Informationssäkerhet i datorjournal

- en studie med användaren i fokus

(HS-IDA-EA-02-303)

Lena Ask (a99lenas@student.his.se)

Institutionen för datavetenskap
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Examensarbete på det systemvetenskapliga programmet under vårterminen 2002.

Handledare: Susanne Kjernald

Informationssäkerhet i datorjournal

- en studie med användaren i fokus

Examensrapport inlämnad av Lena Ask till Högskolan i Skövde, för Kandidatexamen (B.Sc.) vid Institutionen för Datavetenskap.

[2002-06-07]

Härmed intygas att allt material i denna rapport, vilket inte är mitt eget, har blivit tydligt identifierat och att inget material är inkluderat som tidigare använts för erhållande av annan examen.

Signerat: _____

Informationssäkerhet i datorjournal

- en studie med användaren i fokus

Lena Ask (a99lenas@student.his.se)

Sammanfattning

Inom vårdområdet hanteras en stor mängd känslig information och den bör finnas tillgänglig utan organisatoriska hinder. Många vårdanställda får snabbare och enklare tillgång till information genom informationsteknik (IT), men IT ställer även nya krav på medvetandet om informationssäkerhet.

Den i detta arbete studerade litteraturen menar att användarna är den största orsaken till att brister uppkommer i informationssäkerheten. Det kan bland annat förebyggas genom upprättande av informationssäkerhetspolicy samt genom att ge information till och utbilda användaren vid införande av informationssystem.

Syftet med arbetet var att fastställa hur användare av datorjournaler påverkas av kraven på informationssäkerhet och hur användarna påverkar informationssäkerheten. Vidare var syftet att ta reda på om de rekommendationer som Datainspektionen gett ut efterföljs av användarna. Observationer och intervjuer med vårdpersonal har legat till grund för att uppnå arbetets resultat. Resultatet av observationerna och intervjuerna visar att användaren fortfarande bidrar till att det finns brister i informationssäkerheten genom att in- och utloggningsfunktionen inte stödjer personalens arbetssätt. Resultatet visar också en tydlig tendens till att information och utbildning om informationssäkerhet bör ges regelbundet till användarna för att en medvetenhet om informationssäkerhet ska uppnås. Personalen bör även få möjlighet att diskutera och repetera handhavande av datorjournalsystem samt hantering av känslig information.

Nyckelord: informationssäkerhet, datorjournal, användare, säkerhet

Förord

Denna rapport är i första hand avsedd för att redogöra mitt examensarbete inom informationssystemsutveckling. Rapporten behandlar en studie, vars syfte är att studera hur användare påverkas av kraven på informationssäkerhet och hur användarna själva påverkar informationssäkerheten.

Att arbeta med studien och rapporten har varit intressant och stimulerande genom de olika kontakter som undertecknad fått med de personer som på ett eller annat sätt medverkat i studien. Det är flera personer som jag skulle vilja tacka för det stöd jag fått under examensarbetet. Först, vill jag rikta ett speciellt tack till min handledare, Susanne Kjernald, Högskolan i Skövde, vars handledning, kommentarer och förändringsförslag har varit till stor hjälp under arbetet. Sedan vill jag tacka all personal, som medverkat i studien samt Ida Noppa, samordnare för IT-utveckling, Skaraborgs Sjukhus IT för de kontakter som hon bidragit med. Jag vill också ge ett stort tack till min vän och kollega, Ann-Sofie Kvist, för hennes råd och stöd med arbetet. Slutligen, vill jag tacka min familj, min sambo Mikael och mina kära barn Julia och Joel, för deras stöd under tiden jag studerat vid det Systemvetenskapliga programmet på Högskolan i Skövde.

Skövde, juni 2002

Lena Ask

Innehållsförteckning

1 Inledning

Hälso- och sjukvården är i ett skede av stora förändringar. De ekonomiska och demografiska förutsättningarna förändras. Nya vårdformer och medicinsk teknik tillkommer. Trots detta har datateknikens intåg i vården varit långsam. Det beror dels på sjukvårdens komplexitet vad gäller arbetsformer och organisation, men även den konservatism som utmärker sjukvården (Hälso- och sjukvårdsinstitutet, 1998).

Trots den långsamma utvecklingen påverkar informationsteknologi (IT) snart alla verksamheter i samhället och då även hälso- och sjukvården. Tekniken kan förbättra och underlätta vårddokumentation, vårdinformation och beslutsfattande inom vårdområdet. På kort sikt leder ITs intåg i vården till ökade kostnader men i ett längre perspektiv kan det leda till tidsbesparingar och då också kostnadsbesparingar parallellt med ökad vårdkvalité (Collste, 1997).

Medicinsk informatik (MI) handlar enligt Petersson och Rydmark (1996) om informationstillämpning och användning av IT inom hälso- och sjukvårdens utövande, utbildning och medicinsk forskning. Läran om olika sätt att definiera, samla in, organisera, lagra och analysera samt presentera medicinska, vårdmässiga, administrativa och ekonomiska data ses som MI.

Användning av vårdinformationssystem växer konstant i Europa enligt Bourka, Polemi och Koutsouris (2001) eftersom systemen kraftigt ökar informationsutbytet. De gör det lättare att tillhandahålla vårdservice till invånarna på ett mer lämpligt, effektivt och ekonomiskt sätt. Elektronisk kommunikation introducerar viktiga säkerhetsproblem, vilka skall sättas i samband med den komplexa, känsliga och kritiska vårdrelaterade datan, som skall hanteras på ett lämpligt sätt på alla tänkbara nivåer (Bourka m fl., 2001).

Vad som krävs av hälso- och sjukvården är enligt Lagerlund (1999) att alla insatser optimeras och att kunskap och information finns tillgänglig utan organisatoriska hinder. Rätt åtgärd ska kunna sättas in på rätt vårdnivå vid rätt tidpunkt. Alla åtgärder måste dokumenteras så att kvalitetssäkring hela tiden kan äga rum (Lagerlund, 1999). En tredjedel av hälso- och sjukvårdenhets resurser läggs på hantering av patientrelaterad information och administration. Till största delen utförs administrationen med hjälp av datorstöd (Dahlin & Arnesjö, 1996).

Informationsteknik (IT) har givit många vårdanställda snabbare och enklare tillgång till information, men IT ställer även nya krav på säkerhetsmedvetandet (Lagerlund, 1999). Stora mängder information hanteras inom hälso- och sjukvården och en stor del av den är karaktäriserad som känslig. Användningen av datorer ökar vid ökad informationshantering vilket ger tillgång till lagrad information på ett sätt som tidigare inte varit möjligt (Hälso- och sjukvårdsinstitutet, 1996; Lagerlund, 1999; Dahlin & Arnesjö, 1996).

Brister i ansvarsfördelning, organisation och kunskap hos personalen är den största risken med ett fungerande IT-stöd vilket har visat sig i hot och riskanalyser. Det är även den egna personalen som är den största risken för en medveten felaktig hantering av IT-stödet. Samtidigt är det den interna personalen som begår fler brott än personer utifrån som gör intrång i systemen.

Några av de områden och begrepp som berörs i detta arbete beskrivs kort nedan för att ge ett underlag till problemområdet.

Den medicinska *pappersjournalen* består av tre huvuddelar enligt Gratte (1996) vilka är en patientadministrativ- en klinisk- och en laboratoriedel. En välskriven journal är ett arbetsredskap och kommunikationsmedium för sjukvårdspersonal som utreder, behandlar och vårdar patienter.

Enligt Gratte (1996) skall det i stort sett finnas liknande information i *datorjournalen* som i en pappersjournal. Förutom funktioner som underlättar att hitta och läsa vad som finns lagrat i journalen brukar det finnas rutiner för att förenkla hantering av laboratorieprover, läkemedel, remisser, sjukskrivningar, intyg och annan korrespondens. Andra viktiga funktioner i en datorjournal är arkivering, sekretess, systemunderhåll och rapportframtagning (Gratte, 1996). Det övergripande syftet enligt Dahlin och Arnesjö (1996) som journalen har är att underlätta och stödja att patienten får en god och säker vård, vilket förutsätter att journaldatan är tillförlitlig och tillgänglig när den behövs i vården och begriplig för vårdgivarna.

Informationssäkerhet kan sammanfattas med att riktig information ska komma till rätt person vid rätt plats och vid rätt tillfälle (Västra Götalandsregionen, 2000). Lagerlund (1997) menar att varje användare ska tilldelas rätt behörighet och få tillgång till rätt information vid rätt tid och plats. De som inte har rättighet till systemet ska inte kunna komma åt informationen. Det ska synas vem som skapat informationen och informationen ska skyddas mot förändring och förvanskning. Oberoende av om informationen hanteras manuellt eller med hjälp av en dator är lagstiftningen den samma (Lagerlund, 1997). Några grundläggande funktioner för att säkerställa informationssäkerhet är enligt Björner (1999):

- Autentisering; Kontroll av uppgiven identitet
- Behörighetstilldelning; Fastställande av åtkomsträttigheter
- Sekretess eller konfidentialitet; Skydd av information mot otillbörlig insyn
- Integritet; Skydd av information mot oönskad förändring, påverkan eller insyn
- Oavvislighet; Skydd mot att avsändare eller mottagare av information i efterhand kan förneka åtgärd eller kännedom om åtgärd
- Spårbarhet; Möjlighet att kunna spåra åtgärder och händelser till en viss användare och på detta sätt kunna hålla denne ansvarig för sina handlingar.

Hälso- och sjukvårdens informationshantering styrs av flera *lagar*. De ur säkerhetssynpunkt viktigaste lagarna är patientjournal-, sekretess-, personuppgifts-, hälso- och sjukvårds- och vårdregisterlagen.

Enligt Faulkner (2000) bör *användare* som grupperas ha ett likartat beteendemönster med systemet och deras användarkrav bör då vara ungefär de samma. Användare som har mer än en funktion i organisationen kan grupperas i mer än en slutanvändareklass. Det finns enligt Faulkner (2000) fyra olika klasser av slutanvändare som behöver identifieras; direkt-, indirekt-, fjärr- och supportanvändare.

Utifrån dessa bakgrundsområden och begrepp har arbetets problemprecisering tagits fram, vilket beskrivs i efterföljande kapitel. Vidare beskrivs arbetets genomförande, de viktigaste resultaten och slutsatserna och slutligen hur rapporten är uppbyggd.

1.1 Problem

Att hantera information i datorjournaler kräver en god läsbarhet och lätthet att registrera och ta ut patientdata i det dagliga arbetet (Dahlin & Arnesjö, 1996). Enligt Lagerlund (1999) vet vårdpersonal sedan tidigare att känslig information skall skyddas mot insyn, otillbörlig åtkomst och att obehöriga inte skall kunna ändra i informationen. Trots det finns det hos många vårdanställda en osäkerhet om vart gränserna går för vad som är tillåtet i den informationshantering de utför.

Utifrån rekommendationer från Datainspektionen (1998) till registeransvariga inom hälso- och sjukvården och de grundläggande funktionerna för att säkerställa informationssäkerhet, är det betydelsefullt att studera huruvida de efterföljs av användaren. Eftersom användaren står för de största riskerna i informationssäkerhet enligt flera rapporter (Furnell, Gaunt, Holben, Snaders, Stockel, & Warren, 1996; Lagerlund, 1999; Furnell, Dowland, Illingworth, & Reynolds, 2000) är syftet med arbetet delvis att kunna studera om situationen är densamma eller om det skett någon förändring till det bättre angående de risker som användaren utgör inom hälso- och sjukvården. Arbetets problemprecisering är :

- *Hur påverkas användaren av kraven på informationssäkerhet i datorjournaler?*
- *Hur påverkar användaren informationssäkerheten i datorjournaler?*

Det tillvägagångssätt som problemet angripits på beskrivs kort nedan.

1.2 Arbetes genomförande

Arbetet med att genomföra studien har skett genom att litteratur har studerats för att få förståelse för det aktuella problemområdet. Vidare har observationer och intervjuer genomförts med personal på ett sjukhus i mellersta Sverige vilket var lämpligt för att erhålla svar på den problemprecisering som arbetet utgår ifrån. Observationerna varade under tre dagar på tre olika platser inom samma enhet. Under observationerna studerades olika händelser och skeenden vid datoranvändning. Dessa var kategoriserade i ett observationsschema. Fyra användare från observationerna och en systemadministratör valdes ut för att delta i intervjuerna. Intervjuerna bandades, skrevs rent och sändes åter till respondenterna för kontroll. Materialet sammanställdes och analyserades vilket resulterade i några av nedanstående slutsatser.

1.3 De viktigaste resultaten och slutsatserna

Resultatet av observationerna och intervjuerna visar att *användaren påverkar* informationssäkerheten, genom att: in- och utloggningsfunktionen, att de exempelvis inte loggar ut ur systemen på ett korrekt sätt och att de använder varandras behörighet och identitet. Resultaten tyder också på att användarna behöver ytterligare utbildning och information om informationssäkerhet. Detta för att användarna ska erhålla en medvetenhet om informationssäkerhet, vilket är viktigt för att uppnå förtroende från patienterna. Utbildning och information bör därför genomföras kontinuerligt för att ge det stöd som användarna behöver. Personalen bör även få möjlighet att diskutera och

repetera handhavande av datorjournalsystem samt andra system personalen använder sig av i arbetet.

Resultaten visar på att *användarna påverkas* av informationssäkerheten på olika sätt genom att in- och utloggningsfunktionen inte är anpassad efter det arbetssätt som personalen har. Detta eftersom in- och utloggningen tar för mycket tid i anspråk. Vidare visar resultaten att användarna har många samtidiga arbetsuppgifter, exempelvis att telefoner ringer, patienter kallar och kollegor kommer för att få råd. Att personalen sedan blir störda av olika ljud när de ska registrera information är även det en faktor som behöver tas i beaktning för att inte datakvaliteten ska påverkas. Dessa problem kan i längden medföra att användarna känner sig stressade, vilket påverkar användarna själva men även datakvaliteten.

Vidare påverkas användarna genom att system som hanterar känslig information bör loggas. Användare bör få information och vetskap om varför och vilken data som sparas i loggfilen samt vilka rutiner som finns för hantering och kontroll av loggfilen.

Resultatet tyder slutligen på att användarna anser att tillgängligheten till patientinformation har ökat sedan den datoriserade patientjournalen infördes och att anteckningar inte tar längre tid att föra än vid faktasammanställning i pappersjournal.

1.4 Rapportens uppbyggnad

Inledningsvis (kapitel 2) ges en utförligare beskrivning av det område som berörs av arbetet där dels den pappersbaserade- och den datorbaserade patientjournalen förklaras. Vidare beskrivs den medicinska organisationskulturen och datorjournalens integrering med andra system. Informationssäkerhet förklaras sedan ur ett vad och hur perspektiv, där olika funktioner för att säkerställa informationssäkerhet tas upp i enskilda delar. Slutligen ges en förklaring till begreppet användare och faktorer som kan påverka informationssäkerheten.

I kapitel 3 beskrivs problemområde och det preciserade problem som arbetet inriktar sig på. De avgränsningar som gäller för arbetet och det förväntade resultatet tas även upp under det här kapitlet.

I kapitel 4 återges undersökningens upplägg och genomförande där de möjliga metodval som finns för arbetet och de valda metoderna, observation och intervju, tas upp. Fortsättningsvis berörs den undersökningsgrupp, arbetets upplägg, förberedelser och genomförande av observationer och intervjuer. Slutligen diskuteras de erfarenheter och den värdering som gjorts från observationerna och intervjuerna.

Kapitel 5 presenterar de resultat som kommit fram i studien genom en sammanfattning av det material som framkommit under observationer och intervjuer samt en analys av materialet.

I kapitel 6 återges de slutsatser som framkommit utifrån den problemprecisering som finns för arbetet.

Slutligen, under kapitel 7, förs en diskussion kring arbetets resultat, de erfarenheter som gjorts och en kritisk granskning av det egna arbetet. Vidare diskuteras förslag på fortsatt arbete.

2 Bakgrund

I kapitlet ges en bakgrund till problemområdet för att ge underlag och förståelse för vilka olika delar som berörs i detta arbete. Patientjournal och datorjournal beskrivs kortfattat för att få en bild av vilka delar som en journal ska stödja och innehålla. Vidare beskrivs varför utveckling av informationssystem inom hälso- och sjukvården kan tyckas vara svår att genomföra. Arbetet berör till stor del informationssäkerhet vilket beskrivs ur ett vad- och hur-perspektiv. De lagar som berörs vid hantering av patientinformation presenteras kort i kapitlet. Slutligen beskrivs olika slutanvändar-grupper av informationssystem och faktorer som berör informationssäkerhet.

2.1 Patientjournal

Nedan beskrivs patientjournalen kortfattat och en kort redogörelse görs av utvecklingen av datorjournal inom sjukvården och vad som omfattas av en datorjournal.

2.1.1 Pappersbaserad patientjournal

Dahlin och Ljungqvist (1996 s.13) definierar en patientjournal som ”samtlig information som registreras i samband med kontakter mellan patient och vårdgivare.”

Med journal avsågs ursprungligen en enkel liggare som innehöll patientens namn, datum för inskrivning och utskrivning samt eventuell diagnos. Patientjournalen fyller flera olika funktioner förutom att innehålla informationen om patienten. En välskriven journal är ett arbetsredskap och kommunikationsmedium för sjukvårdspersonal som utreder, behandlar och vårdar patienter. Patientjournalen ger grunden för såväl medicinsk, ekonomisk som administrativ statistik och dokumenterar kunskap och erfarenheter vilka utgör en del av den växande kunskapen inom hälsoområdet (Gratte, 1996).

Enligt Gratte (1996) är det generella användningsområdet för journalen den enskilde vårdgivarens patientknutna minnesanteckningar (anamnes-, undersöknings- och åtgärdsanteckningar). Dessa är ett underlag som redovisar en diagnostik och omvårdnadsprocess, ofta i kontakt med andra vårdgivare. Kontakten med andra vårdgivare ger ett behov av ett gemensamt språkbruk (termer, koder och strukturer), ett koncept för kommunikationen och överföring av information mellan olika vårdenheter eller delar av större vårdenheter.

Gratte (1996) menar att patientjournalen kan användas som ett juridiskt dokument. Därför reglerar patientjournallagen rättsligt vad journalen ska innehålla, hur den ska hanteras, vilka personalkategorier som ska föra journal och så vidare. Lagen stärker patientens ställning i vården och markerar dess rätt till god och säker vård. Patientjournallagen är teknikneutral. Den gäller både för manuell och datorstödd journalföring. Patientjournalen skall även innehålla information för patienten vilket är lätt att glömma bort. Journalen som ett juridiskt dokument innebär att det ska vara möjligt att i efterhand utreda om något misstag begåtts. Journalen skall lätt och snabbt kunna läsas för att komma till användning, vilket kanske är den viktigaste egenskapen hos en bra journal (Gratte, 1996).

I en medicinsk journal på papper finns tre huvuddelar enligt Gratte (1996):

- En patientadministrativ del med uppgifter om vårdform, datum för in- och utskrivning samt diagnos.
- En klinisk del som innehåller patientens sjukdomshistoria, den så kallade anamnesen, resultat från kroppsundersökningen, status samt dag- eller besöksanteckningar.
- En laboratoriedel som innehåller resultat från undersökningar utförda vid olika laboratorier.

Dahlin och Arnesjö (1996) anser att pappersjournalen ger många problem och några av dem är att: arkiveringen är utrymmes- och personkrävande och därmed blir dyr; informationen går ofta inte att använda för verksamhetsuppföljning; tillgängligheten är låg och sekretessen är en känslig del av pappersjournalen. Trots detta anses pappersjournalen som mer användarvänlig än de nuvarande datorjournalerna genom sin bättre överskådlighet, kronologiska struktur och bläddерbarhet (Dahlin & Arnesjö, 1996).

