråga och markerar endast ett av de alternativ som erbjuds. Vid de öppna frågorna svarar du med egna ord i de textfält som visas under frågan. Vissa frågor har också följdfrågor

Exempel:

Hur tycker du att vädret är idag?

Svar: På morgonen regnade det men framåt eftermiddagen sken solen och temperaturen steg. Därför anser jag att vädret gick från dåligt till utmärkt.

I detta öppna exempel har användaren med egna ord uttryckt sin åsikt om vädret.

Vänligen svara på samtliga frågor i enkäten. Vi ber om ditt spontana svar för att förkorta din svarstid.

Alla dina svar behandlas anonymt.

När du har svarat på samtliga frågor, ge enkäten till den person som delade ut den.

Tack på förhand!

Johanna Isaksson och Therése Sanne

Jönköping, April 2006

Enkätfrågor

Bakgrund

1. Kön ☐ Man ☐ Kvinna	**2. Ålder** ☐ 18-29 ☐ 30-39 ☐ 40-49 ☐ 50-59 ☐ 60-
3. Var har du din arbetsplats? ☐ Sjukhuset ☐ Vårdcentral ☐ Annat_____	**4. Hur länge har du arbetat på din nuvarande arbetsplats?** ☐ 0-5 år ☐ 6-10 år ☐ 11-15 år ☐ 16-20 år ☐ 20 år eller mer

Datoranvändning

5. Använder du dator i ditt dagliga arbete? ☐ Ja ☐ Nej	**6. Tycker du att datorn är ett bra verktyg för att lösa dina arbetsuppgifter?** ☐ Ja ☐ Nej
7. Hur anser du att den administrativa tiden påverkas av att du använder dator? ☐ Den förkortas ☐ Den ökar ☐ Oförändrad	**8. Tycker du att det är bra att lagra information elektroniskt?** ☐ Ja ☐ Nej **8a. Om nej, varför är detta inte bra?** _____ _____ _____
9. Använder du datorn vid informationssökning för att exempelvis kunna ställa diagnoser? ☐ Ja ☐ Nej	**10. Hur ser du på framtida förändringar gällande datoranvändning på din arbetsplats?** ☐ Positivt ☐ Negativt ☐ Har ingen åsikt **10a. Om negativt, varför?** _____ _____ _____

Informationssäkerhet

11. Informationssäkerhet innebär att känslig information ska skyddas för obehöriga. Anser du att det nuvarande datasystem som finns gör detta?

- ☐ Ja
- ☐ Nej
- ☐ Vet inte

12. Är du nöjd med den nuvarande inloggnings-process som krävs för att använda datasystemet på din arbetsplats?

- ☐ Ja
- ☐ Nej

12a. Om nej, varför är du inte nöjd?

_____

_____

_____

13. Har du någon gång skrivit ner ditt lösenord på exempelvis en papperslapp, skrivbordsunderlägg, etc?

- ☐ Ja
- ☐ Nej

14. Har du någon gång lånat ut dina inloggningsuppgifter till någon annan på din arbetsplats?

- ☐ Ja
- ☐ Nej

14a. Om ja, vid vilken situation?

- ☐ Vid sjukdom
- ☐ Till vikarie
- ☐ Till kollega
- ☐ Annan

_____

_____

15. Vet du hur ofta du ska byta lösenord?

- ☐ Ja
- ☐ Nej

16. Loggar du in på fler än en dator under en dag?

- ☐ Ja
- ☐ Nej

17. Om du sitter vid en och samma dator, behöver du ändå logga in på olika system för att nå den information du behöver?

- ☐ Ja
- ☐ Nej

17a. Om ja, upplever du irritation över att du måste logga in på flera olika system?

- ☐ Ja
- ☐ Nej
- ☐ Vet inte

18. Loggar du alltid ut när du lämnar din dator obevakad?

- ☐ Ja
- ☐ Nej

18a. Om nej, varför gör du inte det?

- ☐ Hinner inte
- ☐ Glömmer bort
- ☐ Annan orsak

_____

_____

19. Anser du att andra kan använda din inloggade dator?

☐ Ja
☐ Nej

19a. Om nej, vad skulle du göra om du upptäckte eller misstänkte att någon annan varit inne i systemet på din inloggning?

☐ Säga till personen
☐ Säga till ansvarig
☐ Ingenting
☐ Annat_____

20. Känner du till de regler som gäller på din arbetsplats om du lämnar din dator obevakad?

☐ Ja
☐ Nej

20a. Om ja, vet du vilka hot och risker som kan uppstå om anställda inte följer de regler som finns?

_____
_____
_____
_____
_____

Loggning

21. Tror du att allt du gör i datasystemet registreras?

☐ Ja
☐ Nej

21a. Om ja, tycker du att det är bra att allt du gör registreras i datasystemet?

☐ Ja
☐ Nej

22. Tror du att du kan dölja något som du har gjort i datasystemet?

☐ Ja
☐ Nej

22a. Om ja, vad tror du att du kan dölja?

_____
_____
_____
_____

Sekretess

23. Anser du att säkerheten gällande hantering av patientjournaler idag är tillräcklig?

☐ Ja
☐ Nej

23a. Om nej, varför?

_____
_____
_____
_____

24. Hur ser du på användandet av elektroniska patientjournaler i ditt dagliga arbete?

☐ Positivt
☐ Negativt
☐ Varken positivt eller negativt

24a. Om negativt, varför?

_____
_____
_____
_____

25. Anser du att säkerheten kring elektroniska journaler är tillräcklig?

☐ Ja
☐ Nej
☐ Vet inte

25a. Om nej, varför?

_____
_____
_____

26. Vet du vilket ansvar du har som anställd då du dagligen hanterar känslig information?

☐ Ja
☐ Nej

26a. Om nej, anser du att arbetsplatsen varit dålig med att informera hur känslig information ska hanteras?

☐ Ja
☐ Nej
Annat_____

27. Känner du till de rättsliga följder som kan uppstå då en anställd läser en patientjournal där det inte finns någon vårdrelation till patienten?

☐ Ja
☐ Nej

Övrigt

_____
_____
_____
_____

Tack för din medverkan!

Bilaga 4 – Sammanställning av enkät

	1. Kön		2. Ålder					4. Hur länge har du arbetat på din nuvarande arbetsplats?				
	Man	Kvinna	18-29	30-39	40-49	50-59	60-	0-5 år	6-10 år	11-15 år	16-20 år	20 år eller mer
1		x		x						x		
2		x		x				x				
3	x			x				x				
4		x	x					x				
5		x				x		x				
6		x					x	x				
7		x			x			x				
8		x			x							x
9	x						x					x
10		x		x					x			
11	x					x						x
12	x				x				x			
13		x	x						x			
14		x		x				x				
15		x				x		x				
16		x			x						x	
17		x				x						x
18		x			x						x	
19		x				x			x			
20		x			x							x
21		x		x					x			
22		x			x						x	
23		x			x					x		
24		x				x					x	

	1. Kön		2. Ålder					4. Hur länge har du arbetat på din nuvarande arbetsplats?				
	Man	Kvinna	18-29	30-39	40-49	50-59	60-	0-5 år	6-10 år	11-15 år	16-20 år	20 år eller mer
25		x		x				x				
26	x					x		x				
27	x		x					x				
28		x		x							x	
29	x					x						x
30		x			x				x			
31	x				x							x
32	x				x				x			
33	x			x					x			
34		x		x					x			
35	x				x						x	
36	x				x				x			
37		x			x			x				
38	x					x						x
39		x	x					x				
40		x			x							x
41		x				x						x
42		x			x			x				
43		x				x		x				
44		x					x					x
45		x			x						x	
46		x		x				x				
47		x		x					x			
48		x			x						x	
49	x					x						x
50		x			x							x

	5. Använder du dator i ditt dagliga arbete?		**6. Tycker du att datorn är ett bra verktyg för att lösa dina arbetsuppgifter?**		**7. Hur anser du att den administrativa tiden påverkas av att du använder dator?**			**8. Tycker du att det är bra att lagra information elektroniskt?**		**9. Använder du datorn vid informationssökning för att ex. kunna ställa diagnoser?**	
	Ja	Nej	Ja	Nej	Den Förkortas	Den ökar	Oförändrad	Ja	Nej	Ja	Nej
1		x	x			x		x		x	
2	x		x				x	x			x
3	x		x			x		x		x	
4	x		x				x	x		x	
5	x		x				x	x		x	
6	x		x		x			x		x	
7	x		x				x	x			x
8	x		x				x	x		x	
9	x			x		x		x		x	
10	x		x				x	x			x
11	x		x				x	x		x	
12	x		x		x			x		x	
13	x		x				x	x		x	
14	x		x				x	x		x	
15	x		x		x			x			x
16	x		x		x			x		x	
17	x		x		x			x		x	
18	x		x		x			x			x
19	x		x		x			x			
20		x	x		x			x			x
21	x		x				x	x			x
22	x		x		x			x		x	
23	x		x			x		x		x	
24	x		x		x			x			x