2.1.2 Datorbaserad patientjournal

På 1950-talet utvecklades enligt Karlberg och Arnesjö (1997) de första datorbaserade vårdinformationssystemen och datorjournalen var det första systemet som utvecklades. På 60-talet gjordes de första datoriseringsförsöken i Sverige, på Serafimerlasarettet i Stockholm, för att skapa ett ”datamaskinellt” system för patientvård. Detta system skulle följa patienten och dennes väg genom sjukhuset, ett datasystem uppbyggt kring patientens problem som även skulle tillgodose forskning. Försök med heltäckande journaler inom primärvården genomfördes under 1983-84, för att skapa stöd för verksamhetsutvecklig och studera de mervärden som datorjournalen ger. Under 1990-talet blev datorjournalen accepterad i primärvården. På grund av sjukhusinformationens komplexitet har utvecklingen gått långsammare på landets sjukhus. Under 1996 hade 85% av vårdcentralerna och 15% av sjukhusen datoriserade journalsystem (Karlberg & Arnesjö, 1997).

Enligt O. Landgren (personlig kontakt, 12 april, 2002) är datorjournalsystemen så gott som utbyggda vid vissa sjukhus i Sverige idag. Med så gott som utbyggda menas att det kan saknas datorjournalsystem vid ett par kliniker inom ett och samma sjukhus. För övrigt är pappersjournalen ersatt med datorjournal inom dessa sjukhus. Användandet av datorjournal varierar dock mellan olika sjukhus i landet, vissa sjukhus har endast påbörjat ett införande av datorjournalsystem medan andra sjukhus är så gott som datoriserade vad gäller journalhantering.

Enligt Gratte (1996) skall det i stort sett finnas liknande information i datorjournalen som i en pappersjournal. Förutom funktioner som underlättar att hitta och läsa vad som finns lagrat i journalen brukar det finnas rutiner för att förenkla hantering av laboratorieprover, läkemedel, remisser, sjukskrivningar, intyg och annan korrespondens. Andra viktiga funktioner i en datorjournal är arkivering, sekretess, systemunderhåll och rapportframtagning (Gratte, 1996).

Petersson och Rydmark (1996, s.14) anser att ”Med datorjournal avses information om patienten lagrad på datormedium med journaltext som är uppbyggd kring sökbara begrepp.” I patientjournalen registreras data av olika slag. Journalen är navet i

patientdokumentationen och datorjournalsystemet ska effektivt och integrerat stödja den informationshantering som är kopplad till patienten (Petersson & Rydmark, 1996).

Dahlin och Arnesjö (1996) menar att journalen har många syften och användningsområden eftersom den beskriver vårdprocessen i vårdkedjan för de enskilda patienterna. Det övergripande syftet som journalen har är att underlätta och stödja att patienten får god och säker vård, vilket förutsätter att journaldata är tillförlitliga och tillgängliga när de behövs i vården samt begripliga för vårdgivarna.

Den datorbaserade patientjournalen bör därför enligt Dahlin och Arnesjö (1996) vara:

- Ett kontinuerligt uppdaterat, lättanvänt och säkert arbetsinstrument i vården.
- En korrekt informationskälla (datasäkerhet).
- Ett juridiskt hållbart dokument (laglighet).
- Ett instrument för metodologisk, kvalitativ och kvantitativ uppföljning och utveckling jämte ekonomisk och administrativ planering av verksamheten.
- Ett instrument för utbildning.

Karlberg och Arensjö (1997) anser på liknande sätt att informationen som genereras i olika hälsokartläggningar och i vården av de enskilda patienterna skall kunna innefattas av ett vårdinformationssystem. Systemen skall underlätta och stödja förebyggande insatser. Därför måste data vara tillförlitlig, förståelig och tillgänglig (Karlberg & Arnesjö, 1997).

Nilsson (1997) anser att med gemensam dokumentation i en datorbaserad patientjournal, som beskriver patientens tillstånd, problem, samtliga insatta åtgärder samt hälsa och välbefinnande, ges möjlighet att utvärdera vården från ett helhetsperspektiv. Det är viktigt att samtliga personalkategoriers insatser kan beskrivas så att det blir möjligt att utvärdera och ta fram resultat från vården (Nilsson, 1997).

Några av de mervärden som datorjournalen har i jämförelse med pappersjournalen är enligt Dahlin och Arnesjö (1996) följande:

- Hög tillgänglighet för vårdgivaren.
- Varierande presentationsmöjligheter.
- Varierande datafångst.
- Effektiv datalagring med snabb access.
- Stor sökbarhet.
- Strukturering enligt användarens krav (källorientering, problemorientering, formulärorientering).
- Högre datasekretess.
- Möjlighet för verksamhetsstyrning genom kombinerad medicinsk och ekonomisk redovisning.
- Möjlighet till kvalitetsutveckling av verksamheten.
- Möjlighet till kopplade beslutsstödsfunktioner.

- Möjlighet till kommunikation.
- Möjlighet att hämta och lägga in data direkt från andra databärare (andra system, ”smart cards” eller patientkort).

Dahlin och Arnesjö (1996) menar vidare att om alla teoretiska fördelar med datorjournalen skall förverkligas krävs en öppenhet att ta till sig ny teknik samt att informationen och informationsöverföringen standardiseras. Datorjournalen kommer då att bli mer användarvänlig och användbar samt ge möjlighet till kommunikation mellan olika system och att bli certifierad, det vill säga kvalitetstestad och godkänd. Kvaliteten i datorjournalen beror dock mest på vilka patientdata vårdgivarna registrerar samt på hur och vilka krav vårdgivarna ställer på datorstödets utformning (Dahlin & Arnesjö, 1996).

Sågänger och Utbult (1998) anser att några fördelar med den datoriserade journalen är att den alltid är rätt sorterad, färre papper kan tappas bort och att det går betydligt lättare att ta fram statistik för uppföljning och beslutsunderlag. Dessutom ger den en högre säkerhet än pappersjournalen eftersom den har ett bra skydd mot intrång.

Vid utformning av datoriserade patientjournalsystem finns det enligt Metzer och Teich (1995) några designförutsättningar som utvecklarna skall ha i åtanke. Dessa är att patientjournalsystem måste:

- vara tillgängliga när användarna behöver dem för att kunna ge patientvård.
- vara tillgängliga när beslut om vård skall göras.
- tillåta snabb och värdefull access till information.
- designas för att passa aktuella patientvårdprocesser och arbetssituationer.
- vara enkla att använda så att de kräver ingen eller lite träning.

Metzer och Teich (1995) menar också att användarna skall ges direkt tillgång till hela systemet, vilket tar mindre tid och maximerar uppmuntran till att använda systemet. Vidare anser författarna att systemen är enklare att använda för personalen om terminologin är känd. För klinikapplikationer, menas det att den medicinska terminologin skall matcha de termer som människor använder i det praktiska arbetet. När personalen begär patientdata eller identifierar en tjänst som de behöver ska de välja ett begrepp som verkar rätt för dem att använda, och inte ett begrepp som krävs enbart för systemet (Metzger & Teich, 1995).

Punkterna ovan är inte specifikt just för patientjournalsystem utan är viktiga att tänka på inom all informationssystemsutveckling för att få ett system som stöder verksamheten och förenklar för användaren.

Några delar som är speciella vid utveckling av patientvårdssystem är enligt Schneider och Reed (1996) den medicinska kulturen och integrering med andra system.

2.1.3 Den medicinska organisationskulturen

Enligt Kajbjer och Lundmark (1997) omfattar hälso- och sjukvården flera typer av verksamheter, personalkategorier, medicinska specialiteter och hjälpmedel av teknisk art. Hälso- och sjukvården bedrivs även på olika sätt i olika länder där verksamheten

präglas av till exempel kultur, sociala förhållanden och undervisning inom vårdområdet. Dessutom är det enligt författarna besvärligt att beskriva patienter, sjukdomar, personal, behandlingar, och omvårdnad i begreppsmodeller (Kajbjer & Lundmark, 1997).

Leffler och Odelhög (2001) menar att IT-stöd inom sjukvården ingår i ett leverantörskoncept och de är ofta speciellt utformade för en viss medicinsk specialitet. Problem uppstår först när information ska återanvändas och när verksamheterna ska kommunicera med varandra. Så länge lösningarna liksom verksamheterna är isolerade uppstår inga problem. Bland annat olikheter mellan teknologi, systemstrukturer och begrepp kräver speciallösningar. Kajbjer och Lundmark (1997) beskriver det som öar av information med var sin egen teknisk, logisk och semantisk struktur. Då fler IT-stöd ska integreras ökar komplexiteten vilken blir allt svårare att hantera. För att minska komplexiteten behövs enligt Leffler och Odelhög (2001) en ökad standardisering inom hälso- och sjukvård.

Den medicinska personalen är enligt Schneider och Reed (1996) krävande kunder till IT-stöd. Medicin, som den för närvarande praktiseras, är både ett yrke och en vetenskap och datorsystem förväntas att stödja båda delar. Den medicinska personalens oberoende och praktiska sätt att arbeta har traditionellt omintetgjort ansträngningar för att använda systemteknologi (Schneider & Reed, 1996).

Leffler och Odelhög (2001) anser att det finns flera trögheter som kan sänka förnyelsetakten. Beslutsprocesserna vid förnyande är långa och förenat med formella upphandlingsregler vilka ofta är förknippade med stora beslut. Det kan även finnas inbyggda trögheter i organisationer då befintliga lösningar är dyra att byta eller förändra. Vidare kan trögheten bero på den komplexa systemstrukturen där det är svårt att foga in nya lösningar. Det är även bristande insikter hos personal inom vården om vilka tekniska potentialer som finns och utvecklingen inom verksamheten driver inte fram effektiva sätt att använda IT-stöd.

Alla dessa trögheter är enligt Leffler och Odelhög (2001) hämmande på förnyelsetakten. Mellan nuläget och de möjligheter IT kan ge uppstår det ett gap. Gapet behöver inte enbart vara fokuserat på befintlig teknikkunskap och hur den används ute i verksamheten utan det kan även relateras till befintlig användarkunskap och vilken kunskapsnivå IT-systemet förväntar sig av användaren. Då sådana gap uppstår innebär det att organisationer inte drar nytta av befintliga IT-lösningar på grund av bristande användarkompetens (Leffler & Odelhög, 2001).

De lagar som berörs vid hantering av personuppgifter inom hälso- och sjukvården gör att utvecklingen av system inom vården blir mer komplext. Om lagarna ändras så att exempelvis information kan skickas mellan olika avdelningar, kommuner och landsting skulle det underlätta och effektivisera arbetet för de vårdanställda.

2.1.4 Integrering med andra system

Enligt Kajbjer och Lundmark (1997) finns det flera exempel på hur den traditionella patientjournalen dokumenteras med hjälp av olika datorlösningar, mer eller mindre strukturerat. Det ställs samtidigt krav på att systemen skall kunna stödja hela vårdprocessen, från utredning till behandling och sedan uppföljning. Det vore önskvärt om informationen kunde delas mellan exempelvis kommun och landsting och vara tillgänglig för personal som behöver information under hela vårdprocessen.

Problemet är enligt Kajbjer och Lundmark (1997) att de olika system som finns inom vården inte kan kommunicera med varandra eller arbeta mot samma databas. Framförallt saknas gemensamma begreppsmodeller. I de olika systemen finns ingen gemensam uppfattning om de begrepp som finns inom hälso- och sjukvården och hur begreppen relaterar till varandra. Att det inte finns en gemensam begreppsmodell gör att det hos varje leverantör, användare och organisation, som utformar egna informationssystem, finns olika uppfattningar om begrepp och lösningar, vilket gör informationen inkonsistent. Inom flera verksamhetsområden, exempelvis inom bankväsendet, flyg, handel och frakt, har man uppnått gemensamma begrepp, modeller och standardisering. Detta har givit resultat i form av snabb, felfri och billig kommunikation mellan självständiga informationssystem. Inom hälso- och sjukvården har språk- och begreppsproblematiken gjort att standardiseringsprocessen tagit lång tid. Huvudsyftet med standardiseringsarbetet är att lösa de kommunikationsproblem som finns inom hälso- och sjukvården och göra det möjligt att utväxla patientrelaterad information mellan befintliga och framtida informationssystem. De framtagna standarderna skall inte begränsa vårdpersonalen i sitt yrkesutövande och inte inskränka deras möjligheter till att planera och dokumentera sitt arbete (Kajbjer & Lundmark, 1997).

Enligt Drazen (1996) är det tre företeelser som verkar klara inom datorjournalssystem ur ett framtida perspektiv. Behovet av datorjournalssystem kommer med tiden att öka och att framgångsrikt kunna implementera datorjournalssystem kommer att bli kritiskt när det byggs upp integrerade vårdsystem. Att stödja patientvård med informationssystem kommer att kräva enorma investeringar av kapital, uppmärksamhet av ledningen och organisationens tid (Drazen, 1996).

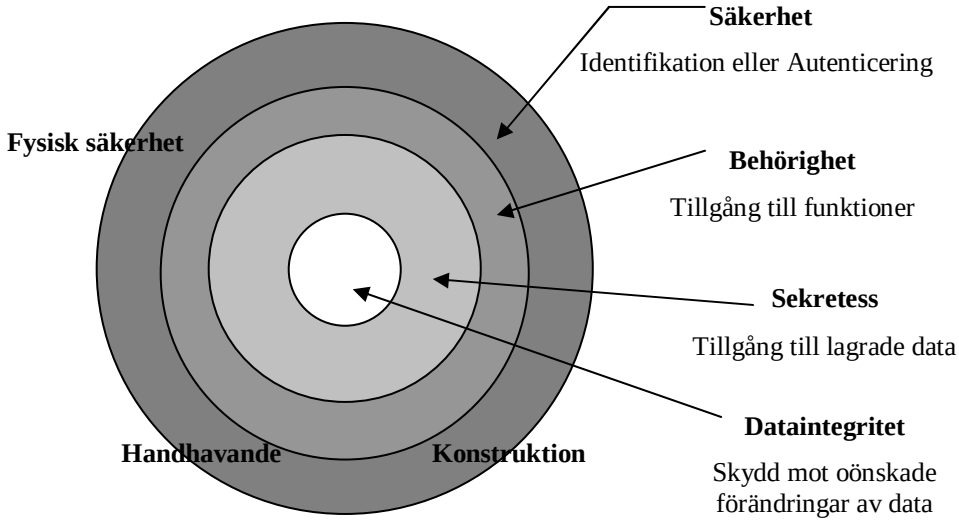
För att hälso- och sjukvården ska erhålla en snabb, felfri och billig kommunikation bör en standardisering ske, dels av de begrepp och dels av de strukturer som systemen byggs upp efter. Detta har exempelvis skett inom bankväsendet. Bankväsendet tar i likhet med vården dagligen hand om känslig information om personer där det skulle vara förödande om något gick fel vid hantering av information. Att enas om en begreppsstandard i likhet med den inom bankvärlden bör inte vara mer komplext än för andra verksamheter. Svårigheten inom hälso- och sjukvården är de lagar som berör informationshanteringen. Dessa bör korrigeras för att det ska vara möjligt att genomföra den informationshantering som efterfrågas. Att informationssystem som stödjer patientvården kräver enorma satsningar av kapital, verksamheters tid tillsammans med den tröghet som finns inom organisationen gör inte problemet mindre komplext.

Ytterligare krav på informationssystem inom vården är att känslig patientinformation ska behandlas på ett informationssäkert sätt. Detta beskrivs i nästkommande kapitel.

2.2 Informationssäkerhet

Information kommer från det latinska ordet *informare* som enligt Petersson och Rydmark (1996) betyder att utbilda, undervisa, forma. När det finns en mottagare till data och när denna ges en innebörd blir data till information. När information förstås och tillvaratas av mottagaren utgör den kunskap (Petersson & Rydmark, 1996; Alter, 1999; Avison & Fitzgerald, 1997).

Dahlin och Arnesjö (1996) anser att all information som är datorlagrad är sårbar och speciella åtgärder måste därför alltid vidtas för att säkra data. Vårdgivaren skall följa de lagar som gäller för informationshantering i hälso- och sjukvården, nämligen Sekretesslagen och Patientjournallagen. De delområden som bör uppmärksammas vid kvalitetsbedömning av datorjournalens datasäkerhet är säkerhet, behörighet, sekretess och dataintegritet. ”Skydd mot oönskad förändring av data”, vilket är datasäkerhetens kärna, fordrar många skyddsområden vilket framgår av figur 1.



Figur 1. Datasäkerhet för datoriserade patientjournaler

(Efter Dahlin & Arnesjö, 1996, s. 120)

Datasäkerhet för en patientjournal kräver enligt Dahlin och Arnesjö (1996) att data: inte förloras; kan komma i orätta händer; är tillgängliga när de behövs och är tillförlitliga. Datasäkerhet är enligt Nationalencyklopedin (2002) en samlingsterm för allt som rör säkerhet inom databehandling. Ordet datasäkerhet används vid handlingar som riktar sig mot data. Informationssäkerhet, som är den alternativa termen, inriktar sig på den information som data representerar och skyddsbehovet från det perspektivet (Nationalencyklopedin, 2002).

Björner (1999) menar att informationssäkerhet kan vara svårt att definiera för dem som arbetar inom hälso- och sjukvården. Säkerhet är ett självklart krav för allt som utförs inom vården och information i olika former är en nödvändig förutsättning för vårdpersonalens arbete. För att förankra begreppet informationssäkerhet bör VAD- och HUR-begreppen noga särskiljas. Att beskriva informationssäkerhet enligt Björner (1999, s.10) med hjälp av VAD: ”(…) handlar om saken eller frågan i sig själv utan att (…) snegla(…) på lösningar.” De begrepp som författaren avser handlar om IT-säkerhet utan att definiera eller förutsätta hur säkerheten åstadkoms. ”HUR handlar

om frågan när den på något sätt parats med en lösning.” (Björner, 1999, s.10). De begrepp som används vid beskrivning av lösningar på säkerhetsproblem är exempelvis behörighetsprofil, loggning, kryptering och digitalasignaturer (Björner, 1999).

I efterföljande kapitel beskrivs begreppet informationssäkerhet ur både ett vad- och ett hur-perspektiv, men ingen vikt kommer att läggas på att förklara rent tekniskt hur informationssäkerhet skall uppnås. De lagar som berör området informationssäkerhet inom hälso- och sjukvårdsområdet beskrivs även kort.

2.2.1 Vad är informationssäkerhet?

Nedan har en ansats gjorts till att förklara begreppet ur ett VAD perspektiv.

Lagerlund (1999, s.16) anser att ”Med informationssäkerhet menas den samlade effekten av åtgärder för att minimera risker som riktar sig mot informationens tillgänglighet, sekretess, riktighet och spårbarhet.” Lagerlund (1997); Barber och Davey (1996) beskriver dessa delar av informationssäkerheten som:

Tillgänglighet – De behöriga användarna skall få tillgång till de funktioner och den information som de behöver för att utföra sina arbetsuppgifter.

Sekretess – Patientjournalsystemen skall ha funktioner för kryptering av data och ha ett behörighetskontrollsystem som reglerar vilka användare som får tillgång till den lagrade datan.

Integritet – Dataintegritet, den lagrade datan skall inte kunna förändras på ett oönskat sätt. Personintegritet skyddar mot intrång i den personliga integriteten, genom de olika sätt som information om enskilda individer får lagras och registreras.

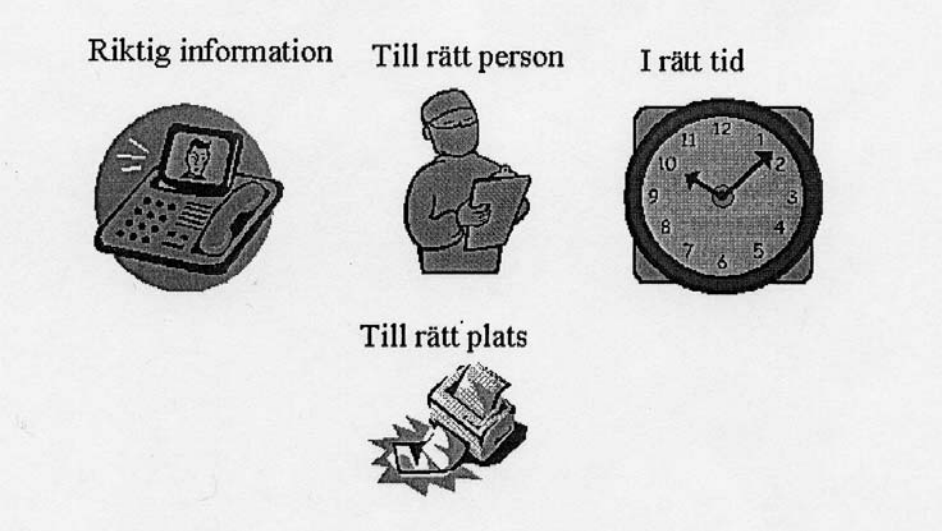
Spårbarhet – Funktioner för att följa upp användningen av systemet. Man skall kunna se på vilket sätt en användare utnyttjat systemets funktioner och den lagrade informationen.

Lagerlund (1997) menar vidare att varje användare ska tilldelas rätt behörighet och få tillgång till rätt information vid rätt tid och plats. De som inte har rättighet till systemet ska inte kunna komma åt informationen. Det ska synas vem som skapat informationen och informationen ska skyddas mot förändring och förvanskning. Oberoende av om informationen hanteras manuellt eller med hjälp av en dator är lagstiftningen den samma (Lagerlund, 1997).

Med informationssäkerhet menas enligt Informationssäkerhetspolicy från Västra Götalandsregionen (2000) att riktig information skall komma till rätt person vid rätt tid och till rätt plats (se figur 2).

- Riktig information innebär att man får rätt och oförvanskad information i tillräcklig omfattning för den givna situationen
- Rätt person innebär att utsedd roll vid en given situation får tillgång till information. En person kan tilldelas olika roller för olika situationer till exempel medborgare, politiker, läkare och så vidare.
- Rätt tid innebär att informationen skall erhållas vid den tidpunkt behovet uppstår.
- Rätt plats innebär att informationen skall finnas tillgänglig där den behövs.

I beskrivningarna av informationssäkerhet ovan nämns tillgänglighet till rätt och riktig information som ett viktigt argument. Ett annat är att de personer som skall få tillgång till informationen bara skall ta del av den om behov finns i arbetet med att vårda patienten. Slutligen skall personalen få tillgång till information när behov uppkommer och användarnas nyttjande av systemet skall kunna spåras.



Figur 2. Summering av informationskrav (Med tillstånd av Västra Götalandsregionen, 2000, s.1)

2.2.2 Lagar som påverkar persondatahantering

Hälso- och sjukvårdens informationshantering styrs av flera lagar. De ur säkerhetssynpunkt viktigaste lagarna beskrivs kort nedan.

Patientjournallag

Lagerlund (1997) anser att patientjournallagen uttrycker klart under vilka former sjukvården är skyldig att dokumentera. Enligt patientjournallagen räknas alla handlingar och anteckningar som innehåller uppgifter om patientens tillstånd och de åtgärder som genomförts och planeras till journalhandlingar. Skyldigheten som vårdgivaren har är att dokumentera och avgöra vilka uppgifter som skall dokumenteras (Lagerlund, 1997).

Patientjournallagen är teknikneutral, den gäller både för information på papper och vilket annat medium som helst exempelvis disketter eller röntgenfilm (Sjölenius, 1996). Patientjournallagen (SFS 1985:562) reglerar bland annat när en patientjournal skall föras, vilka personalkategorier som skall föra journal samt vilka uppgifter journalen skall innehålla. Reglerna är i princip desamma för både den offentliga och den privat drivna hälso- och sjukvården.

I 9 § anges enligt Sjölenius (1996) att var och en som för patientjournal ansvarar för sina uppgifter. Vidare står det att patientjournal ska föras vid vård, undersökning och behandling av patienter. Patientjournal skall föras för varje enskild patient och inte vara gemensam för flera patienter. Huvudregeln, § 3, säger att en patientjournal skall innehålla de uppgifter som behövs för en god och säker vård av patienten. Patientjournalen skall innehålla uppgift om patientens identitet, bakgrund till vården,

om ställd diagnos och vidtagna och planerade åtgärder. Den skall även innehålla uppgifter om vem som gjort anteckningar och när detta skedde (Sjölenius, 1996).

I patientjournallagen 7 § står det att: ”Varje journalhandling skall hanteras och förvaras så att obehöriga inte får tillgång till den.”

Ett led i hanteringen är rättelse av patientjournalen vilket regleras i 6 §. Detta får inte ske hur som helst utan det skall anges vem som gjort ändringen och när (Sjölenius, 1996).

I 16 § patientjournallagen föreskrivs att på begäran av en patient skall en journalhandling så snart som möjligt tillhandahållas honom för läsning eller avskrivning på stället eller i avskrift eller kopia. Om den private vårdgivaren vägrar patienten att ta del av sin journal skall ärendet omedelbart rapporteras till Socialstyrelsen för prövning. Det saknas regler för om någon annan än patienten själv vill ta del av uppgifter i en journal.

Sekretesslag

Sekretesslagen gäller för den offentliga hälso- och sjukvården. Genom lagen regleras gemensamt handlingsekretessen och tystnadsplikten. Med sekretess avses förbud att röja uppgifter, det gäller såväl muntliga uppgifter som att lämna ut en allmän handling, exempelvis patientjournal, eller att på något annat sätt yttra sig om hemlig uppgift (Sjölenius, 1996). Lagerlund (1997) beskriver att sekretesslagen anger vad som är sekretessbelagt och undantaget från den regel att myndigheters allmänna handlingar är offentliga.

All personal har tystnadsplikt om vad den vet om patienten. Enligt 7 kap 1§ sekretesslagen (SFS 1980:100) säger huvudregeln ”(…) att uppgift inom hälso- och sjukvården om enskilds hälsotillstånd eller andra personliga förhållanden kan lämnas ut endast om det står klart att den enskilde eller någon honom närstående inte lider men.”

Personuppgiftslag (PUL)

Personuppgiftslagen (SFS 1998:204) trädde i kraft den 24 oktober 1998. Den ersätter datalagen och reglerar behandling av personuppgifter (Datainspektionen, 1998).

Några av huvudpunkterna i personuppgiftslagen är enligt Datainspektionen (2000) att:

- Individer skall skyddas mot att deras personliga integritet kränks genom behandling av personuppgifter.
- PUL omfattar både automatiserad och manuell behandling av personuppgifter.
- Om det i en annan lag eller i en förordning finns bestämmelser som avviker med PUL, gäller de bestämmelserna istället.
- Vissa grundläggande krav finns på behandling av personuppgifter. Dessa krav innebär bland annat att personuppgifter får behandlas bara för särskilda, uttryckligt angivna och berättigade ändamål.
- Personuppgifter får bara behandlas om de uppfyller de krav ovan och att den registrerade lämnar sitt samtycke. Det finns undantag till denna regel.
- För behandling av känsliga uppgifter exempelvis hälsa och politisk åsikt gäller strängare regler.

- Den registrerade har rätt att ta del av information om behandling av personuppgifter som berör denne.

Vårdregisterlagen

Lagen om vårdregister (SFS 1998:544) trädde i kraft den 24 oktober 1998. Lagen reglerar all behandling av personuppgifter i vårdregister. Lagen avser vård enligt den definition på vård som finns i hälso- och sjukvårdslagen, tandvårdslagen, lagen om psykiatrisk vård, lagen om rättspsykiatrisk vård samt smittskyddslagen. I lagen om vårdregister finns inga övergångsbestämmelser, vilket har till följd att de register som avses omfattas av lagens bestämmelser (Datainspektionen, 1998).

Hälso- och sjukvårdslagen

I hälso- och sjukvårdslagen (SFS 1982:763) (HSL) stadgas bland annat i 2§ andra stycket att ”Vården skall ges med respekt för alla människors lika värde och för den enskilda människans värdighet.” I 2a § anges bland annat att ”Hälso- och sjukvården skall bedrivas så att den uppfyller kraven på en god vård. Det innebär att den skall särskilt (…) bygga på respekt för patientens självbestämmande och integritet (…). Vården skall så långt det är möjligt utformas och genomföras i samråd med patienten.” Av 3 § framgår att landstingen är skyldiga att erbjuda en god hälso- och sjukvård.

Dessa lagar måste beaktas vid informationshantering inom vården och de krav som bör uppmärksammas för att uppnå en informationssäker miljö beskrivs i kommande kapitel.

2.2.3 Hur uppnås informationssäkerhet?

Hur informationssäkerhet erhålls med hjälp av tekniska lösningar kommer här inte att beskrivas. Istället kommer tonvikten ligga på att förklara de olika delar som berör hur informationssäkerhet skall uppnås.

Björner (2000) har tagit fram några synpunkter på hur informationssäkerhet skall uppnås. I grunden måste hela organisationen veta vad som menas med informationssäkerhet, från användare till ledning. Ledningen måste känna engagemang och ansvar. När en informationssäkerhetspolicy antagits skall riktlinjer och strategier att arbeta efter tas fram. Slutligen läggs en säkerhetsplan fram som beskriver ett strukturerat arbetssätt. De säkerhetsrisker som kan uppstå vid användandet av IT-system bör prioriteras och nämnas ofta. Även utbildning i hur systemen ska användas bör genomföras kontinuerligt. Utbildning är den faktor som är viktigast för att system skall fungera på ett rätt och riktigt sätt. För att bygga ett säkerhetstänkande bland användarna bör utbildningen peka på de hot, risker och möjligheter som finns. Alla som använder systemet måste känna och veta att de har ett eget ansvar för det de gör och det de borde ha gjort. Vid val av säkerhetsnivå skall informationen klassificeras på hur integritetskänslig den är, hur åtkomlig den behöver vara och vilka eventuella hot som informationen kan utsättas för (Björner, 2000).

Enligt Dahlin och Arnesjö (1996) krävs det att varje vårdinrättning har en skriftlig informationspolicy som ska:

- Hänvisa till och ta fram de regler och lagar som gäller.
- Ge anvisningar för handläggning av patientinformation i olika situationer, speciellt i hur man skyddar och handskas med känslig patientinformation vad gäller insamling, registrering, användande, ändringar av grundkonceptet, kommunikation inom och utom enheten, förvaring och förstöring.
- Ge säkerhetsanvisningar för skydd av data mot missbruk, förstörelse eller stöld; det gäller också skydd och regler mot användning utom vid enskild patient-vårdgivarkontakt.
- Ge regler för skydd och för användning och tillgång till data (enbart den personal som behöver uppgifterna för att kunna fullgöra sitt arbete får ha terminalåtkomst till patientjournaluppgifter i registret; det hindrar inte att uppgifter ur registret lämnas ut med hjälp av automatisk databehandling eller på annat sätt efter sedvanlig sekretessprövning).

Enligt Lagerlund (1997) kan informationssäkerhetsarbetet organiseras på många sätt. De grundläggande och viktigaste delarna för att uppnå god säkerhet är kunnig personal och genomarbetade rutiner. På de olika nivåerna bör därför kontaktpersoner utses och informations- och utbildningsinsatser genomföras kontinuerligt. Lagerlund (1999) anser att det inte räcker med säkerhetsfunktioner i system och teknik utan det krävs ett strukturerat arbetssätt för säkerhetsarbetet i sin helhet.

Överstyrelsen för civilberedskap (ÖCB), (1993:242) föreskriver att ett samhällsviktigt datasystem, som utgör nödvändigt stöd för verksamhet av vikt för samhällets förmåga att fungera även under höjd beredskap, där information lagras eller bearbetas skall vara så konstruerat att det för att få tillgång till systemet krävs behörighetskontroll eller fysisk tillträdeskontroll. Beslut om tilldelad behörighet skall även dokumenteras. Dessa delar av datasystemet skall vara så konstruerade att det finns logg där det framgår vem som har använt systemet och när detta skett. I särskilda fall kan en logg ersättas med manuell registrering. I säkerhetsinstruktionen skall det anges hur tilldelning, uppdatering och uppföljning av behörighet till dessa datasystem skall ske. Vidare skall det anges hur datamedia tillhörande samhällsviktigt datasystem med för verksamheten nödvändig information skall skyddas mot obehörig åtkomst. Av säkerhetsinstruktionen skall även framgå vem som ansvarat för analys av loggar, i vilken omfattning analys skall ske och hur länge en logg skall sparas (ÖCB, 1993:242).

Några grundläggande funktioner för att säkerställa informationssäkerhet är enligt Björner (1999):

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

- Spårbarhet; möjlighet att kunna spåra de åtgärder och händelser till en viss användare och på detta sätt kunna hålla denne ansvarig för sina handlingar.

Funktionerna beskrivs mer utförligt i efterföljande kapitel.

2.2.4 Autentisering

För att åstadkomma en god informationssäkerhet är en säker identifiering av aktörerna i hälso- och sjukvården en förutsättning (Björner, 2000). Utan identifiering blir andra informationssäkerhetstjänster, såsom loggning och behörighetskontroll meningslösa. Autentisering används i vårdprocessen vid identifiering av patienter, vårdgivare, organisatorisk enhet, verksamhetsfunktion och systemobjekt. Olika informationssäkerhetsnivåer finns vid identifiering av aktörerna (Björner, 2000).

Det finns enligt Furnell, Dowland, Illingworth och Reynolds (2000) tre approacher för att identifiera personer nämligen att använda sig av:

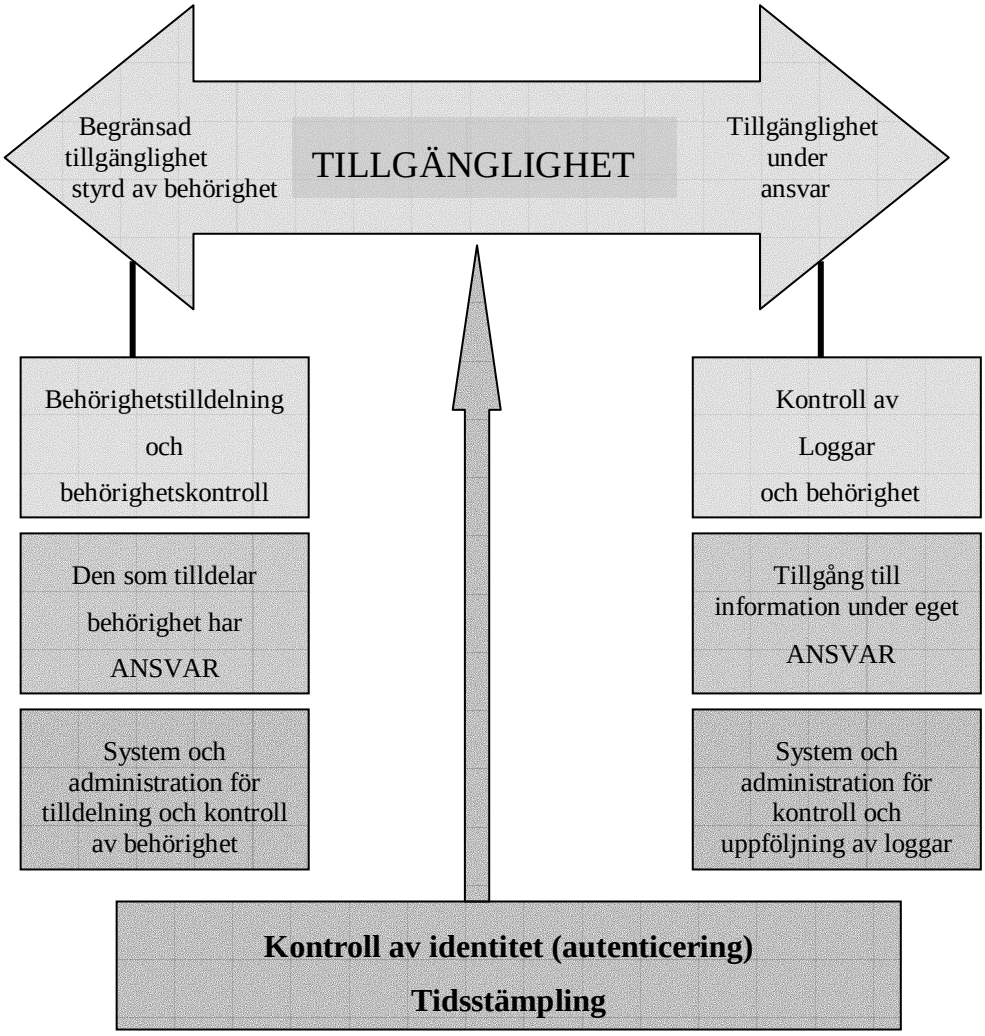
- något som personen vet; exempelvis ett lösenord eller en PIN-kod.
- något som personen har; exempelvis ett kort, legitimation.
- något som personen är; exempelvis fingeravtryck eller iris-scanning.

2.2.5 Behörighetstilldelning

Vilka som ska få tillgång till patientinformation kan lösas genom två olika modeller, enligt figur 3 (Lagerlund, 1999):

- Behörighetsmodellen: efter reglering av åtkomst av tillgänglig information för användaren.
- Loggningsmodellen: under användarens eget ansvar ges fritt tillträde till information som kan efterkontrolleras genom loggning.

Att välja enbart loggningsmodellen kan minska trovärdigheten hos sjukvårdens informationshantering, medan att enbart ha en renodlad behörighetsmodell kan kräva en omfattande administration som troligtvis kan falla på grund av detta. I olika lagar regleras tillgängligheten, främst i Sekretess- och Patientlagen. I Hälso- och sjukvårdslagen, Lagen om yrkesverksamhet på hälso- och sjukvårdens område och Vårdregisterlagen finns det regleringar av tillgängligheten som ska beaktas. Dessa lagar har det gemensamt att endast den som deltar i vården av en patient får ta del av dokumentationen om patienten (Lagerlund, 1999).



Figur 3. Balansgång mellan behörighets- och loggningsmodellen (Efter Björner, 2000, s.37)

En identifierad användare får tillgång till de delar av informationssystemet som användaren behöver för att kunna utföra sina arbetsuppgifter och blir därmed behörig att använda dessa delar eller funktioner (Lagerlund, 1997).

Dahlin och Arnesjö (1996) anser att något som också är direkt knutet till behörigheten är signering av journalanteckningar. Att signera en informationsmängd innebär enligt Lagerlund (1996) att denna godkänns och låses i databasen. Att överlåta sin personliga behörighet att registrera, ändra eller ta del av personuppgifter på annan anser Dahlin och Arnesjö (1996) inte får förekomma. Enligt Patientjournallagen får en patientjournal inte läsas om man inte har behov av det för patientens vård. Behörigheten är också en del av rättssäkerheten, vilken betyder att allt som görs med hjälp av behörigheten ansvarar respektive användare för. Därför skall användare inte låna ut sin behörighet till någon annan person. Ett lösenord skall väljas så att det inte går att gissa och det måste hållas hemligt. Ett lösenord bör bestå av minst sex tecken med bokstäver och siffror blandade. Att byta lösenord bör också göras minst en gång i kvartalet eller om man tror att någon råkat få se det (Dahlin & Arnesjö, 1996).