	5. Använder du dator i ditt dagliga arbete?		6. Tycker du att datorn är ett bra verktyg för att lösa dina arbetsuppgifter?		7. Hur anser du att den administrativa tiden påverkas av att du använder dator?			8. Tycker du att det är bra att lagra information elektroniskt?		9. Använder du datorn vid informationssökning för att ex. kunna ställa diagnoser?	
	Ja	Nej	Ja	Nej	Den Förkortas	Den ökar	Oförändrad	Ja	Nej	Ja	Nej
25	x		x			x		x			x
26	x		x		x			x		x	
27	x		x		x			x		x	
28	x		x		x			x			x
29	x		x			x		x			x
30	x			x		x		x			x
31	x		x			x		x			x
32	x		x				x	x			x
33	x		x		x			x			x
34	x		x		x			x			x
35	x		x		x			x			x
36	x		x				x		x		x
37	x		x		x			x			x
38	x		x			x		x			x
39	x		x				x		x		x
40	x		x		x			x			x
41	x		x			x		x			x
42	x		x		x			x			
43	x		x		x			x			x
44	x		x		x			x			x
45	x		x			x		x			x
46	x		x		x			x			x
47	x		x		x			x			x
48	x		x					x		x	
49	x		x				x	x			x
50	x		x				x	x			x

	10. Hur ser du på framtida förändringar gällande datoranvändning på din arbetsplats?			**11. Informationssäkerhet innebär att känslig information ska skyddas för obehöriga. Anser du att det nuvarande datasystem som finns gör detta?**			**12. Är du nöjd med den nuvarande inloggningsprocess som krävs för att använda datasystemet på din arbetsplats?**		**13. Har du någon gång skrivit ner ditt lösenord på exempelvis en papperslapp, skrivbordsunderlägg, etc?**	
	Positivt	Negativt	Har ingen åsikt	Ja	Nej	Vet inte	Ja	Nej	Ja	Nej
1		x		x			x		x	
2	x			x				x	x	
3		x				x		x	x	
4	x			x				x	x	
5	x				x		x		x	
6	x					x	x		x	
7	x			x			x		x	
8	x			x			x		x	
9		x		x				x		x
10	x			x			x		x	
11	x				x			x	x	
12	x			x				x		x
13	x			x			x		x	
14	x			x			x			x
15	x			x			x		x	
16	x			x			x		x	
17	x			x				x	x	
18	x			x				x	x	
19		x		x			x		x	
20	x			x				x	x	
21	x			x			x			x
22	x			x				x		x
23	x			x			x		x	
24			x	x			x			x

	10. Hur ser du på framtida förändringar gällande datoranvändning på din arbetsplats?			**11. Informationssäkerhet innebär att känslig information ska skyddas för obehöriga. Anser du att det nuvarande datasystem som finns gör detta?**			**12. Är du nöjd med den nuvarande inloggningsprocess som krävs för att använda datasystemet på din arbetsplats?**		**13. Har du någon gång skrivit ner ditt lösenord på exempelvis en papperslapp, skrivbordsunderlägg, etc?**	
	Positivt	Negativt	Har ingen åsikt	Ja	Nej	Vet inte	Ja	Nej	Ja	Nej
25	x			x			x		x	
26	x				x			x	x	
27	x			x				x		x
28	x			x			x			x
29	x			x			x			x
30		x		x			x		x	
31	x			x			x			x
32			x	x			x			x
33	x			x			x		x	
34	x				x			x		x
35	x			x			x			x
36	x			x			x			x
37	x			x			x			x
38	x			x				x		x
39	x			x				x		x
40	x			x			x		x	
41	x			x				x	x	
42	x			x			x		x	
43	x			x				x	x	
44	x			x			x		x	
45		x		x			x		x	
46	x			x			x		x	
47	x			x			x			x
48	x			x				x	x	
49	x				x			x		x
50	x				x			x		x

	14. Har du någon gång lånat ut dina inloggningsuppgifter till någon annan på din arbetsplats?		**14a. Om ja, vid vilken situation?**				**15. Vet du hur ofta du ska byta lösenord?**		**16. Loggar du in på fler än en dator under en dag?**		**17. Om du sitter vid en och samma dator, behöver du ändå logga in på olika system för att nå den information du behöver?**	
	Ja	Nej	Vid sjukdom	Till vikarie	Till kollega	Annan	Ja	Nej	Ja	Nej	Ja	Nej
1		x						x	x		x	
2		x					x		x		x	
3		x					x		x		x	
4	x				x			x	x		x	
5		x					x		x		x	
6		x					x			x	x	
7		x					x		x		x	
8	x			x			x			x	x	
9		x					x		x		x	
10		x						x	x		x	
11	x				x	x	x		x		x	
12	x		x			x	x		x		x	
13		x						x	x		x	
14		x					x		x		x	
15		x						x	x		x	
16		x						x		x	x	
17	x					x	x		x		x	
18		x					x		x		x	
19		x					x			x	x	
20		x					x		x		x	
21		x					x			x	x	
22		x						x	x		x	
23		x					x		x		x	
24		x					x		x			x