2.2.6 Sekretess

De grundbestämmelser som rör sekretess inom hälso- och sjukvårdens område finns i Sekretesslagen (se kapitel 2.2.2).

Sekretess definieras av Västra Götalandsregionen (2000) som ”Att hålla information och resurser otillgänglig och inom önskad tid.”

Enligt Lagerlund (1999) finns det i huvudsak sex olika möjligheter när uppgifter får lämnas ut.

- Vid patientens samtycke.
- Efter skade- och menprövning.
- För att fullgöra, exempelvis remisser, i den egna verksamheten.
- Om stöd finns av lag eller förordning.
- Med reservation (att sekretessen gäller hos mottagaren).
- Om en nödsituation kräver det.

Inre och yttre sekretess

Lagerlund (1999) menar att de användare som tilldelats behörighet själva kan hämta den information som behövs via datorn. Vid den inre sekretessen är den person som hämtar information ansvarig för att det är en tillåten handling, att exempelvis informationen behövs för att kunna ge en bra vård. Tekniken idag möjliggör att informationen kan bli direkt åtkomlig oberoende av avstånd, vilket innebär att den inre sekretessens verksamhetsgräns har vidgats. Var den inre och yttre sekretessen går finns det idag olika tolkningar om mellan myndigheter. Den yttre sekretessen var dominerande innan de nya tekniska möjligheterna kom. Parten som sänder information är ansvarig för att den som tar emot informationen är behörig att ta del av informationen. I Vårdregisterlagen finns ett stöd för utvidgningen av den inre sekretessen, men i Sekretesslagen finns inget självklart stöd av den (Lagerlund, 1999).

2.2.7 Integritet

Behörighetsregler och behörighetssystem skall garantera att inga obehöriga exempelvis ska kunna läsa, skriva eller ändra uppgifter i journalsystemen (Dahlin & Arnesjö, 1996). Detta ger en trygghet för både patient och personal. De uppgifter som patienten lämnar ut skall inte vara tillgängliga för andra än de som behöver dem i vården av patienten. Enligt Dahlin och Arnesjö (1996) skall de som skriver i journalen vara säker på att ingen kan ändra det som är registrerat i patientjournalen, vilket är en rättsäkerhetsfråga.

Dataintegritet är enligt Lyckséus, Wahlgren och Lindqvist (1998) förmågan att upprätthålla ett värde eller innehåll genom att skydda det mot oönskade förändringar, påverkan eller insyn.

Dataintegritet och datakvalitet

Informationskvalitet eller datakvalitet kan enligt Lagerlund (1996) betraktas ur flera perspektiv, exempelvis noggrannhet, validitet, tillförlitlighet och dataintegritet. Gratte

(1996) anser att information lagrad i datorer är till ingen nytta om personalen inte kan lita på kvalitén hos de lagrade uppgifterna, den så kallade datakvaliteten. Att skydda kvalitén på den lagrade informationen blir allt svårare och viktigare, när data flyttas mellan avdelningar, vårdcentraler och sjukhus. Inom vården är det viktigt att den information som användaren erhåller är av sådan kvalitet att han eller hon kan använda sig av informationen. Att data skall vara korrekta är något som är självklart för att inte fel åtgärder skall utföras. En hög datakvalité är viktigt inom vården för att flera av de beslut som tas, vilka bygger på att data är korrekt, berör patientens hälsa. Fel kan bland annat uppstå vid inmatning genom exempelvis skrivfel, missförstånd, stress och så vidare. Fel kan även uppkomma vid överföring av data och i samband med medveten manipulering. Några exempel på allvarliga fel, är att fel personnummer registreras vid dödsfall eller att ett decimalkomma blir felplacerat i ett läkarrecept. Därför är det viktigt att kunna bedöma vad utskrifter från datorn egentligen säger oss som användare (Gratte, 1996).

Kvalitén på data i datasystem har några svaga punkter (Högskolan Skövde, 2002). Dessa är insamling, registrering och sammanställning eller behandling av data. De flesta datasamlingar innehåller felaktigheter och en övertro på data som är producerade av datorer gör att användarna lämnar över kontrollen till datorn och litar på svaret (Högskolan Skövde, 2002; Fisher & Kingma, 2001). När insamling av data ska ske kan det vara flera orsaker till att fel uppstår, exempelvis att formuläret har otydliga instruktioner, dålig layout eller format, fel person fyller i formuläret eller om motivet med insamlandet är oklart och att användaren är oaktsam. Vidare kan patienten ljuga om data eller identitet men användaren kan även skriva in avsiktliga fel. Vid registrering av data kan fel uppstå då indata är felaktiga, användaren kan utelämna viss data eller skriva in data på fel plats. Datakvaliteten kan försämras när användaren har erhållit dåliga instruktioner för inmatning. Vid lagring, sammanställning och behandling av data kan försämring av datakvalitén uppstå exempelvis när det är fel på hårdvaran, vid felaktig programmering, vid sabotage, förlorade dataposter och dålig behörighetskontroll (Högskolan Skövde, 2002).

Förebyggande åtgärder som kan vidtas är att upprätta en policy, olika kontrollrutiner och definiera befogenheter och ansvar som berör datakvalitet. Vidare kan granskningar och stickprov göras på hur policy och kontrollrutiner följs. Att ändra lösenord och utbilda personalen om vikten av datakvalitet gör att användarna blir medvetna om risken med felaktig data (Högskolan Skövde, 2000).

Kajbjer och Lundmark (1997) anser att med hjälp av olika standarder inom hälso- och sjukvården kommer användaren av informationssystem att uppleva en bättre datakvalitet och få ett ökat förtroende till den information som redan finns. Vidare kommer standarderna att ge flera möjligheter till en effektiv användning av informationen (Kajbjer & Lundmark, 1997).

2.2.8 Oavvislighet

Enligt Björner (2000) används begreppet oavvislighet mest vid meddelandehantering, med skickande och mottagande av meddelande. Den som säger sig ansvara för innehållet i en informationsmängd, det kan vara ett meddelande eller en text i patientjournalen, skall i efterhand inte kunna förneka detta. Oavvislighet kan åstadkommas med elektronisk signatur. Enligt Björner (2000, s.25) är en elektronisk signatur ”(…) data i elektronisk form som är fogade till eller logiskt knutna till en

elektronisk handling och som används för att kontrollera om innehållet härrör från den som framstår som undertecknare.”

För att skicka patientdata utanför den egna enheten fordras patientens medgivande och mottagarens identitet måste kunna styrkas vid all kommunikation (Dahlin & Arnesjö, 1996). Det är viktigt att både äkthetsidentifiering och mottagaridentitet kontrolleras. Överföring av personuppgifter ska ske i krypterad form när uppgifterna skickas utanför den registrerades lokaler. Kraven på sekretess och säkerhet måste ställas vid all överföring av patientdata med hjälp av exempelvis telefax och trådlös kommunikation (Dahlin & Arnesjö, 1996).

2.2.9 Spårbarhet

Spårbarhet är enligt Västra Götalandsregionen (2000) att ”Verksamheten och tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer.”

En viktig del i skyddet av personuppgifter är enligt Dahlin och Arnesjö (1996) möjligheten att i efterhand kunna kontrollera hur informationen har bearbetats. Åtkomst till personuppgifter och gjorda transaktioner av behörighetssystemet ska kunna följas upp i efterhand genom ett maskinellt underlag (logg). Av underlaget skall det framgå vem som har haft åtkomst till personuppgifterna och vid vilken tidpunkt åtkomsten skedde (Dahlin & Arnesjö, 1996).

Enligt Björner (2000) kan loggningsfunktionen delas upp i två olika typer: juridisk logg och säkerhetslogg. Den *juridiska* loggar all information som hanteras i systemet. Informationsutbytet skall sparas i oförvanskat format eller det ska vara möjligt att kunna återskapa informationen. Dessa loggar skall sparas i minst tre år eller om särskilda föreskrifter finns. *Säkerhetsloggen* kontrollerar vem som gjort vad, vid vilken tidpunkt och hur innehållet förändrats. En bevakningsfunktion skall finnas i avseende på de felaktigheter som kan uppstå (Björner, 2000).

Dessa funktioner för att säkerställa informationssäkerhet bör användaren få information och utbildning om, för att problem inte ska uppstå som beskrivs i efterföljande kapitel. De olika typer av användare som kan finnas av ett informationssystem och dess olika nivåer av kunskap beskrivs även i kapitlet.

2.3 Användaren, dess roll och faktorer relaterade till informationssäkerhet

Begreppet användare omfattas av olika klasser. Här nedan beskrivs dessa för att få förståelse för vilka olika användare som finns av ett system och vilken nivå av kunskap de har samt något om användarens roll och olika användarrelaterade faktorer som påverkar informationssäkerhet.

2.3.1 Slutanvändare

Enligt Faulkner (2000) bör användare som grupperas ha ett likartat beteendemönster med systemet och deras användarkrav bör då vara ungefär de samma. Användare som har mer än en funktion i organisationen kan grupperas i mer än en slutanvändareklass.

Det finns enligt Faulkner (2000) fyra olika klasser av slutanvändare som behöver identifieras; direkt-, indirekt-, fjärr- och supportanvändare.

Direktanvändare beskrivs av Faulkner (2000) som de personer vilka använder sig av systemet för att utföra sina arbetsuppgifter. Exempelvis en undersköterska som läser i datorjournal för att kunna ge patienten rätt och riktig vård. Den *indirekta användaren* är enligt författaren de personer som ber andra att utföra tjänster för deras räkning. Exempel på det kan vara en person som ringer och vill ändra på en undersökningstid då mottagaren av samtalet får ändra i det patientadministrativa systemet. *Fjärranvändare* använder inte systemet själva men är ändå beroende av vad det ger för avkastning, exempelvis en användare som tar ut pengar från en bankomat. *Supportanvändaren* är den del av personalen som administrerar systemet och tekniskt hjälper andra så att de kan genomföra sina uppgifter. Det kan exempelvis vara personal på helpdeskavdelning eller en systemadministratör (Faulkner, 2000).

Faulkner (2000) beskriver vidare att beroende på vilket förhållande slutanvändarna har till systemet och hur de använder systemet för att utföra sitt arbete kan ytterligare två klasser komplettera ovanstående klasser. Den första är den ”tvingade” användaren som måste använda systemet som en del i sitt arbete. Om systemet ligger nere försvåras arbetet för dessa användare. Den andra klassificeringen är den användare som har befogenhet att själv kunna välja efter omständigheterna om han eller hon vill använda sig av ett datorsystem för att utföra sina arbetsuppgifter (Faulkner, 2000).

2.3.2 Användare och olika nivåer av kunskap.

Enligt Faulkner (2000) är det också viktigt att beskriva användarnas nivå av kunskap och bakgrund och inte bara placera användare i olika klasser efter vad de får ut av att använda systemen. När användare skall klassificeras i olika nivåer av kunskap kan de placeras i följande kategorier; nybörjare, ”medelkunnig” och expert. Nybörjaren har lite eller ingen erfarenhet av att använda datorer och de kan vara osäkra när de ska lära sig använda dem. De behöver frekvent respons från systemet för att försäkra sig om att det de gör är riktigt. Den medelkunnige användaren är enligt Faulkner (2000) den person som bara använder systemet ibland eller under vissa perioder, för att sedan komma tillbaka efter några månader och använda systemet. De kan innefatta både nybörjaren och expertanvändarens karaktärer. De är skyldiga att komma ihåg en stor del av systemet men inte några detaljer. Det är därför viktigt att dessa användare får stöd när de behöver hjälp och att funktionaliteten är konsistent i hela systemet. En expertanvändare kan inte allt om systemen. När okända frågor kommer upp behöver även experter hjälp men använder då i högre grad hjälpsystem för att utföra uppgiften på ett riktigt sätt. De behöver inte använda den supportpersonal som finns utan betraktas och är säkrare i sitt sätt att interagera med systemet (Faulkner, 2000).

2.3.3 Användarens roll och faktorer relaterade till informationssäkerhet

Användaren brukar IT-systemen som ett stöd i sin verksamhet. I Västra Götalandsregionen (2000) beskrivs att användaren är den som har mest kontakt med systemet och kan därför oftast bäst bedöma om IT-systemet gör nytta. Användaren skall därför bevaka och rapportera hur IT-systemet fungerar och ansvara för att detta görs. En skyldighet som användaren har är att utföra incidentrapportering. Användarna har enligt Västra Götalandsregionen (2000) även ett egenansvar där de

”(…) som tar del av, skapar, lagrar eller överför information för (…) verksamhet ansvarar i sina arbetsuppgifter för att informationen hanteras i enighet med informationsansvariges direktiv.”

Gaunt och Roger-France (1996) anser att det är viktigt att sjukvårdspersonal förstår varför det är viktigt att upprätthålla en säkerhetsmiljö för information som de lagrar om patienterna och deras vård samt hur denna skall organiseras. Detta utförs bäst genom ett väl strukturerat utbildningsprogram som involverar all personal (Gaunt & Roger-France, 1996).

Sågänger och Utbult (1998) menar att var tredje journal inte är tillgänglig när personalen behöver den för mötet med patienten. Det kan också vara det omvända så att de anställda får tillgång till så mycket information att de inte hinner ta in den information de behöver för patientmötet. Sågänger och Utbult (1998) menar att sjukvårdspersonal använder minst 30 % av sin arbetstid till informationshantering. Hantering av information kräver disciplin av de anställda, som matar in uppgifterna, för att de skall vara korrekta när de hämtas ut. De anställda måste lära sig att arbeta med datorjournalen för att kunna få de fördelar som finns, annars skapas lätt stress. Några kritiska användare till datorjournalen menar på att det tar mycket längre tid att skriva omvårdnadsdokumentation på ett strukturerat sätt i datorn, vilket i sin tur skapar stress. Vid muntliga ordinationer kan det lätt hända att personer som skall registrera beställning antingen glömmer eller gör fel vid inskrivning, exempelvis registrerar i fel läkares namn (Sågänger & Utbult, 1998).

Gratte (1996) menar att en mycket stor andel av säkerhetsproblemen orsakas av den mänskliga faktorn genom feloperationer. Av allt att döma beror detta på att användarna saknar tillräcklig utbildning och att dokumentation är svårbegriplig och otillräcklig. Det mest effektiva sättet skulle vara att ge människorna kunskaper och att förändra deras attityder. Problemen ligger ofta i attityder. Användarna förstår inte att informationen är viktig, utan hanterar informationen i datorer på ett sätt som avviker från när motsvarande information finns på papper. Gratte (1996) anser att 80 % av alla brister i säkerheten kan hänvisas till personalen. Orsaker till dessa säkerhetsbrister kan vara ansvarslöshet, brist på insikt eller brist på information (Gratte, 1996).

Gratte (1996) anser vidare att:

- Många i personalen anser alltför ofta att säkerheten inte är deras problem. De har dessutom ofta för dåliga kunskaper för att känna igen ett hot mot säkerheten.
- Det är svårt att se värdet i informationen och att den måste skyddas.
- Flera användare tycks tro att tekniken vid datoranvändning alltid fungerar.

För höga och för låga krav skapar lätt stress menar Gratte (1996), vilket kan ge upphov till fel. Lagom mängd krav i arbetet ger stimulans och vidareutveckling. Höga krav i form av ont om tid och svåra arbetsuppgifter skapar stress. Även alltför låga krav med brist på omväxling i arbetsuppgifterna kan åstadkomma stress. En vanlig stressorsak är att man inte behärskar den nya tekniken på ett tillfredställande sätt eller att det ofta uppstår oförutsägbara problem med datorer som att program beter sig ”ologiskt” eller att datorn ”hänger sig” utan synlig anledning (Gratte, 1996).

Datainspektionen (1998) redogör i sin rapport för att det ofta förekommer slarv med säkerheten. Ett skäl kan vara att säkerhetsåtgärderna uppfattas som en extra belastning

i den redan hårda arbetssituationen. Utbildning inom IT-säkerhetsområdet har kraftigt åsidosatts på många vårdinrättningar, likaså saknas motivation till ett bra säkerhetstänkande inom personalen (Datainspektionen, 1998).

Ett sekretessproblem är att någon glömmer att logga ut och nästkommande person kan ta del av information de inte borde få tillgång till. Risk finns att anställda avslöjar sitt lösenord för någon som sedan använder det för brottslig gärning (Sågänger & Utbult, 1998). Enligt Furnell m fl. (2000) skall 26 % av användarna komma ihåg lösenord och användarnamn till fem eller flera applikationer. Krav på att komma ihåg så stort antal lösenord utgör ett problem för användarna. Det är därför inte konstigt att de väljer enkla och kända namn som är lätta att komma ihåg (Furnell m fl., 2000). Dowland, Furnell, Illingworth och Reynolds (1999) uppger i sin artikel att 29 % av de tillfrågade medger att andra personer känner till deras lösenord. Vid misstanke att personal utnyttjat sin befogenhet till känslig information går det i efterhand att få fram användarnamnet i loggregistret för att kontrollera om personen gjort fel (Sågänger & Utbult, 1998). 75 % av personalen som använder datorer i arbetet utnyttjar utrustningen för icke arbetsrelaterade aktiviteter (Dowland m fl., 1999).

Datorsystem tillåter ofta en noggrann kontroll av de användare som utnyttjar systemen. Enligt Gratte (1996) kan denna form av övervakning vara psykiskt påfrestande om den går för långt. Furnell m fl. (2000) redogör för att 45 % av användarna inte litar på användningen av dataloggning. Användarna tror att loggningen inte enbart används för datasäkerhetsövervakning utan även för att mäta produktiviteten vid inmatningsarbetet (Furnell m fl., 2000).

Informationssäkerhet inom vårdområdet bör vara en viktig del i det dagliga arbetet för personal, för att inga obehöriga ska få del av information om patienterna. Informationssäkerhet är också en viktig aspekt för personalen eftersom de måste kunna få tillgång till korrekt information när de behöver den för att kunna ge patienten en bra vård. Tillgänglighet till information i datorjournalen har ökat vilket ställer höga krav på att olika rutiner och skyddsåtgärder fungerar inom vården. För att en säker miljö ska kunna erhållas krävs det även att personalen förstår och är medvetna om vad som innefattas av informationssäkerhet. Alla användare av informationssystem inom vården bör därför få adekvat utbildning om informationssäkerhet för att kunna rätta sig efter de krav som ställs på säkerheten. Det är även viktigt att de lagar som berörs vid informationshantering inom vården efterlevs för att patienterna ska få förtroende för den personal som arbetar inom hälso- och sjukvården.

De brister i informationssäkerhet som beskrivits i kapitlet ovan leder in på det problemområde och den problemprecisering som arbetet berör. I efterföljande kapitel beskrivs dessa.

3 Problembeskrivning

I kapitlet beskrivs det problemområde som arbetet berör och en definiering av problemet. Vidare beskrivs de avgränsningar som gjorts i arbetet och det förväntade resultatet.

3.1 Problemområde

”Den ökande specialiseringen och utvecklingen mot en alltmera processtyrd vård gör att allt flera personer deltar i vården av varje patient” (Lagerlund, 1999, s. 12). Patientinformation kan göras tillgänglig för allt fler med hjälp av informationsteknologi. Sjukvården är dessutom en informationsintensiv verksamhet där informationen ofta är mycket känslig. Användningen av IT-stöd ökar inom alla områden i hälso- och sjukvården och kraven på informationssäkerhet ökar i takt med att datorstöd i allt högre grad utnyttjas i det direkta vårdarbetet (Lagerlund, 1997).