	14. Har du någon gång lånat ut dina inloggningsuppgifter till någon annan på din arbetsplats?		**14a. Om ja, vid vilken situation?**				**15. Vet du hur ofta du ska byta lösenord?**		**16. Loggar du in på fler än en dator under en dag?**		**17. Om du sitter vid en och samma dator, behöver du ändå logga in på olika system för att nå den information du behöver?**	
	Ja	Nej	Vid sjukdom	Till vikarie	Till kollega	Annan	Ja	Nej	Ja	Nej	Ja	Nej
25		x					x		x		x	
26		x						x	x		x	
27	x			x	x		x		x		x	
28		x					x			x	x	
29	x				x		x		x		x	
30	x				x			x	x		x	
31		x					x		x		x	
32		x						x	x			x
33	x			x	x		x		x		x	
34	x			x	x			x	x		x	
35		x					x		x		x	
36		x						x	x			x
37		x					x			x	x	
38		x						x	x		x	
39	x				x		x		x		x	
40	x				x		x			x	x	
41	x			x			x		x		x	
42	x				x		x			x	x	
43		x					x		x		x	
44	x			x				x		x	x	
45		x					x		x		x	
46		x					x		x		x	
47	x			x	x		x		x		x	
48		x					x		x		x	
49		x						x	x		x	
50		x						x	x		x	

	17a. Om ja, upplever du irritation över att du måste logga in på flera olika system?			**18. Loggar du alltid ut när du lämnar din dator obevakad?**		**18a. Om nej, varför gör du inte det?**			**19. Anser du att andra kan använda din inloggade dator?**	
	Ja	Nej	Vet inte	Ja	Nej	Hinner inte	Glömmer bort	Annan orsak	Ja	Nej
1			x	x					x	
2	x			x					x	
3	x				x	x	x	x	x	
4	x			x						x
5	x			x					x	
6	x			x						x
7		x		x						x
8	x			x						x
9	x				x			x		x
10	x				x	x		x		x
11	x				x		x			x
12	x				x	x	x	x		x
13		x			x			x	x	
14	x			x					x	
15		x		x						x
16	x			x					x	
17	x			x						x
18	x				x			x		x
19	x				x			x		x
20	x			x						x
21	x			x						x
22	x				x	x			x	
23	x			x					x	
24					x	x		x	x	

	17a. Om ja, upplever du irritation över att du måste logga in på flera olika system?			18. Loggar du alltid ut när du lämnar din dator obevakad?		18a. Om nej, varför gör du inte det?			19. Anser du att andra kan använda din inloggade dator?	
	Ja	Nej	Vet inte	Ja	Nej	Hinner inte	Glömmer bort	Annan orsak	Ja	Nej
25	x				x			x	x	
26	x			x						x
27	x				x			x	x	
28		x		x						x
29		x		x					x	
30	x			x						x
31		x			x			x		x
32				x						x
33		x		x						x
34	x			x						x
35		x		x						x
36					x			x		x
37	x				x			x		x
38	x			x					x	
39	x				x		x		x	
40		x			x			x	x	
41	x				x			x		x
42	x			x					x	
43	x				x			x		x
44	x			x						x
45	x				x			x		x
46		x			x	x				x
47		x			x			x	x	
48	x				x		x		x	
49	x				x			x	x	
50	x				x			x	x	

	19a. Om nej, vad skulle du göra om du upptäckte eller misstänkte att någon annan varit inne i systemet på din inloggning?				**20. Känner du till de regler som gäller på din arbetsplats om du lämnar din dator obevakad?**		**21. Tror du att allt du gör i datasystemet registreras?**		**21a. Om ja, tycker du att det är bra att allt du gör registreras i datasystemet?**	
	Säga till personen	Säga till ansvarig	Ingenting	Annat	Ja	Nej	Ja	Nej	Ja	Nej
1					x		x		x	
2						x	x			x
3					x		x		x	
4		x				x	x		x	
5						x	x		x	
6		x			x		x		x	
7	x				x		x		x	
8	x					x	x		x	
9	x	x				x	x		x	
10			x			x	x		x	
11	x	x			x		x		x	
12	x	x		x		x		x		
13						x	x		x	
14				x	x		x		x	
15	x				x		x		x	
16						x	x			x
17	x				x		x		x	
18	x				x		x		x	
19					x			x		
20	x					x	x		x	
21		x			x		x		x	
22				x		x	x		x	
23						x	x			x
24	x					x	x		x	