Att hantera information i datorjournaler kräver en god läsbarhet och lätthet att registrera och ta ut patientdata i det dagliga arbetet. Det kräver också en god säkerhet, sekretess, laglighet och möjlighet att få ut den data som krävs för verksamhetsuppföljning och kvalitetsutveckling (Dahlin & Arnesjö, 1996).

Enligt Lagerlund (1999) vet vårdpersonal sedan tidigare att känslig information skall skyddas mot insyn, otillbörlig åtkomst och att obehöriga inte skall kunna ändra i informationen. Trots det finns det hos många vårdanställda en osäkerhet om vart gränserna går för vad som är tillåtet i den informationshantering personalen utför. Osäkerheten har eventuellt förstärkts genom IT:s inträde i vården och att ny lagstiftning inte ännu funnit sin tillämpning och tolkning (Lagerlund, 1999). Enligt Meyer, Lundgren, Moor och Fiers (1998) måste vårdpersonalen få tillgång till rätt patientdata för att kunna ställa rätt diagnos och för att ge en optimal vård. Systemet skall skyddas så mycket som möjligt från fel gjorda av användaren. Användaren i sin tur skall tränas i hur systemet skall användas och bli medveten om de säkerhetshot han eller hon är kapabel till att göra (Meyer m. fl., 1998).

Att användare har tillgång till för mycket eller för lite information och inte kan genomföra sina uppgifter på ett riktigt sätt skapar lätt stress, vilket i sin tur påverkar informationssäkerheten. Användaren kan även uppfatta in- och utloggning som en omotiverad uppgift i den hårda arbetsbelastning som kan uppkomma på arbetsplatsen. Vid loggning av systemen kan personalen känna sig övervakade vilket kan vara påfrestande i olika arbetssituationer.

Den största risken med ett fungerande IT-stöd är enligt Lagerlund (1999) brister i ansvarsfördelning, organisation och kunskap hos personalen vilket har visat sig i hot och riskanalyser. Rapporter visar också på att det är den egna personalen som är den största risken för en medveten felaktig hantering av IT-stödet. Den interna personalen begår fler brott än personer utifrån som gör intrång i systemen (Lagerlund, 1999).

I datainspektionen rapport (1998) ges rekommendationer till registeransvariga inom hälso- och sjukvården, några av dessa är att:

- Personalen skall alltid vara vaksam vid registrering av känsliga uppgifter så att förväxling av personnummer (p.nr.) och registrering på annans p.nr. inte sker. Identitet på patienten skall alltid säkerställas genom kontroll.

- Eftersom lagen om vårdregister trätt i kraft måste alla personuppgiftsansvariga lägga upp strategier för att kunna uppfylla de stränga informationskrav som lagen ställer.
- Registeransvariga måste förvissa sig om att tillämpliga författningar eller andra regler distribueras inom organisationen så att föreskrifterna efterlevs.
- Arbetsstationer som är påloggade får aldrig lämnas utan uppsikt.
- Dataskärmar med känslig information får inte placeras så att förbipasserande kan se innehållet.
- Samtliga användare av datasystem skall bara använda sig av sitt egna lösenord och se till att inga andra får tillgång till det.
- Kontroller av att inga kvarlevande accessrättigheter finns kvar på personal som slutat sin anställning.
- Regelbundna kontroller av IT-säkerheten inom organisationen måste genomföras av de personuppgiftsansvariga.
- Utbildning i IT-säkerhet bör fortlöpande ske till alla användare av datasystemen.
- All åtkomst till personalregister som innehåller känslig information bör loggas och kontrolleras fortlöpande.

Utifrån dessa rekommendationer och de grundläggande funktionerna: autentisering, behörighetstilldelning, sekretess, integritet, oavsiktlighet och spårbarhet, för att säkerställa informationssäkerhet, är det betydelsefullt att studera huruvida de efterföljs av användaren. Eftersom användaren står för de största riskerna i informations-säkerhet enligt flera rapporter (Furnell m fl., 1996; Lagerlund, 1999; Furnell m fl., 2000) är syftet med arbetet delvis att kunna studera om situationen är densamma eller om det skett någon förändring till det bättre vad gäller de risker i informationssäkerhet som användare står för inom hälso- och sjukvården.

3.2 Problemprecisering

Projektet syfte är att kartlägga, utifrån de grundläggande funktioner och rekommendationer som finns på informationssäkerhet:

- *Hur påverkas användaren av kraven på informationssäkerhet i datorjournaler?*
- *Hur påverkar användaren informationssäkerheten i datorjournaler?*

3.3 Avgränsning

Hur informationssäkerhet skapas med hjälp av tekniska lösningar avses inte att tas fram i arbetet. Projektet kommer enbart att beröra informationssäkerheten som sker vid och i anslutning till datorer.

Med användare menas i det här arbetet de personer som har tillgång och behörighet till de datoriserade patientjournalerna och kan läsa, skriva eller förändra data i journalen.

3.4 Förväntat resultat

Flera rapporter visar på att användarna är den största orsaken till att kraven på informationssäkerheten inte efterföljs. Den stress och arbetsbelastning som kan uppstå på arbetsplatsen tillsammans med bristen på utbildning leder ofta till att användaren slarvar med in- och utloggning, hantering av lösenord och feloperationer vid in- och utmatning. Resultatet av arbetet förväntas därför påvisa dessa brister.

Vidare bör arbetet kunna påvisa användarens syn på och kunskap om informationssäkerhet och skapa förbättrade möjligheter att uppfatta vilka brister i informationssäkerheten som kan uppkomma i användandet av en datorjournal. Arbetet förväntas även visa på om användarna behöver ytterligare utbildning i informationssäkerhet.

4 Undersökningens upplägg och genomförande

I kapitlet beskrivs några av de möjliga tekniker som finns för insamling av information för arbetet, de tekniker som valts för insamling av information, samt arbetets upplägg och genomförande.

4.1 Möjliga metoder och metodval

Enligt Patel och Davidson (1994) finns bland annat följande tekniker för att samla information. Dessa är dokument, dagböcker, intervjuer, enkäter, attitydformulär och observationer.

De tekniker som valts för att samla information om problemområdet är att studera olika dokument, observationer och intervjuer. Valet av insamlingsteknik har baserats på olika förutsättningar och resurser. För att få en förståelse för problemområdet har olika dokument så som böcker, vetenskapliga artiklar och tidskrifter studerats. Observationer har valts delvis för att kunna ta del av hur olika användare arbetar med datorn, men även för att samla in information från beteenden så som fysiska handlingar, verbala yttranden och skeenden i olika situationer. Utifrån observationerna kan tolkningar göras om användarna gör på det sätt som de tror sig göra. Observationer kan kompletteras med intervjuer med de observerade för att säkerställa det observationsmaterial som tagits fram. Eftersom intervjuer kan förtydliga den information som framkommit under observationerna är det en av anledningarna till att intervjuer valts som teknik. Intervju med de observerade personerna kan även ge svar på frågor som uppkommer under observationerna. Intervjuer valdes också för att få en personlig kontakt med respondenten eftersom vissa av frågorna blev av känslig karaktär. Hade telefonintervju eller enkät istället valt att göras hade respondenten enklare kunnat ignorera att svara på dessa frågor.

4.1.1 Observationer

Enligt Patel och Davidson (1994) är observationer framförallt användbara när information från beteenden så som fysiska handlingar och verbala yttranden och skeenden i olika situationer ska insamlas. För övrigt används observationer för att komplettera den information som fås från andra tekniker. En fördel är att skeenden och beteenden kan studeras när de faktiskt sker. En annan är att observationer är relativt obundna av personers villighet att lämna information. Tekniken kräver mindre aktivitet och samarbete av den grupp som skall observeras än med de flesta andra tekniker. En nackdel är att den anses vara dyr och tidsödande. Vid bearbetning av materialet, då observationer av beteenden och skeenden har gjorts, bör observatören tänka på om det som framkommit är representativt, vilket kan ses som en ytterligare nackdel (Patel & Davidson, 1994).

En observation kan enligt Patel och Davidson (1994) vara strukturerad eller ostrukturerad. Den strukturerade observationen förutsätter att det är givet vilka situationer och beteenden som kommer att ingå i observationen. Det går då att ställa upp ett antal kategorier som avses att undersöka. Med utgångspunkt från dessa kategorier kan ett observationsschema skapas. De ostrukturerade observationerna används mest i utforskande syfte, där syftet är att hämta så mycket information som möjligt kring ett problemområde. Vid dessa observationer används inget schema utan

istället bör så mycket som möjligt antecknas under själva observationen. Observatörens registrering består ofta av att skriva ned nyckelord, vilket gör att det är viktigt att observatören gör en fullständig redogörelse så fort som möjligt efter observationens slut (Patel & Davidson, 1994).

Enligt Patel och Davidson (1994) bör observatören ta ställning till hur denne skall förhålla sig i observationssituationen. Författarna beskriver fyra olika sätt som observatören kan förhålla sig till dem som skall observeras, vilka är:

- deltagande
- icke deltagande
- känd
- okänd.

Den deltagande observatören går in som medlem i den grupp som är aktuell och tar aktivt del i situationen. Är denne känd av gruppen bör alla acceptera observatörens närvaro och det är viktigt att observatören inte betraktas tillhöra någon del av gruppen, utan är opartisk. I samband med deltagande observation där observatören är känd kan en nackdel vara att observatören stör gruppens vanliga beteende. Om observatören är deltagande och okänd kan problem uppstå där denne måste hålla en mängd information i minnet, vilket kan ge fel resultat. Dessutom kan det ge etiska problem när inte de observerade kan ge sitt samtycke till att medverka (Patel & Davidson, 1994).

De problem som uppkommer vid deltagande observation kan enligt Patel och Davidson (1994) undvikas om observatören är icke deltagande. Är observatören känd måste denne även här accepteras av gruppen. Vid icke deltagande observation kan personerna bli påverkade av observatören till en början, för att de sedan återgå till deras vanliga beteende då observationen kan börja. Problemet med att vara icke deltagande och okänd är av mer praktisk natur det vill säga, var skall observatören placera sig utan att upptäckas (Patel & Davidson, 1994).

4.1.2 Intervjuer

Intervjuer är uppbyggda på frågor för att samla information. Enligt Patel och Davidson (1994) är det två aspekter som bör beaktas när frågor används för insamlandet av information. Dessa är graden av standardisering och strukturering. Vid standardisering av frågor är det viktigt att tänka på hur mycket ansvar som lämnas till intervjuaren när det gäller frågornas formulering och ordning. När intervjuaren själv formulerar och ställer frågorna i den ordning som är mest lämpad för respondenten, under själva intervjun, betecknas det som en låg grad av standardisering. Hög grad av standardisering blir sådeles att frågorna kommer i exakt samma ordning till varje respondent. I vilken omfattning frågorna är fria för tolkning av intervjupersonen kallas grad av strukturering. När intervjun är helt strukturerad lämnas ett litet utrymme för den person som intervjuas och det är förutsägbart vilka svar som respondenten kan välja att svara emellan. Om intervjun istället är ostrukturerad lämnas stort utrymme att svara inom för den person som blir intervjuad (Patel & Davidson, 1994).

Att genomföra intervjuer ger flera fördelar enligt Ejlertsson (1996), några är att intervjuundersökningen ger möjlighet till mer komplicerade frågor. Vidare kan intervjun gå ner mer på djupet genom att följdfrågor kan ställas. I en intervju kan identiteten styrkas och den intervjuade kan ställa frågor om något är oklart. Det stora bortfallet som kan finnas med enkäter är inte lika stort i intervjuundersökningar, då en bättre kontroll över de skäl som personerna har att inte vilja medverka i undersökningen fås. Nackdelar med intervjuer är att respondenten kan påverkas av intervjuarens sätt att ställa frågorna. Känsliga frågor är inte lätta att besvara i en intervju och respondenten kan känna press genom att intervjuaren väntar på svar. Personen som intervjuas kan heller inte kontrollera faktauppgifter under en intervju som han eller hon skulle ha kunnat vid en enkätförfrågan. De svar som fås vid en intervju blir mer svårtolkade än vid en enkät därför att svaren blir olika vid varje utfrågning. En avgörande faktor vid val av teknik är ofta kostnaden och en intervjuundersökning kan bli kostsam om avstånden är stora. Även restiden för att kunna genomföra intervjun kan vara avgörande (Ejlertsson, 1996).

4.2 Upplägg

Arbetet omfattar en kvalitativ fallstudie, för att erhålla en djupare förståelse och kunskap om problemet, där verbala analysmetoder kommer att användas. Undersökningen görs på en mindre avgränsad grupp inom hälso- och sjukvården men utgår från ett helhetsperspektiv och försöker få så täckande information som möjligt om arbetets problemområde på det sätt som Patel och Davidson (1994) beskriver. Arbetet kommer till viss del även att vara explorativt där information från observationerna kommer att ligga till grund för några av de frågor som kommer att ställas vid intervjuerna.

- Arbetet inleds med att olika dokument studeras för att få förståelse för det valda problemområdet.
- Utifrån problemområdet preciseras det problem som ska studeras.
- Olika tekniker för att lösa problemet studeras och en eller flera insamlingstekniker vilka anses lämpliga för fallstudien väljs.
- Genom att studera litteratur framställs ett observationsschema vilket anses omfatta de händelser och skeenden som ska studeras. Schemat gås igenom för att upptäcka eventuella brister.
- En första kontakt tas med lämpliga divisioner på sjukhus som kan medverka i studien.
- Efter urval av lämpliga observationsplatser bestäms tid för observations-tillfällen.
- Observationer genomförs och bearbetning utförs av observationsmaterialet, vilket tillsammans med material som studerats under tidigare steg kommer att ligga till grund för utformning av intervjufrågor. Frågorna kontrolleras för att se om de är relevanta för problemet.
- Tider bestäms för intervjuer med respondenter och därefter bokas lokaler för intervjuer.

- Intervjuer genomförs och materialet renskrivs och skickas därefter ut till respondenterna för kontroll.
- Bearbetning och analys av material från observation och intervju fullföljs och sammanställs.
- De slutsatser som tas och en diskussion om hela arbetet redogörs slutligen i rapporten.

Ett arbete som läggs upp utefter punkterna ovan förväntas kunna bidra till svar på den tidigare presenterade problempreciseringen.

4.3 Förberedelser och genomförande av observationer

I kapitlet beskrivs urval av observationsgrupp, utformningen av det schema som används under observationerna och om observatören varit deltagande eller ej. Vidare beskrivs genomförandet av observationerna.

4.3.1 Urval av observationsgrupp

Den undersökningsgrupp som arbetet inriktade sig på är personal på en sjukhusdivision i mellersta Sverige. Urvalet grundade sig dels på att divisionen använder sig av datorjournal och dels att några av de anställda arbetar vid en och samma dator. Att studera anställda som delar på en eller flera datorer har valts för att få möjlighet att studera om användarna följer de rekommendationer som finns från Datainspektionen. Exempelvis avsågs att undersöka om användarna använder varandras eller egen identitet vid in- och utloggning och på så sätt åskådliggöra sätt som användaren påverkar informationssäkerheten.

På divisionen använder de sig i i nuläget av datorjournalsystemet Melior och ett flertal andra informationssystem bland annat Beakta, som är ett beräkningssystem för att beräkna vårdtid för varje patient och Labsvar, som behandlar svar från olika laboratorier.

4.3.2 Utformning och test av observationsschema

Ett observationsschema (bilaga 1) togs fram genom att de olika funktionerna för att säkerställa informationssäkerhet (kapitel 2.2.3) låg till grund för de kategorier som ingick i schemat. Något som bidrar till att observationen är strukturerad (Patel & Davidson, 1994). Genom att bearbeta och tänka ut olika händelser i förväg som kunde uppkomma under observationerna inom de aktuella funktionerna, autentisering, behörighetstilldelning, sekretess, integritet, oavvislighet och spårbarhet, var avsikten att det skulle bli enklare att föra en skriftlig redogörelse under själva observationen. På grund av etiska skäl, för att inte utsätta andra människor för att det egna arbetet ska bli bättre, genomfördes ingen pilotobservation. För att kontrollera observationsschemat och att kategorier som fanns i schemat motsvarade de händelser som kan uppkomma utfördes en kontroll i samråd med handledare. Observationsschemat kontrollerades då med avseende på valda observationspunkter. De ändringar som då gjordes var att flera tomma rader placerades efter själva schemat

för att manuellt kunna skriva in de händelser som uppkom utöver de kategorier som valts.

4.3.3 Observatörens deltagande

Observatören hade inte för avsikt att vara deltagande i det arbete som utfördes på avdelningen och för att bli accepterad av gruppen skrevs ett informationsbrev (bilaga 2) som gav en förklaring till vem observatören var och kort om studiens syfte. Innan observationerna ägde rum gjordes ett besök på avdelningarna för att ge möjlighet för personalen att bekanta sig med observatören och ställa frågor om något var oklart. Besöket gjordes även för att kunna presentera arbetets syfte. Informationsbrevet delades under besöket ut till de ansvariga på de olika avdelningarna och på de aktuella observationsplatserna. Personalen fick därmed även här möjlighet att läsa om arbetets syfte.

4.3.4 Genomförande av observationer

Besöket genomfördes på divisionen för att kunna få uppfattning av vilka platser som var lämpliga att genomföra observationerna på. Tre olika platser, där personalen delade på en eller flera datorer, valdes ut inom divisionen. Antalet anställda per dator på de utvalda platserna var 3-4 personer.

Observationerna genomfördes under tre dagar på tre olika platser inom enheten. Fördelen med detta var att kunna få en större inblick i hur de arbetar med datorjournal på flera platser inom samma enhet och att få fram ett vidare underlag till arbetets resultat. De datorer som var i bruk användes av flera ur personalen från olika personalgrupper. De olika personalgrupper som fanns på enheten var: undersköterska, sjuksköterska, vårdföreståndare, läkare och arbetsterapeut. Observationerna gick till på följande sätt; Observatören iakttog arbetet inne på en expedition och antecknade de händelser som var relevanta för problemställningen. Händelserna antecknades i observationsschema (bilaga 1) utifrån olika kategorier, med en personsiffra exempelvis Person3 (P3), när de uppkom för att kunna följa vad varje användare gjorde vid användning av datorerna. Anteckningar gjordes även på händelser som inte omfattades av de olika kategorier i observationsschemat, men som ändå var intressanta för arbetet.

Observationsdagarna började med att observatören fikade tillsammans med personalen.

Den första observationsplatsen var en expedition med två datorer som användes av undersköterskor och sjuksköterskor på hela avdelningen. De hade också två datorer i två angränsande rum, där de kunde sitta mera avskilt och föra anteckningar.

Den andra platsen för observation låg mellan två avdelningar men användes bara av den ena avdelningens personal. Expeditionen var ett genomgångs rum mellan de olika avdelningarna om de olika avdelningarnas personal behöver samtala med varandra. På expeditionen fanns fyra datorer som används av all personal på avdelningen utom läkare och vårdföreståndare.

Den tredje observationsplatsen var en expedition som var uppdelad i två rum. I det ena rummet satt sex stycken personer som delade på två stycken datorer och i det

mindre rummet satt två personer som hade tillgång till en dator. Datorerna används enbart av en yrkesgrupp, arbetsterapeuter.

Observationerna varade från kl. 9.30 till 14.00 med avbrott för lunchrast.

4.4 Förberedelser och genomförande av intervjuer

I kapitlet beskrivs urval av intervjupersoner till intervjuerna, utformning av de frågor som används under intervjuerna och själva genomförandet av dessa intervjuer.