	19a. Om nej, vad skulle du göra om du upptäckte eller misstänkte att någon annan varit inne i systemet på din inloggning?				**20. Känner du till de regler som gäller på din arbetsplats om du lämnar din dator obevakad?**		**21. Tror du att allt du gör i datasystemet registreras?**		**21a. Om ja, tycker du att det är bra att allt du gör registreras i datasystemet?**	
	Säga till personen	Säga till ansvarig	Ingenting	Annat	Ja	Nej	Ja	Nej	Ja	Nej
25					x		x		x	
26	x					x	x		x	
27						x	x		x	
28	x					x	x		x	
29					x		x		x	
30				x		x	x		x	
31	x				x		x		x	
32		x				x	x			
33	x					x	x		x	
34			x			x	x			x
35	x				x			x		
36						x	x		x	
37	x	x			x			x		
38						x	x			
39						x	x		x	
40			x			x	x		x	
41	x				x		x			x
42		x			x		x		x	
43	x	x			x		x			
44		x			x		x		x	
45			x		x		x		x	
46	x					x		x		
47					x			x		
48						x	x			x
49					x		x			x
50					x		x			x

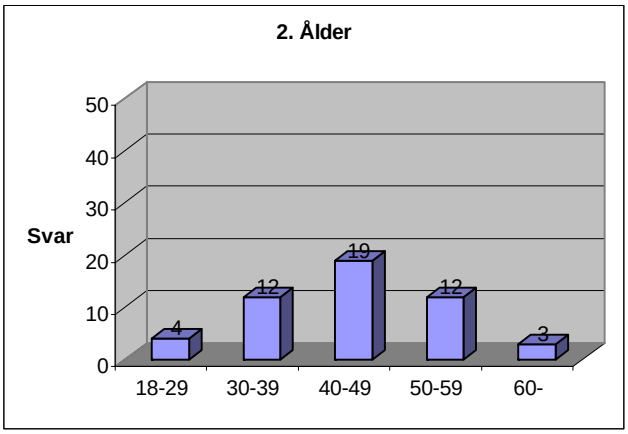
	22. Tror du att du kan dölja något som du har gjort i datasystemet?		**23. Anser du att säkerheten gällande hantering av patientjournaler idag är tillräcklig?**		**24. Hur ser du på användandet av elektroniska patientjournaler i ditt dagliga arbete?**			**25. Anser du att säkerheten kring elektroniska journaler är tillräcklig?**		
	Ja	Nej	Ja	Nej	Positivt	Negativt	Varken positivt eller negativt	Ja	Nej	Vet inte
1		x	x				x			x
2		x		x	x			x		
3		x		x		x		x		
4		x	x		x			x		
5		x	x		x			x		
6		x	x		x					x
7		x		x			x			x
8		x	x		x			x		
9		x	x		x			x		
10		x	x		x			x		
11		x		x	x				x	
12		x	x		x			x		
13		x	x		x			x		
14		x	x		x			x		
15		x	x		x			x		
16		x	x		x			x		
17		x	x		x			x		
18		x	x		x			x		
19	x		x		x			x		
20		x	x		x			x		
21		x	x		x			x		
22		x		x	x				x	
23		x	x		x			x		
24		x	x				x			x

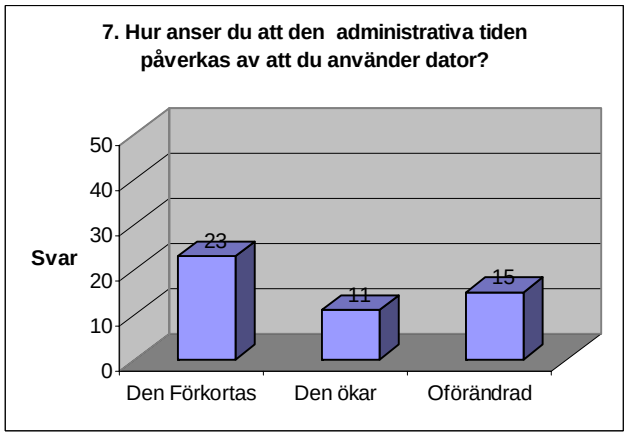
	22. Tror du att du kan dölja något som du har gjort i datasystemet?		**23. Anser du att säkerheten gällande hantering av patientjournaler idag är tillräcklig?**		**24. Hur ser du på användandet av elektroniska patientjournaler i ditt dagliga arbete?**			**25. Anser du att säkerheten kring elektroniska journaler är tillräcklig?**		
	Ja	Nej	Ja	Nej	Positivt	Negativt	Varken positivt eller negativt	Ja	Nej	Vet inte
25		x		x	x			x		
26		x	x		x			x		
27		x	x		x			x		
28		x	x		x			x		
29		x	x		x			x		
30		x	x				x		x	
31		x	x		x			x		
32		x	x				x	x		
33		x	x		x			x		
34		x		x	x				x	
35		x	x		x			x		
36		x		x			x	x		
37		x	x		x				x	
38		x	x		x			x		
39		x	x		x				x	
40		x	x		x			x		
41		x	x		x			x		
42		x	x		x			x		
43		x		x			x			x
44		x		x			x			x
45		x		x			x			x
46		x	x				x			x
47		x		x	x					x
48		x		x	x			x		
49		x		x	x				x	
50		x		x	x				x	