4.4.1 Urval av intervjupersoner

En viktig del i en undersökning är enligt Patel och Davidson (1994) att göra noggranna förberedelser när det gäller val av intervjupersoner. Sammanlagt har fem personer intervjuats, en systemadministratör och fyra sjuksköterskor. Inom organisationen finns flera systemadministratörer vilka ansvarar för olika program. I detta arbete har systemadministratören för ett datorjournalsystem, intervjuats. Av de personer som observerats valdes fyra stycken sjuksköterskor ut, som är av typen direktanvändare som dagligen måste använda sig av datorjournalen.

4.4.2 Utformning och test av intervjufrågor

Framställning av intervjufrågor till intervjuerna utgick dels från datainspektionens rekommendationer till registeransvariga, de grundläggande funktionerna för att säkerställa informationssäkerhet och dels från frågor som uppkom under bearbetning av de observationer som gjorts. Frågorna ställdes i samma ordning vid varje intervju, vilket gör att intervjun var standardiserad. Intervjuerna inleddes med neutrala frågor exempelvis vilken grad av datoranvändning de har utöver den i arbetet, enligt en teknik som kallas ”tratt-teknik”. Tekniken innebär enligt Patel och Davidson (1994) att man börjar med stora öppna frågor för att sedan övergå i mer specifika. Frågor som riktades till systemadministratören syftade bland annat till, att få kunskap om det finns några informationssäkerhetsrutiner och i vilken omfattning användarna får utbildning. Svaren från administratören kunde därmed jämföras mot de svar som användaren gav för att bedöma om det fanns skillnader mellan de olika svaren.

Någon pilotintervju har inte genomförts av etiska skäl samt att sekretessen gör att inte verksamheten tillåter att detta sker. Problem som kan uppstå med att inte genomföra en pilotintervju är att det blir svårt att se om frågorna ger de svar som är tänkt, men även att intervjun hålls inom en rimlig tid. De frågor som var framtagna var många till antalet, vilket var det största problemet till att tro att intervjutiden skulle bli lång. Tillsammans med handledare kontrollerades därför frågorna om de var relevanta för att ge svar till det problem som skall lösas. Frågornas art gjorde att enbart några frågor togs bort, vilka inte ansågs relevanta eller där svar redan framkommit under observationen. De frågor som slutligen används i intervjuerna kan återfinnas i bilaga 3. I vilken ordning frågorna ställdes kan ses i Ask, (2002).

4.4.3 Genomförande av intervjuer

En särskild intervjulokal bokades där det fanns möjlighet att prata ostört. Detta för att inte någon skulle komma och avbryta under själva intervjun. Intervjuerna varade från cirka trettio minuter med systemadministratören till en timma och femton minuter med en av användarna.

En intervju med systemadministratör för enheten genomfördes för att få kännedom om vilken omfattning användarna har tillgång till olika författningar, regler och eventuell utbildning, som berör informationssäkerhet. Utifrån de personer som observerats tillfrågades fyra personer om de var intresserade att medverka i intervjuer.

Innan intervjun startade informerades respondenten om syftet med arbetet och varför det är viktigt att de medverkar. De fick även tillgång att läsa det informationsbrev (bilaga 2), som getts ut vid observationen tidigare, för att föra fram budskapet om arbetes syfte på flera sätt. I informationsbrevet framgår det att materialet behandlas konfidentiellt. Respondenten tillfrågades om det gick bra att använda bandspelare under intervjun. I samband med förfrågan gavs en förklaring varför bandspelare används. Intervjuaren berättade även att de skulle få möjlighet att läsa igenom det renskrivna materialet och att kontrollera om något blivit felaktigt och göra förändringar. Materialet fångar då en klar och rättvis bild av respondenternas åsikter och kunskap.

Frågorna ställdes i samma ordning under de fyra intervjuerna, men med olika följdfrågor. De renskrivna intervjuerna skickades via e-post till tre av respondenterna och via brev till två respondenter. I breven skickades ett frankerat svarskuvert med för att underlätta för mottagaren.

Det bearbetade materialet från observationer och intervjuer tillsammans med informationsbrev, observationsschema och de olika intervjuunderlagen sammanställdes i en rapport. Rapporten är inte tänkt att publiceras på grund av de medverkandes integritet men ska ändå finnas tillgänglig för de som önskar ta del av materialet.

4.5 Erfarenheter och värdering av observation och intervjumaterial

Intervjuaren vill först tala om att hon blivit mycket väl bemött hos samtliga respondenter. Vid två tillfällen har respondenterna uttryckt att det var positivt med de frågeställningar som togs upp under intervjun, vilket gjorde respondenten motiverad till nya tankar och funderingar om informationssäkerhet.

Att fika med personalen innan själva observationen började var bra för att minska den eventuella spänning som fanns för att bli observerad. Personal och observatör hade möjlighet att samtala på neutral mark och lära känna varandra närmare.

Något som beaktas när materialet bearbetas är att den observerade personalen varit påverkad av observatören och inte utfört de handlingar som de brukar. En indikation av det fick observatören när denne gick tillbaka till en tidigare observationsplats, där inga större felaktigheter ur informationssäkerhetssyfte studerats men vid besöket var flera datorer påloggade utan synlig personal.

De underlagsfrågor som tagits fram för intervjuerna följdes i den ordning som bestämts. Enbart kortare följdfrågor ställdes mellan de ordinarie frågorna. Följdfrågorna ställdes på grund av vissa oklarheter skulle förklaras men även för att få

fram ytterligare information som var relevant för problemställningen. Systemadministratören gav skriftlig information efter intervjuns slut som berörde systemens back up och när detta görs för att klarlägga de svar som givits.

Att använda sig av bandspelare under intervjun har varit positivt eftersom intervjuaren kunde ägna sig åt vad respondenten sa och inte hade behov av att skriva under intervjun. Genom att ställa följdfrågor kunde ytterligare aktuell information erhållas. Dessa utredde vissa oklarheter samt att relevant information kom fram. Nackdelen med att använda sig av bandspelare var att bearbetningen från band till papper tog lång tid.

Vid en av de fem intervjuerna stannade bandspelaren när ljudnivån blev låg. Detta upptäcktes i ett tidigt skede av intervjun och stödanteckningar gjordes därför under resten av intervjutiden. Att bandspelaren vållade besvär gjorde att både respondenten och intervjuaren kände sig besvärade av situationen. Intervjun varade något kortare tid, dels för att intervjuaren inte kunde koncentrera sig lika bra på vad den tillfrågade svarade som vid de tidigare intervjuerna och dels att svaren var kortare från respondenten än vad de varit vid de andra intervjuerna.

Vid val av personer till intervju kunde materialet kanske blivit ett annat om flera yrkeskategorier hade valts och inte som i detta fall enbart sjuksköterskor.

Respondenterna har inte gjort några större förändringar i det renskrivna intervjumaterialet. Orsaken till detta kan vara att bandspelare används under intervjun vilket medförde att inga oklarheter uppstått.

Materialet som framkommit under observationerna och intervjuerna presenteras och analyseras i efterföljande kapitel.

5 Resultat och analys

I kapitlet sammanfattas det material som framkommit under observationerna och intervjuerna. En utförligare redogörelse av det framkomna materialet finns i Ask, (2002). Redovisning av material från intervjuerna kommer att ske utifrån vissa kategorier som frågorna placerats inom. En sammanställning av frågorna återfinns i bilaga 3. Efter redovisning av observations- och intervjumaterial görs en analys av dessa delar.

5.1 Sammanfattning av material från observationer

Under de två första dagarna som observationerna varade talade personalen på de olika avdelningarna om att det var mycket lugnt på respektive avdelningen och att det är betydligt mer att göra under andra dagar. På den tredje observationsplatsen var det enligt personalen en ”normal” dag, med varken mer eller mindre att göra.

När personalen börjar på dagen läser de ur datorjournalen om de patienter som de är ansvariga för. De har inga samtalsmöten där de pratar om de olika patienterna och vad som har hänt under dagen, utan var och en får när de börjar gå in i datorjournalen och läsa den information som krävs för att vårda patienterna.

Medicinlistor och laboratoriesvar är inte tillgängligt genom datorjournalen utan finns i pärmar på expeditionen. Eventuellt träningsschema för patienterna finns upphängd på en tavla i korridoren, där initialerna uppger identiteten för patienten. Patienten men även obehöriga kan där läsa om de patienter som ligger på avdelningen.

På de observerade expeditionerna var datorskärmarna placerade så att inga obehöriga kunde gå förbi i korridoren och läsa vad som står på skärmen. På två av de tre observationsplatserna fanns skrivare inom räckhåll från datorn men på det tredje måste personalen gå iväg för att hämta sin utskrift. Skrivaren stod i ett angränsande rum som inte var låst.

Vid identifiering av personalens behörighet så att de skall få tillgång till att använda datorn, används ett ID-nummer och ett eget lösenord. Skall de använda något program som finns i programfönstret får de återigen logga in med ID-nummer och samma eller ett annat lösenord som de själva bestämt. För att använda Internet behövs inga fler identifieringar. I programfönstret finns de program som respektive person har behörighet till.

Ingen av de personer som observerades har haft något papper för att läsa sitt lösenord från utan personerna komihåg lösenordet ändå när de loggade in i datorn.

Under observationstiden nyttjades datorerna vid trettio olika tillfällen. Ett tillfälle betraktas som att personalen utför något vid datorn och sedan loggar ut eller går och lämnar datorn för annat ärende. Efter dessa tillfällen loggade inte personalen ut från servern vid nio tillfällen och från datorjournalen vid sex tillfällen. De tillfällen då datorn var åtkomlig för obehöriga varade från ca 5 min till ett par timmar.

Vid tre olika tillfällen använde två personer någon annans identitet när de skulle utföra uppgifter i program som de hade behörighet till. Dessa program var inte datorjournalen. Vid tillfället fann observatören att det går att vara inloggad på två datorer samtidigt med samma identitet utan att användaren får vetskap om att den är inloggad på en annan dator.

När personalen skriver in i datorjournalen gör de oftast det utan några anteckningar som stöd. Efter förfrågan till personalen om stödanteckningar talade personen om att hon hade noteringar i ett anteckningsblock. Under observationen var det ingen ur personalen som använde sig av sådana noteringar. Vid ett par tillfällen har de skrivit ut dokument ur olika program exempelvis Labsvar för att använda som stöd vid registrering i datorjournalen. Personal ifrågasatte vid ett tillfälle vilket läkarens namn var när de skulle registrera i datorjournalen, för att sedan enbart skriva in dennes förnamn.

Personalen tycker det är frustrerande att det tar så lång tid när de ska starta upp datorerna och logga in på servern samt i datorjournalen. Särskilt om de enbart ska göra mindre registreringar eller för att läsa lite om en enskild patient. Vid flertal tillfällen har personer gjort kortare ärenden utan att logga ur datorjournalen på grund av denna orsak.

Vid två av de tre observationsplatserna blir personalen, som sitter och försöker göra anteckningar, störda av patienter eller telefon som ringer eller att annan personal kommer och ger upplysningar eller ber om råd. De måste då ha flera patienter i minnet samtidigt.

Vid två av de tre platserna som observerats har problem uppstått vid användning av de olika program som användarna har behörighet till. Svårigheter uppstår med själva programmen parallellt med att personalen verkar ha svårt att förstå sig på vissa delar av de program som används och personalen har vid ett par tillfällen frågat sig själva ”hur gör man här då?”. Personalen har även framfört till observatören att de är ”osäkra” vid användning av datorer. En person som observerades ansåg att problemet som finns med att skriva i datorjournalen är att olika personer skriver in liknade fakta men på olika sökbegrepp. Personen önskar istället ett gemensamt inskrivningsdokument för all personal för att slippa skriva in samma information flera gånger, vilket är tidskrävande och skulle ge mera tid för patienten enligt personen.

Fax används bland annat för att skicka patientinformation mellan sjukhuset och olika kommuner. Ibland avidentifierar de informationen men för det mesta skickar de iväg patientdata som den är. Personalen ringer till de personer som skall få tillgång till informationen och skickar sedan iväg faxet. Faxmeddelandet består av själva patientinformationen och ett försättsblad där kontaktpersonens namn står angivet och att de skall ringa tillbaka när faxet kommit fram. Personalen får i efterhand ett kvitto på att överföringen gått till det telefonnummer som de angett. Informationen som skickas är inte krypterad. Under observationen anlände två stycken faxmeddelanden som personalen inte riktigt visste vart de hörde eller till vilken avdelning de egentligen skulle.

Enligt personalen på två av de tre observationsplatserna var det lugnt under själva observationstiden men enligt vad observatören kunde se fick personalen ha ”många bollar i luften” samtidigt för att kunna genomföra sina arbetsuppgifter.

5.2 Analys av observationsmaterial

Användarna får vid inloggning uppge först ett användar-ID och ett lösenord för att komma åt servern och beroende på vilket program de ska använda får de ange användar-ID och lösenord ytterligare en gång, vilket kan vara detsamma vid de båda inloggningarna. De lösenord som används kommer användarna ihåg utan att behöva något stöd för minnet. Vid ett flertal tillfällen påpekar användarna att de tycker det tar

lång tid vid inloggningen och att starta upp datorn. När användaren ska gå in för att göra enklare registreringar i datorjournalen tar inloggningen en stor del av den tiden det tar att utföra arbetsuppgiften. Personalen blir ofta avbruten när de gör anteckningar och får gå iväg från platsen där datorn är placerad. Det arbetssätt som personalen har, att de till exempel ideligen blir avbrutna av patienter som ringer, gör att de inte ansvarar för in- och utloggning på ett korrekt sätt. För att underlätta för personalen skulle smarta kort tillsammans med lösenord kunna användas vid inloggningen. Ett smart kort är enligt Åhlfeldt (2002) ett plastkort vilket innehåller en krets som möjliggör en säker identifiering tillsammans med ett lösenord. De behöver då enbart ta ut kortet när de ska utföra en annan uppgift och inte vara beroende av den tid det tar att logga ut. Någon annan av personalen skulle kunna få möjlighet att utnyttja datorn.

Under de timmar när datorerna inte var utloggade på ett korrekt sätt kunde dels obehörig personal och dels utomstående få tillgång till information om olika patienter, vilket är en förseelse mot sekretess och integriteten. Perioder då datorerna inte var utloggade kunde någon ta del av, utföra en oönskad förändring och påverka informationen i datorjournalen. Att personal inte loggar ut ur datorjournalen och servern på ett korrekt sätt gör att de blir ansvariga för någon annan persons handlingar som utförs på datorn.

Under observationerna hände det vid några tillfällen att en person beviljade någon annan person att använda den egna identiteten och behörigheten, vid datoranvändning. Detta kan vara en brist i förståelsen varför inloggning och behörighet finns. Systemet bör också ge en indikation på att användaren är inloggade på mer än en dator, för att uppmärksamma användaren på en sådan situation.

När användarna registrerar in uppgifter om patienter används sällan något stöd för minnet. Personal blir ofta avbruten när de sitter och för in information i datorjournalen genom att telefon eller patienter ringer och annan personal rådfrågar personen. När användaren ska behandla uppgifter om flera patienter samtidigt krävs det mycket av honom eller henne för att inga fel ska uppstå vid registrering i journalen.

Den osäkerhet som fanns vid att använda olika program i datorn och att programmen i sig var besvärliga gjorde att olika hanteringsproblem uppstod, vilket gjorde användarna frustrerade och irriterade över situationen. Det bör kunna lösas med ytterligare utbildning av personalen och om användargränssnittet skulle vara tydligare. Problem med att liknande information skrivs in i journalen på flera ställen bör ses över, vilket kommer att göras enligt de intervjuade. All personal behöver erhålla en gemensam syn på hur information bör registreras för att undvika redundans, vilket spar lagringsplats men framförallt tid vilken kan ges till patienten.

Patientinformation fanns tillgänglig på flera ställen på expeditionerna förutom i datorn, bland annat genom medicinlistor och laboratoriesvar, vilka kan komma obehöriga till del. Datorskärmarna däremot var placerade på ett sådant sätt att förbipasserande inte kunde ta del av känslig information utan att vara tvungna att gå in på expeditionen för att se vad som står. Vilket är en av de punkter som Datainspektionen ger som rekommendation till organisationer när det gäller datorskärmens placering.

Information som skrivs ut på skrivare från datorjournalen kan av misstag glömmas och kan bli tillgänglig för obehöriga. En av de skrivare som används av personalen fanns i ett närbeläget rum som inte var låst, vilket gör det enklare att glömma utskriften än om skrivaren skulle stå i direkt anslutning till datorn.

Fax användes flitigt för att skicka patientinformation till andra vårdinrättningar. I nuläget är inte informationen krypterad och endast vid några tillfällen avidentifierade personalen informationen. Att personalen ringer in och talar om att ett faxmeddelande kommer att skickas är bra, för att personen ska kunna ta hand om meddelandet med en gång så att det inte blir liggande vid mottagarens fax. Att enbart få ett kvitto i efterhand ger inga garantier på att informationen kommer dit den ska eftersom den mänskliga faktorn gör att fel nummer kan bli uppringt. Personalen behöver få mer information om risker med att skicka information via fax eftersom de inte var medvetna om de problem som kan uppkomma.

5.3 Sammanfattning av material från intervjuer

Beskrivning av material från intervjuer med en systemadministratör och fyra sjuksköterskor. Frågorna som ställdes vid intervjuerna har placerats i olika kategorier (se bilaga 1) för att underlätta bearbetning av intervjumaterialet. Utifrån varje kategori har svaren på frågorna presenterats under liknande rubriker nedan.

5.3.1 Inledande frågor

Sjuksköterskorna som intervjuades har alla lång yrkeserfarenhet men det varierade hur länge de arbetat inom den division där observationerna och intervjuerna utförts. Som sjuksköterska arbetar de i team tillsammans med läkare, arbetsterapeuter, sjukgymnaster och undersköterskor. De arbetar med att samordna och planera vården kring patienterna och är delaktig i omvårdnaden av dem. Sjuksköterskorna utför dokumentation i datorjournalen i stor omfattning samt verkställer ordinationer från läkare. Sjuksköterskorna hade olika områden som de specialiserat sig på och ansvarar över. Antalet patienter som de ansvarar för varierar från 2-14 stycken beroende på bemanning.

Arbetet som systemadministratör består bland annat av att lägga till och ta bort användare, bygga termer, mallar och sökord till datorjournalen, sammanställa dikteringsmallar för läkare, revidera rutiner, samarbeta med leverantör för uppgraderingar och felanmälningar samt utvecklingsarbete. Vidare skall systemadministratören utbilda, stödja och vägleda användare om datorjournalen samt deltaga i förvaltargruppen för Melior.

Sjuksköterskorna har en varierande kunskap i att använda datorer. Alla hade tillgång till dator i hemmet men de använde den sällan eller aldrig. Utav de tillfrågade hade alla gått någon typ av utbildning där de använt sig av datorer. De har även tillgång att utbilda sig, exempelvis i Windows, Word och Excel, på arbetstid. Något de alla hade dragit nytta av.

De strategier som finns inom divisionen för att försäkra sig om att de informationskrav som lagen ställer efterföljs är att alla måste ha ett eget användar-ID och lösenord. De har även tre olika behörighetsnivåer i datorjournalsystemet; aktiv, inaktiv eller spärrad.

Aktiv: Användaren kan logga in i datorjournalen.

Inaktiv: Användaren kan ej logga in i datorjournalen, temporärt ledig. De inaktiverar användare som slutat hos dem men som de tror kan komma tillbaka någon gång i

framtiden, detta för att slippa lägga upp ett nytt ID. De som är borta på grund av exempelvis sjukdom eller föräldraledighet inaktiveras.