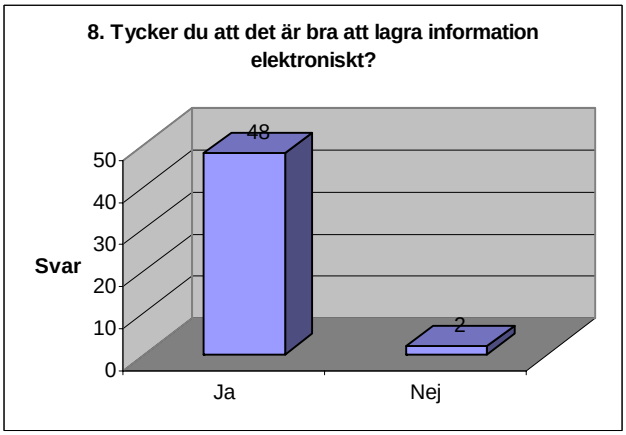
	26. Vet du vilket ansvar du har som anställd då du dagligen hanterar känslig information?		**26a. Om nej, anser du att arbetsplatsen varit dålig med att informera hur känslig information ska hanteras?**		**27. Känner du till de rättsliga följder som kan uppstå då en anställd läser en patientjournal där det inte finns någon vård-relation till patienten?**	
	Ja	Nej	Ja	Nej	Ja	Nej
1	x				x	
2	x				x	
3	x				x	
4	x					x
5	x				x	
6	x				x	
7	x				x	
8	x				x	
9	x				x	
10	x				x	
11	x				x	
12	x				x	
13	x					x
14	x				x	
15	x					x
16	x					x
17	x				x	
18	x				x	
19	x			x	x	
20	x					x
21	x				x	
22	x				x	
23	x			x	x	
24	x				x	

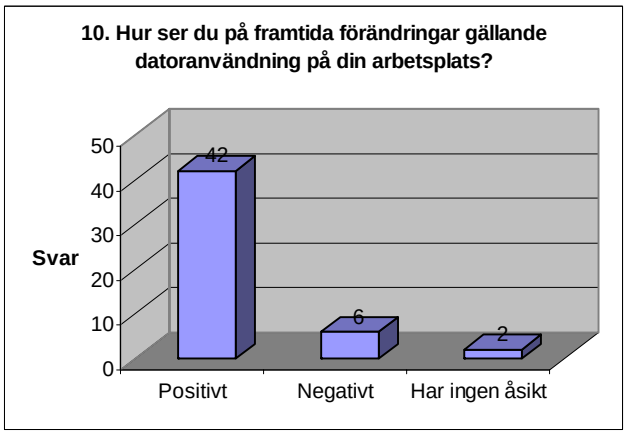
	26. Vet du vilket ansvar du har som anställd då du dagligen hanterar känslig information?		**26a. Om nej, anser du att arbetsplatsen varit dålig med att informera hur känslig information ska hanteras?**		**27. Känner du till de rättsliga följder som kan uppstå då en anställd läser en patientjournal där det inte finns någon vård-relation till patienten?**	
	Ja	Nej	Ja	Nej	Ja	Nej
25	x				x	
26	x				x	
27		x	x			x
28	x				x	
29	x				x	
30	x				x	
31	x				x	
32	x				x	
33	x				x	
34	x					x
35	x					x
36	x				x	
37	x		x		x	
38		x	x		x	
39	x				x	
40	x				x	
41	x			x	x	
42	x				x	
43	x				x	
44	x					
45	x				x	
46	x				x	
47	x				x	
48	x				x	
49	x				x	
50	x				x	

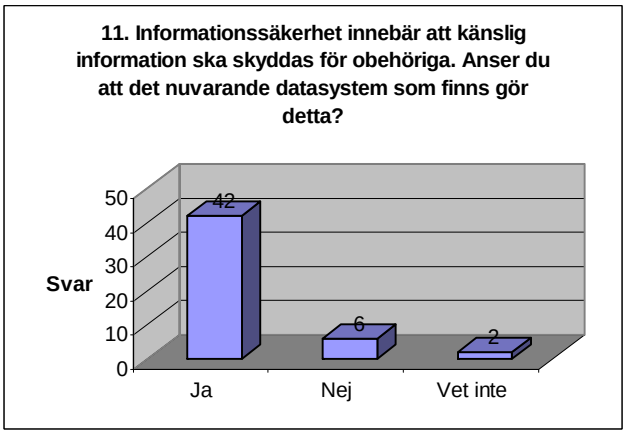
Bilaga 5 – Grafisk sammanställning av enkät