Spärrad: När användaren bytt till exempel titel eller namn men ska läggas upp på nytt med samma signatur eller användar-ID. De användare som slutar sin tjänstgöring inom organisationen kan även spärras.

Det är inte alltid som systemadministratören får reda på att personalen är borta. Administratören har gjort ett särskilt register i Excel över alla användare vilka är sorterad efter de olika användargrupperna, ansvarig sjuksköterska, sjukgymnast eller arbetsterapeut. Administratören kontrollerar med jämna mellanrum att listan stämmer.

5.3.2 Utbildning och information

Ingen av de tillfrågade har erhållit utbildning i informationssäkerhet. I det informationshäfte, som varje anställd får av systemadministratören när de börjar, går det att läsa att det är viktig att logga ut eftersom det är den inloggade personen som blir ansvarig om någon annan använder dess identitet och gör något otillåtet. Det står också att byta av lösenord mot nätet måste ske var sextionde dag och att de måste logga ut när de lämnar datorn. Vidare ges tips vid programproblem och vem som skall kontaktas när problem uppstår.

Det finns i nuläget inget utbildningsprogram i organisationen för att utbilda vårdpersonal i informationssäkerhet. På organisationens intranät finns Landstingets informationssäkerhetspolicy tillgängligt för de anställda samt att vårdcheferna har fått tagit del av policyn.

Den kunskap som användarna fått vad gäller säkerhetspolicy finns i informationshäftet och att de ansvariga för systemen påpekar att det är viktigt att logga in och ut på ett korrekt sätt. Organisationen följer inte upp och utvecklar policyn inom organisationen.

Någon specifik strategi för utbildning i säkerhetsfrågor fanns inte när datoriseringen av journalen började. De som hade tillgång till datorer i början var inte så många men de fick utbildning i samband med Melior infördes. Den utbildning som användarna fick var grundutbildning i Windows.

Information om författningar och regler vad gäller datorjournalen får användarna när de kommer som nyanställda i det häfte som tagits upp ovan. I samband med utbildning i Melior får de ett häfte där det står vikten av lösenord, att användarnamnet i kombination med ett hemligt lösenord gör det omöjligt för någon annan att gå in i journalen under din signatur. De användare som intervjuats har inte nämnt detta häfte. En av de intervjuade berättar istället att information kommer från systemadministratören eller vårdföreståndare direkt. De har även en informationspärm på expeditionen men den läses sällan eller aldrig av de personer som berättade om pärmen. Användarna själva skulle vilja få ytterligare information eftersom de inte tänker på vilka skyldigheter de har när de lämnar datorn påloggad och att information om säkerhet skulle ges med jämna intervall.

Användarna tycker att de påverkas av kraven på informationssäkerhet på flera sätt. Dels att det blivit flera säkerhetskontroller då de får göra inloggningar, vilket gör användarna frustrerade och irriterade för det tar alldeles för lång tid enligt dem själva. Dels att ständigt bli avbruten när de skriver i datorjournalen för att göra kortare ärenden och då vara tvungna att logga ur. De höga krav på sekretess är en svår punkt

tycker en av de intervjuade, exempelvis om en journal ligger framme kan vem som helst gå in på expeditionen och få tillgång till känslig information om patienter, vilket händer enligt personalen. Personen i fråga tänker sig mera för nu, i vilka journaler hon går in i, eftersom hon vet att hon måste kunna säga varför hon varit inne i en viss journal. Att identifiera en patient kan kännas otrevligt tycker en av sjuksköterskorna men det är tvunget för att kunna säkerställa identiteten på patienten.

5.3.3 Autentisering

De grundregler som finns, enligt de tillfrågade, för att kontrollera en patients identitet är att begära legitimation om personalen inte har kännedom om personen. Patienten ska med en identitetshandling kunna visa att de är den de säger sig vara. De kan även vara identitetsmärkta med ett band runt handleden, när de kommer från en annan avdelning. För att ID-märka en patient finns det strikta regler och vem som helst får inte sätta på bandet. På avdelningarna som berörts av studien får bara vårdföreståndaren sätta på bandet vilket inte fungerar i praktiken. Därför delegeras märkningen ut på några sjuksköterskor, vilket förnyas årligen. Om patienten själv inte kan identifiera sig, exempelvis om denne är medvetslös, då akutmärker personalen patienten med ett tillfälligt nummer fram till dess att patienten kan identifiera sig. I datorjournalen finns ett sökord ”Identitetskontroll” som sjuksköterskorna får fylla i vid registrering av ankomstsamtalet.

Personalen kontrollerar patientens ID-handling om att patienten har tillgång till en sådan. Flera av patienterna är gamla och har inte ofta vare sig körkort eller annan ID-handling. Vid fråga hur personalen gör då vet de inte riktigt för situationen uppstår sällan eftersom patienterna ofta kommer från annan avdelning eller vårdplats och redan är ID-märkta. När patienten redan är ID-märkt frågar personalen endast efter deras personnummer. Om det är en tillräckligt identifikation vet personalen inte.

Hur personalens identitet kontrollerades vid nyanställning är svårt att säga för de intervjuade har varit anställda under en lång tid och glömt av detta. En av de tillfrågade svarade med personbevis men övriga har inget minne av att de behövde legitimera sig.

Personalens identitet kontrolleras vid inloggning med ett unikt användar-ID som är samma till alla program som de har behörighet till. Personalen har också ett eller fler lösenord som de får ange vid inloggning till de olika programmen.

5.3.4 Autentisering och behörighetstilldelning

Flera av de tillfrågade har använt någon annans identitet när de skrivit i datorjournalen. Vid olika situationer har detta hänt exempelvis när de själva trott sig vara inloggade men upptäckt att så inte var fallet när de skulle signera aktiviteten som de skrivit in. En annan situation då det skett är när det varit rörigt och mycket att göra. De gånger det händer ber personen att den som är inloggad ska läsa igenom det hon skrivit och signera det istället. Detta istället för att göra om proceduren under hennes egen identitet. Personalen berättar att när det är stressigt och en person redan är inloggad mot servern går det att logga in med det egna lösenordet mot datorjournalen. Detta tycker personen att hon kan göra eftersom det går att spåra den som skriver i datorjournalen trots att någon annan är inloggad mot servern. Tre av de fyra intervjuade har inte tillåtit någon att använda sig av deras identitet men de säger

samtidigt att det säkert har hänt när de inte loggat ur på ett korrekt sätt. En av de fyra säger sig ha tillåtit andra att använda dennes identitet vid inloggning. Organisationen har inga rutiner för att kontrollera att personalen använder sin egen användaridentitet eller lånar någon annans. Istället blir personalen ansvarig för det som skrivs i datorjournalen eller annat program under den egna identiteten.

Personalen tycker det är jobbigt med in- och utloggningsproceduren för att det tar lång tid, men förstår samtidigt att den måste finnas. Några av de utfrågade är inloggade mot servern den mesta tiden när de arbetar men vet inte om detta är en riktig handling. De anser att det inte finns någon praktisk möjlighet att logga ur hela tiden, när de är tvungna att gå ifrån datorn en liten stund, vilket är stressande för dem. Önskvärt vore att kunna var inloggad hela tiden och att alla har sin egen dator. Några av de intervjuade önskade att det skulle finnas en timeout-knapp som de kunde trycka på exempelvis som det finns i Beakta-programmet, för att programmet skulle låsas och inte kunna användas av någon. Ett annat alternativ som kom upp under intervjuerna var att använda en skärmsläckare som gör att tillgängligheten till programmet låses efter en viss tid för att på så sätt slippa att logga ur hela tiden.

Alla beslut som tas angående tilldelad behörighet dokumenteras. Användarna delas in i olika grupper beroende på vilka program de behöver få tillgång till i sitt arbete. Beroende på vilka program användarna ska ha behörighet till skickas användar-ID till de olika systemadministratörerna, som få lägga upp användare för de olika programmen.

5.3.5 Behörighetstilldelning och lösenord

I datorjournalen ges ingen indikation på att byte av lösenord bör ske. De kan därför använda samma lösenord hela tiden vilket bekräftas av systemadministratören. Mot själva nätverket måste personalen byta var sextionde dag då de får en påminnelse att detta ska göras exempelvis inom fem inloggningar. I Beakta, ett vårdmätnings-program, får de byta var fjärde vecka då det ger indikation på att detta bör göras. Att byta lösenord i de olika programmen gör att personalen använder sig av olika system för att inte glömma bort de olika lösenorden.

De anställda har flera olika lösenord som de måste komma ihåg. De som intervjuats använder 3-4 stycken lösenord utan att räkna med lösenordet för stämpelklockan. För att komma ihåg dessa använder personerna olika system. En av personerna byter i alla program samtidigt, en annan har ett system att hon ökar på siffran i slutet av lösenordet och en tredje skriver upp sina lösenord i en bok som hon har liggande på expeditionen. På expeditionen har de även de lösenord som de använder gemensamt insatta i en pärm. Dessa lösenord går till program på Internet där de beställer exempelvis mat, förrådsmateriel och städmaterial. Vid semestrar skriver flera av de intervjuade upp sina lösenord för att inte glömma bort dem under sin semester. Att diskutera sina lösenord är det ingen av de intervjuade som gjort men enligt en av de intervjuade har de flesta lösenorden nedskrivna i anteckningsboken som de har i fickan.

Tre av de intervjuade har ett lösenord som är kopplat till en nära anhörigs namn eller liknande, vilket de kombinerat med siffror.

5.3.6 Sekretess

De rutiner som finns i organisationen som påverkar vilka personer som ska få access till information i datorjournalen är att all personal, utom fritidsledaren, har tillgång till allt. Dessutom är den information som kuratorer och psykologerna skriver spärrad. Vid förfrågan till sjuksköterskorna svarade de att de har skriv- och läsrättighet i datorjournalen medan undersköterskorna enbart har läsrättighet. Ingen av dessa yrkeskategorier har läs- eller skrivrättighet till psykologernas eller kuratorernas akter. Sjuksköterskorna kan även gå in och signera vad en annan sjuksköterska skrivit men vid frågan om de kan signera en läkares skrift visste inte vederbörande detta. Vid samtal uppkom det att det är önskvärt att få en genomgång regelbundet för att diskutera vad personalen får och inte får göra i datorjournalen. Personalen tycker ändå att rutinerna för accessrättigheterna är tydliga och att de blev underrättade om dem när de anställdes, i den utbildningen de fick i datorjournalsystemet. Organisationen har ett stort antal rutiner för olika regler och författningar som bland annat revideras av systemadministratörerna och det är på det sättet som organisationen kontrollerar att de upprätthålls.

Obehöriga förhindras access till datorjournalen genom användar-ID och lösenord men ingen visste om informationen i systemen var krypterad. Att skyddet kan förbättras är upp till personalen anser de intervjuade, om de sköter in- och utloggningen, och i jämförelse med pappersjournalen är datorjournalen säkrare. Ett komplement till skyddet skulle vara om en skärmsläckare gick på efter en viss tid eller en timeout-knapp som förhindrar den direkta tillgången till informationen vilket tagits upp tidigare.

Personalen har tillgång till fax och e-post men för att skicka patientinformation till andra vårdinrättningar använder de enbart fax. Den fax som används krypterar inte informationen som skickas. Användarna ringer upp den person som ska få tillgång till informationen och talar om att de skickar faxmeddelandet, denne i sin tur ska ringa tillbaka när meddelande anlänt men det görs inte så ofta. Informationen är oftast inte avidentifierad utan skickas som den är. Personalen skickar med ett försättsblad som anger till vem meddelandet hör och att de ska ringa och bekräfta meddelandet. Personalen får i efterhand ett kvitto på att meddelandet gått iväg till det uppringda numret.

Personalen kontrollerar inte att mottagaren är behörig att få tillgång till patientinformationen men de måste se till att de har patientens samtycke till att skicka över informationen. I datorjournalen finns ett sökord där personalen kan skriva in om patienten gett sitt samtycke till att information skickas utanför det egna sekretessområdet.

5.3.7 Oavvislighet

Personalens osignerade aktiviteter kan ligga i datorjournalen under lång tid men systemadministratören går in och kontrollerar detta och skickar ett e-post meddelande om det finns många osignerade aktiviteter. En av de intervjuade hade osignerade utvärderingar kvar sedan år 1999. Informationen hade inte gått fram om att detta skulle göras och flera av de intervjuade visste inte hur länge en osignerad aktivitet kunde finnas kvar i datorjournalen. Flera av de osignerade fallen berörde personer som i dag är avlidna.

5.3.8 Spårbarhet

Allt som personalen gör i systemen loggas. Detta gäller även Internet- och e-postanvändning. Det är enbart systemadministratören som hanterar och kan kontrollera loggfilen över datorjournalen. Administratören har tillgång till ett program, Syslog, för att göra kontroller av loggfilen. I dag finns inga rutiner på att kontrollera loggfilen och administratören har aldrig kontrollerat loggfilen. Personalens vetskap om vilken information som loggas i systemen eller om det görs är dålig. De hade inte fått någon information om vad som loggas och hur loggfilen hanteras eller kontrolleras. Personalen var ändå positiv till att systemen är loggade eftersom behörigheten kan missbrukas. De tyckte att det var en trygghet både för dem själva och för säkerheten mot patienterna. En av de intervjuade kunde dock känna att det är jobbigt att veta att ”storebror ser dig”.

5.3.9 Integritet

Att komma ihåg patientinformation om flera patienter samtidigt tyckte flertalet inte var något problem. De hade olika system för att komma ihåg att registrera informationen på patienterna. Alla förde någon typ av minnesanteckningar i ett anteckningsblock som de bar med sig i fickan. Det som en av de intervjuade istället ansåg vara jobbigt var att datorjournalen inte är överskådlig utan personalen skriver anteckningar på flera olika sökord istället för att skriva i kronologisk ordning. Detta skulle de för övrigt få lära sig inom en snar framtid.

Att det finns olika rättigheter för att läsa och skriva har redan framkommit tidigare men hur användarna får ändra eller ta bort i datorjournalen var inte alla de intervjuade helt säkra över. Exempelvis hur de ska göra när de skrivit in på fel patient som händer alla någon gång enligt de intervjuade personerna. Enligt administratören har sekreterarna en högre behörighet då de till exempel kan byta personnummer om det är någon patient som fått ett tillfälligt nummer eller om någon skrivit in fel personnummer på en patient, som har hänt vid ett tillfälle. Vid intervjuerna framkom det även att personal tillåter studenter att träna på att skriva och arbeta i datorjournalen under deras identitet.

Hur data sparas var oklart men troligtvis sparas den på disk och det framkom inte om den var krypterad. Data är alltid tillgänglig för de har ingen gallringsplan att spara undan data på annan plats.

Obehöriga kan få tillgång till patientinformation som skrivs ut på skrivare och glöms kvar i de lokala skrivarna. Det finns även en nätskrivare att tillgå men den finns i ett separat rum som är låst.

En kopia skrivs ut av vad som registrerats i datorjournalen på inneliggande patienter när epikrisen, de slutanteckningar som görs om patienten, är signerad och hela vårdtillfället är avslutat. När patienten är på mottagning eller om någon ringer in görs anteckningar i datorjournalen som skrivs ut direkt i en papperskopia för att arkiveras.

Datorjournalen är tillgänglig dygnet runt alla dagar, även helger. En backup körs varje natt och varje timma görs även en backup på transaktionsloggen. Backup görs först till disk som sedan förs över till band. Om de till exempel ska uppgradera till en ny version så meddelas användarna om driftstoppet i förväg och avdelningspersonalen kan då skriva ut den information de behöver för de inneliggande patienterna under de timmar som uppgraderingen pågår.

5.3.10 Avslutande frågor

Personalen tänker inte alltid på att de har att göra med känslig information för det blir en del av arbetet. Att skriva in informationen i datorjournalen har blivit svårare på grund av att patienten ska få tillgång till att läsa sin journal vilket gör att de får tänka sig för hur de formulerar sig. Det som står om patienten ska vara det som patienten upplever, exempelvis vid samtal, och inte så som sjukvårdspersonalen anser det vara. Ett annat exempel är om patienten missbrukar narkotika eller har gjort försök till självmord om sjuksköterskan ska skriva det eller inte. En sjuksköterska tycker det vore bra att få samtala om dessa bitar för att få en tankeställare om hur de gör när de registrerar information.

När det blir avbrott i tillgängligheten till datorjournalen orsakar det stor irritation och frustration. Det blir kaos enligt de intervjuade sjuksköterskorna, inte så att de inte kan ta hand om patienterna men det upplevs som jobbigt. De tycker det är besvärligt att inte ha informationen tillgänglig. Vet de om att det blir driftstopp skriver de ut alla journaler och sätter in dem i en pärm. Sedan får de föra anteckningar för hand som de i efterhand skriver in i datorjournalen. Personalen gör det på ordinarie arbetstid vilket tar tid ifrån patienterna. Informationssäkerheten påverkas enligt de intervjuade av att informationen då ligger framme i pärmar då det blir enklare för obehöriga att få tillgång till informationen. När de sedan skriver in anteckningarna i datorjournalen igen händer det att de får signera någon annans anteckningar, vilket inte är riktigt. Andra yrkesgrupper som vill få tillgång till information om patienten för att genomföra behandling kan få tillgång till för lite information för att informationen inte är införd ännu utan fortfarande sitter i pärmen.

Trots det har tillgängligheten till informationen i datorjournalen blivit bättre om personalen jämför med pappersjournalen. De behöver inte springa och leta efter den utan den finns alltid tillgänglig. Det som krävs är att alla måste lära sig att läsa journalen på ett korrekt sätt och att läsa och skriva in på rätt sökord.

Kraven i vårdarbetet har ändrats under åren, särskilt dokumentationsansvaret och omvårdnadsansvaret. Den tysta kunskap som vårdpersonalen har i huvudet ska nu föras in i datorjournalen enligt de lagar som finns. Enligt en sjuksköterska kräver arbetet att de har en relativt stor datorkunskap och att det ligger i deras eget ansvar att söka kunskap om de inte kan. En sjuksköterska utryckte att hon ”känner att de värderas av hur de gör sina pappers- eller datorarbeten och inte hur de vårdar patienten”.

Arbetsförhållanden inom divisionen verkar vara bra. De intervjuade trivs med sitt arbete och de kan planera och påverka inläggningen av patienter. Verksamheten flyter då på vilket är viktig för att kunna ge en bra vård.

5.4 Analys av intervjumaterial

Samtliga intervjuade sjuksköterskor hade lång erfarenhet av sitt arbete men det varierade hur länge de varit inom divisionen. Sjuksköterskorna samarbetar med flera yrkeskategorier och får vara ”som spindeln i nätet” som en av de intervjuade uttryckte det.

Personerna som medverkat i studien hade varierande kunskaper i att använda datorer från att vara nybörjare till att vara ”medelkunnig”. De hade alla genomgått utbildning i att hantera olika program genom arbetet. Flera av de intervjuade berättade att de

tagit avstånd från datorn så länge det gick och utbildningen kan vara avgörande för om de ska våga använda tangenterna och inte vara så rädda. Vilket talar för att utbildning är mycket viktigt i sammanhanget.

För att säkra att de informationskrav som lagen ställer efterföljs har de inom divisionen olika strategier. Alla måste använda ett eget användar-ID och lösenord och datorjournalsystemet är indelat i olika behörighetsnivåer, aktiv, inaktiv och spärrad.