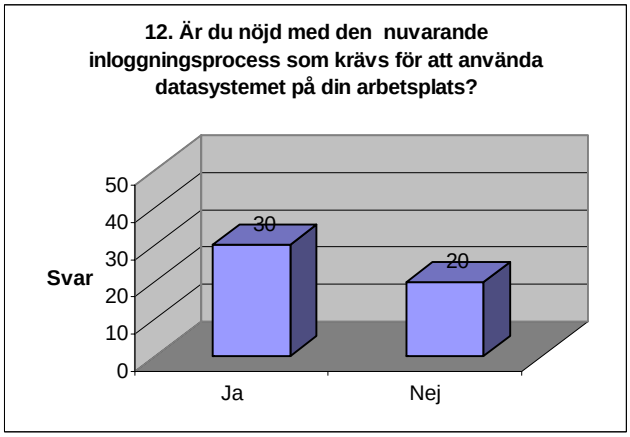




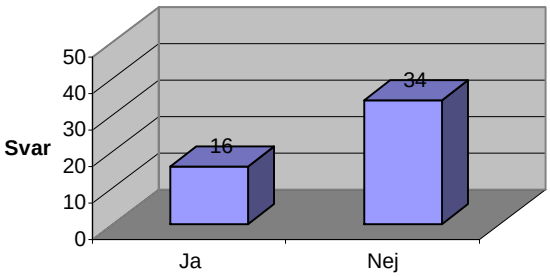




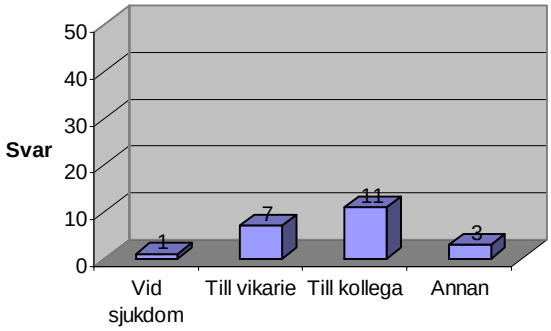




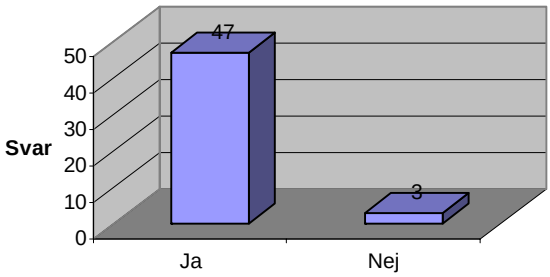
14. Har du någon gång lånat ut dina inloggningsuppgifter till någon annan på din arbetsplats?



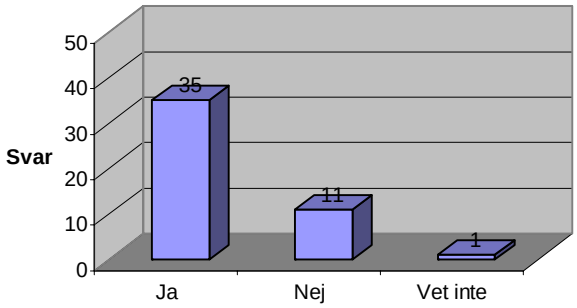
14a. Om ja, vid vilken situation?



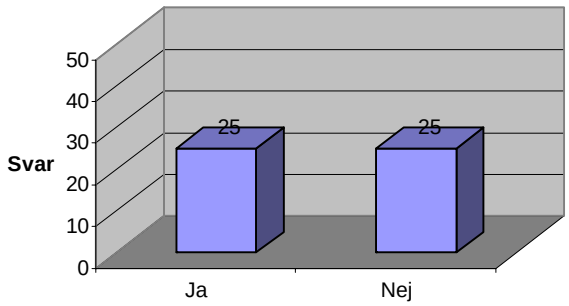
17. Om du sitter vid en och samma dator, behöver du ändå logga in på olika system för att nå den information du behöver?



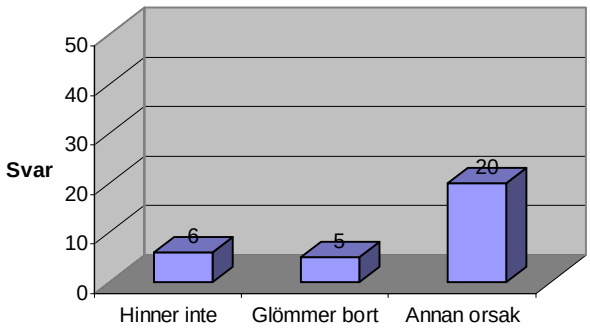
17a. Om ja, upplever du irritation över att du måste logga in på flera olika system?



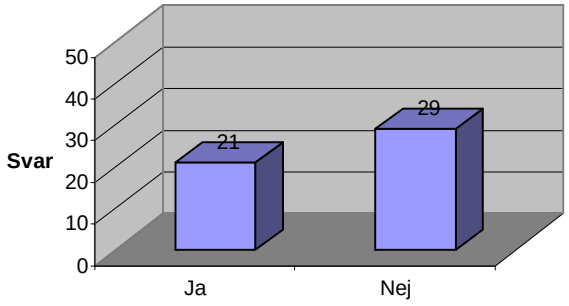
18. Loggar du alltid ut när du lämnar din dator obevakad?



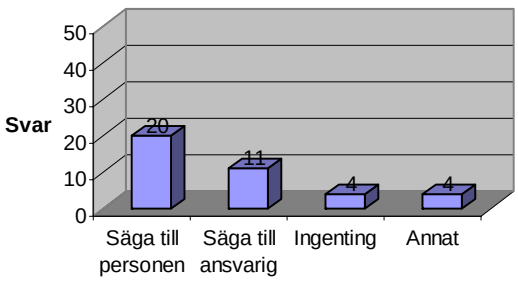
18a. Om nej, varför gör du inte det?



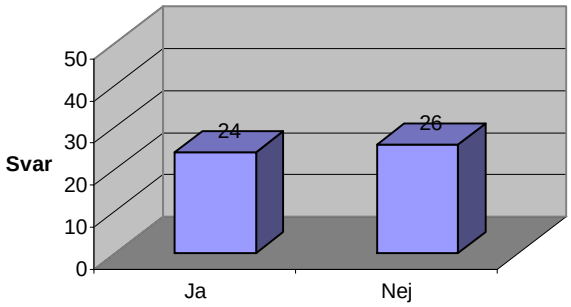
19. Anser du att andra kan använda din inloggade dator?



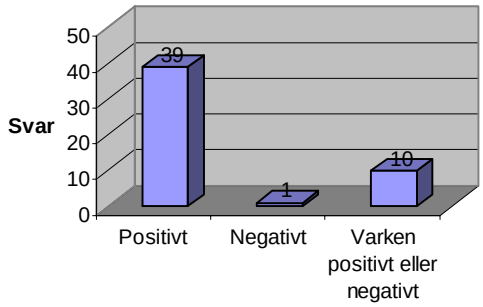
19a. Om nej, vad skulle du göra om du upptäckte eller misstänkte att någon annan varit inne i systemet på din inloggning?



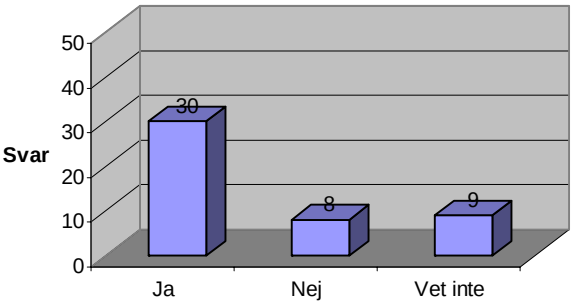
20. Känner du till de regler som gäller på din arbetsplats om du lämnar din dator obevakad?



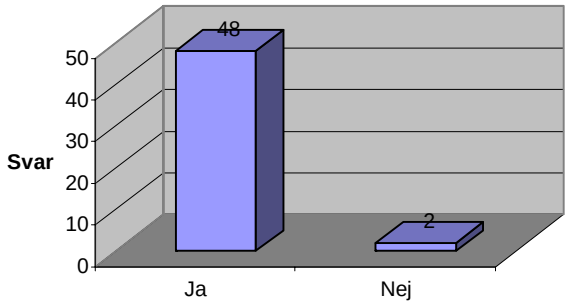
24. Hur ser du på användandet av elektroniska patientjournaler i ditt dagliga arbete?



25. Anser du att säkerheten kring elektroniska journaler är tillräcklig?



26. Vet du vilket ansvar du har som anställd då du dagligen hanterar känslig information?



27. Känner du till de rättsliga följder som kan uppstå då en anställd läser en patientjournal där det inte finns någon vårdrelation till patienten?