Systemadministratören får inte alltid reda på att personalen är borta, vilket är viktigt för att denne ska kunna kontrollera att inga kvarvarande accessrättigheter finns kvar på de som slutat sin anställning. Administratören har därför konstruerat en lista för att kunna kontrollera att användarna är i tjänst, vilket kontrolleras med jämna mellanrum. Denna rutin är viktig för att inga obehöriga ska få tillgång till patientinformation de inte längre behöver i sin tjänst. Ett förslag till förbättring av denna rutin är att administratören får ett automatgenererat e-postmeddelande från personalavdelningen när personal är borta en längre tid eller slutar sin tjänst.

5.4.1 Information och utbildning

Samtliga av de intervjuade svarade att de inte genomgått utbildning i informationssäkerhet och att det inom organisationen inte finns något utbildningsprogram vad gäller informationssäkerhet. Den kunskap om informations-säkerhet som användarna får i dagsläget är vid nyanställningen, då de erhåller ett välkomsthäfte där de informeras om hur de skall logga in på nätet, byta lösenord, att alla måste logga ut när de går ifrån datorn och så vidare. Vid utbildning av datorjournalsystemet, Melior, får de ytterligare ett häfte där de informeras av vikten av att använda sitt lösenord på ett korrekt sätt. Information om organisationens informationssäkerhetspolicy finns att tillgå på organisationens intranät men under intervjuerna har det inte framgått att personalen känner till detta. Det talar för att ytterligare information till och utbildning av personalen vore värdefull.

Enligt användarna själva anser de att de påverkas av kraven på informationssäkerhet på olika sätt. De får göra flera inloggningar är förut, vilket tar mycket tid i anspråk. När de sitter och registrerar information om patienter blir de ofta avbrutna och är då tvungna att logga ut vilket känns onödigt vid kortare ärenden. En av de intervjuade förtydligar en sådan situation, när det sker ett patientlarm går patienten i första hand och inte att de ska logga ut ur datorn. De höga kraven på sekretess är svåra att uppnå rent praktiskt i deras arbete anser en av de intervjuade och obehöriga får tillgång till information de inte skulle få vetskap om. Samtidigt tänker en av personerna efter mer nu, eftersom hon måste kunna redogöra varför hon varit inne i vissa journaler. Att be om en patients ID-handling kan anses som stötande och är därför en uppgift som anses otrevlig att utföra. Det är viktigt att informera patienterna om varför personalen måste utföra identitetskontroll.

Personalen efterfrågar information om informationssäkerhet eftersom de inte tänker på vilka skyldigheter de har, vilket är viktigt för att säkra patientinformationen. Även i detta fall skulle information till och utbildning av personalen fylla en viktig funktion.

Enligt de intervjuade personerna fick de ingen utbildning i frågor som berör övrig IT-säkerhet, utöver det som finns i häftet när datoriseringen av journalen började och någon strategi för säkerhetsutbildning fanns inte. Den utbildning som användarna får om IT-säkerhet är i likhet med den ovan vad gäller informationssäkerhet. Information om regler och författningar får personalen vid nyanställning och genom

administratören och vårdföreståndaren. Personalen har tillgång till en pärm på expeditionen där de sätter in information men den fyller till synes inte sin funktion eftersom enbart två av de intervjuade talade om att den fanns men att de nästan aldrig använde den.

5.4.2 Autentisering, behörighet och sekretess

Personalen ska enligt lag utföra kontroll av patientens identitet. De ska även ange i datorjournalsystemet på vilket sätt kontrollen har skett. Till divisionen kommer ofta patienterna från någon annan avdelning eller vårdinrättning och är därför redan ID-märkta med ett band. Personalen frågar oftast bara om personnummer men personalen är osäker på om det räcker. Om personer får tillgång till ett ID-band skulle det vara enkelt för dem att uppge fel identitet eftersom kontrollen inte är mer omfattande. När patienter kommer utifrån till avdelningen ber personalen patienten om ID-handling. Problemet är att patienterna ofta är gamla och inte har vare sig körkort eller annan identitetshandling. En osäkerhet finns hur personalen ska göra vid dessa tillfällen. Ett alternativ till personnummer är det akutnummer som patienter får når de inte själva kan identifiera sig exempelvis vid medvetslöshet. Detta nummer bör kunna användas då patienter inte har någon identitetshandling.

Identitetskontroll av nyanställd personal är viktig för att ingen obehörig personal ska kunna arbeta med patienterna, den dyrbara utrustning och de mediciner som finns på ett sjukhus. Kontroll bör därför göras när anställningen sker. Om det görs i dagsläget har inte framkommit under studien eftersom de flesta av de intervjuade arbetat en längre tid inom vården och inte kommer ihåg om de behövde legitimera sig. Noteras bör ändå att den person av de intervjuade som anställdes sist inte har något minne av att de bad om någon typ av identitetshandling när denne anställdes.

Det sätt som personalens identitet kontrolleras vid inloggning mot servern och olika program var med hjälp av ett användar-ID och lösenord.

Att personal använder varandras identitet är naturligtvis inte bra ur patientsäkerhets-synpunkt men också för deras egen skull. Att personalen ofta slarvar med säkerheten redogör även Datainspektionen (1998) för i sin rapport där ett av skälen sägs vara att säkerhetsåtgärderna uppfattas som en belastning i det redan hårda arbetsbelastningen. Problemet med att de är inloggade på varandras identitet uppkommer i de flesta fall när de det var stressigt och mycket att göra eller att de trott att de själva var inloggade. Att de själva tror att de är inloggade visar på att de inte skött utloggningen på ett korrekt sätt eftersom de gått från datorn och kommit tillbaka för att fortsätta där de slutade. När inskrivning i journalen redan påbörjats ber personen den inloggade att kontrollera och signera i dennes ställe för att slippa göra om proceduren under den egna identiteten. Några förslag på hur problemet skulle kunna lösas kan vara med smarta kort, vilket användaren identifieras med tillsammans med ett användar-ID och lösenord. Användarna kan ta ur kortet och datorn kan användas av annan användare. När användaren gjort kortare ärenden behöver de endast sätta tillbaka kortet och skriva in sitt lösenord vilket förkortar tiden för inloggning. Vidare skulle en skärmsläckare eller en knapp kunna användas för att hindra obehörig tillgång till programmen. Skärmsläckaren bör starta efter en viss tid och göra programmen oåtkomliga för de personer som inte har tillgång till rätt lösenord. Den knapp som skulle kunna användas fungerar på liknande sätt som skärmsläckaren och avbyter då programmet.

En person säger sig kunna gå in med en annan persons identitet mot servern och sin egna mot datorjournalen, vilket inte bör fungera utan att systemen säger ifrån när detta sker. Merparten av de intervjuade tillåter inte andra att använda den egna identiteten men att någon gör det påvisar att informationen om riskerna i samband med behörighet och identitet inte varit tillräcklig. Organisationen har inga rutiner för att kontrollera detta utan påpekar för personalen att de blir ansvariga för vad som görs under den egna identiteten. Samtliga intervjuade vet om att de är ansvariga för vad som skrivs under den egna identiteten men samtidigt verkar de inte vara medvetna om de risker de tar eftersom det inte görs på ett korrekt sätt.

Byte av lösenord bör ske med jämna mellanrum och detta görs också mot servern och i programmet Beakta, där indikation gör att användarna måste byta inom ett visst antal inloggningar. I datorjournalen däremot finns inte något krav från systemet på att byte av lösenord bör ske, vilket bör ses över eftersom det i detta system ligger mest känslig patientinformation. Vid intervjuerna framkom också att personalen inte behöver byta lösenord i datorjournalen. Hur personalen gör med byte av lösenord varierar.

Att personal har flera olika lösenord att komma ihåg gör att de behöver något slags system för att hålla dessa i minnet. I intervjuerna berättade samtliga att de använder sig av olika system. Att använda anhörigs namn och att skriva upp lösenorden anses vara mindre bra eftersom de enkelt kan listas ut och komma i orätta händer. I intervjuerna framkom det att båda dessa system används för att personalen inte ska glömma sitt lösenord. Under intervjuerna framkom det att kollegor enkelt skulle kunna lista ut lösenordet vilket inte är bra. Ofta är inte personer medvetna om att det är den egna personalen som gör mest skada, medvetet eller omedvetet, vilket personal behöver upplysas om vilket stöds av Meyer m.fl. (1998).

De beslut som tas angående behörighet dokumenteras och användarna delas in i grupper beroende på vilka program de behöver för att utföra sitt arbete. I organisationen finns rutiner som påverkar vilka som ska få access till information i datorjournalen. De flesta ur personalen, utom fritidsledaren, har tillgång till att läsa nästan all information i journalen, även på avdelningar inom divisionen vilka de inte arbetar på för tillfället. Det som kuratorer och psykologer skriver är dock spärrat. Beroende på vilken yrkesgrupp användaren tillhör kan de även få skrivrättigheter. Att få behörighet till mer information än vad som behövs för arbetet kräver att skyddet kompletteras med en loggningsfunktion och att personalen vet om att de loggas. Personalen uppgav att det vore önskvärt att få information regelbundet om vad de får och inte får göra i datorjournalen. I jämförelse med pappersjournalen ansåg personalen att datorjournalen är mer säker ur sekretessynpunkt, vilket också Dahlin och Arnesjö (1996) anser vara ett av de mervärden som finns med datorjournalen.

Vid de tillfällen fax används för att skicka information gör de oftast det utan att avidentifiera patientinformation, vilket inte är korrekt. Information som inte är krypterad kan avlyssnas på vägen till mottagaren då obehöriga får tillgång till känslig information om patienter. Att föra över information som inte är krypterad gör att andra kan ta del av informationen om personalen ringer upp fel nummer när de skickar faxmeddelanden. Personalen var inte insatt i eller tänkte på att problem kunde uppstå när de skickar meddelanden, vilket de behöver få vetskap om.

5.4.3 Oavvislighet

De intervjuade personerna kontrollerar inte att mottagaren är behörig att få tillgång till patientinformation när de samtalar per telefon eller när de använder sig av faxen. De flesta litar på att de är den person som de uppger sig vara, vilket de troligtvis är. Personerna kontrollerar enbart att patienten gett sitt samtycke till att information får ges ut utanför det egna sekretessområdet. Någon sorts kontroll skulle vara önskvärd för att inte patientinformationen ska skickas iväg till obehöriga.

Hur länge osignerade aktiviteter kan finnas i en datorjournal vet inte någon av de intervjuade sjuksköterskorna. Eftersom personalen glömmer att utföra signeringar bör systemet ge indikation på hur många osignerade aktiviteter som personen har exempelvis vid inloggning i datorjournalen för att göra användaren uppmärksam på situationen. En orsak till att en av intervjupersonerna inte signerat sina utvärderingar kan vara att det finns brister i användargränssnittet, vilket gör att användaren inte uppfattar var handlingen skall eller bör ske. Information till och utbildning av personalen om dessa frågor är viktig för att inte ovan nämnda situationer ska uppstå.

5.4.4 Spårbarhet

All åtkomst till personregister som innehåller känslig information bör enligt Datainspektionens rekommendationer loggas och kontrolleras fortlöpande. Under intervju med systemadministratören framkom att systemen loggas men att ingen kontroll av loggfilen genomförs och att det inte finns någon rutin för att göra det. När systemen loggas bör personalen få vetskap om att så sker och hur loggfilen hanteras och kontrolleras. De intervjuade var positiva till att de var loggade och en av respondenterna uttryckte att det görs för förtroendet mot patienterna, bryter vi mot det så tappas förtroendet för det vi gör. En rutin bör dessutom utvecklas för att kontrollera loggfilen och informera personalen att det görs och varför.

5.4.5 Integritet

Personal ska enligt Datainspektionens rekommendationer vara vaksam vid registrering av känsliga uppgifter så att ingen förväxling av personnummer eller registrering på annans personnummer sker. Flertalet av de intervjuade tyckte inte att det var något problem att komma ihåg på vilken patient de skulle föra in vilken information. Trots det hade alla registrerat in fel information på fel patient någon gång. En av respondenterna påpekade att hon behöver lugn och ro för att hon inte kan koncentrera sig när kollegor sitter och läser, skrattar och när det väsnas runt omkring henne. Ytterligare en orsak till att fel uppstår kan vara att de ofta blir avbrutna när de registrerar information om patienterna. Det som personalen istället upplevde som problematiskt var att journalen inte var överskådlig och att personer skriver in liknande uppgifter på olika sökord. Att standardisera begrepp inom organisationen men även inom hälso- och sjukvård skulle bidra till enklare informationshantering.

Att personalen alltid hanterar känslig information kan enkelt glömmas bort eftersom det blir en del av arbetet. En av respondenterna uttryckte det som så ”(…) att naturligtvis färgas jag av mina egna värderingar, det vill ju verkligen till att jag skriver vad patienten känner”. Att personal tillåter studenter att träna, skriva och arbeta i datorjournalen under personalens egna identitet och behörighet är inte bra ur informationssäkerhets synpunkt. De anställda bör informeras om att de istället enbart

bör använda den fiktiva datorjournalen som finns att tillgå i utbildnings syfte. Upplysning och information med jämna mellanrum skulle vara värdefullt för att påminna personalen om vilken typ av information de behandlar i sitt dagliga arbete, vilket stöds av Gratte (1996).

Alla vårdtillfällen skrivs ut i en kopia för att sparas i ett arkiv, vilket ställer stora krav på informationssäkerheten. Risk finns att information glöms att skrivas ut eller att utskrivna dokument kommer bort vid hanteringen.

Vid de tillfällen när tillgängligheten till datorjournalen går ner orsakar det stor irritation och merarbete för personalen. Att inte få tillgång till patientinformation upplevs besvärligt av personalen, vilket är ett problem med den datoriserade journalen. De skriver då ut alla patienters journaler och skriver noteringar för hand vid de avbrott som personalen får vetskap om i förväg. När dessa noteringar ska föras in i datorjournalen kan en sjuksköterska signera någon annans anteckningar vilket inte är riktigt. Sköterskan ska inte ta del av information om patienten som hon inte behöver för att kunna ge en bra vård och kan för övrigt inte garantera att uppgifterna är riktiga. Att andra yrkesgrupper inte får tillgång till korrekt information om patienterna vid rätt tidpunkt, eftersom informationen fortfarande är kvar i pärmen, kan orsaka felbehandlingar. Enligt Meyer m. fl. (1998) måste vårdpersonal få tillgång till rätt patientdata för att kunna ställa rätt diagnos och för att ge korrekt vård.

Tillgängligheten till patientinformation har blivit bättre när de övergått till datorjournal och dokumentation tar inte längre att tid att utföra vilket en av respondenterna poängterade.

Utifrån bakgrunds- och analyserat material kommer slutsatser att dras från den tidigare nämnda problempreciseringen. Dessa slutsatser presenteras i efterföljande kapitel.

6 Slutsatser

Hälso- och sjukvården är en informationsintensiv verksamhet vilket kräver att all personal inom organisationen vet vad begreppet informationssäkerhet innebär. Vidare måste ledningen känna ansvar och engagemang för att en informationssäker miljö ska erhållas. För att en säker miljö ska kunna skapas bör en informationssäkerhetspolicy samt riktlinjer och strategier att arbeta efter tas fram. Därefter bör en säkerhetsplan tas fram, vilken på ett strukturerat sätt beskriver hur organisationen ska arbeta med informationssäkerhet.

Hantering av information bör ske på ett sätt som genererar större säkerhet för patienten. Dessutom bör hanteringen medföra att personalen inom vården ska får mer tid att ägna sig åt att ta hand om och vårda de som kommer till sjukvården, vilket är deras huvudsakliga uppgift (Sågänger & Utbult, 2000).

Utifrån arbetets problemprecisering:

- *Hur påverkas användaren av kraven på informationssäkerhet i datorjournaler?*
- *Hur påverkar användaren informationssäkerheten i datorjournaler?*

kan nedanstående slutsatser tas fram.

Resultatet tyder på att inte tillräckliga åtgärder vidtagits ur ett informationssäkerhetsperspektiv eftersom det finns brister i det sätt personalen arbetar på. För det mesta är personalen enligt France (2001) inte medveten om hur de ska hantera den datoriserade journalen och de informationssäkerhets problem som kan uppstå något som även resultaten från studien visar.

Användarna *påverkas* av kraven på informationssäkerhet genom att:

- *inloggningsfunktionen inte fungerar på ett tillfredställande sätt*, exempelvis genom det sätt som inloggningen sker på vilket inte är anpassat efter hur användarna arbetar, vid byte av lösenord i systemet, in- och utloggning tar lång tid och svårigheter uppkommer med att komma ihåg lösenord.
- *användaren inte är medveten eller har tillräcklig kunskap*, om exempelvis informationssäkerhet, olika regler och föreskrifter, olika funktioner i datorjournalsystem, risker, hotbilder.
- *systemen loggas*, för att stödja spårbarhet.
- *avbrott sker i tillgängligheten* till datorjournalen.

Den arbetsmiljö som användare, av datorjournalen inom vården, arbetar i kan vara stressande. Resultatet av undersökningen visar på att användarna har otillräcklig kunskap om systemen, att systemet inte riktigt är funktionellt anpassat efter användarnas arbetssituation och att svarstiderna vid in- och utloggning är långa.

Vidare visar resultaten att användarna har många samtidiga arbetsuppgifter, exempelvis när telefoner och patienter ringer samt kollegor kommer för att få råd. Att personalen sedan blir störda av olika ljud när de ska registrera information är även en faktor som behöver tas i beaktning för att det inte ska påverka datakvaliteten.

Ovanstående är några av de faktorer som Engström (2002) beskriver som stressrelaterade. De risker som finns vid arbete där någon av dessa faktorer påvisas är

belastningsskador, konflikter, felaktig data vid registrering och utskrift, ökad sjukfrånvaro och ”utbrändhet”. För att undvika att detta uppstår bör användarna bland annat få en grundlig utbildning i hur datorn och systemen fungerar (Engström, 2002).

Resultaten tyder även på att vårdpersonal registrerar liknande patientinformation i datorjournalen under olika begrepp, vilket gör att personalen får läsa på flera ställen i journalen för att erhålla en helhetsbild. Att information skrivs in på olika ställen i journalen gör att viss patientinformation kan utelämnas vid utredning, vilket kan medföra att fel beslut tas för behandling.

Användare kan på grund av okunskap om informationssäkerhet, datorer och skickande av faxmeddelande påverkas negativt eftersom de inte vet att de gör på ett felaktigt sätt. De kan bli ansvariga för att medverka i en felaktig handling utan att de har vetskap om att handlingen är felaktig.

Davey (2001) menar att organisationen ofta förbiser eller ignorerar användarens intressen i säkerhet och ansvar för säkerheten. Ett sådant tillvägagångssätt räknas nästan till att nonchalera användarna. Detta på grund av att det är användarna och deras patienter som blir lidande av säkerhetsöverträdelser och i något fall kan dessa bli allvarliga. Den viktigaste orsaken att involvera användarna är att de är ansvariga för sina handlingar och resultaten i informationssystemen. De ska uttryckligt förstå hur ansvaret kan påverkas av andras handlingar vilket de vanligtvis inte har någon kontroll över (Davey, 2001).

När användarna får behörighet till mer patientinformation än vad arbetet kräver för att vårda patienten bör användaren få vetskap om vilka regler och författningar de har att följa. Detta för att inga tveksamheter ska uppstå kring vad de får och inte får göra vid hantering av känslig information.

Resultat från undersökningen tyder på att alla användare inte vet om att systemen inom vården loggas och hur verksamheten hanterar och kontrollerar loggfilen. Enligt Engstöm (2002) har användarna rättighet att få utbildning och information om vilka rutiner organisationen har vad gäller hantering och kontroll av loggfilen och vilken data som sparas i loggfilen. Trots att användarna inte vet om att systemen loggas tyder resultaten på en förändring till det bättre i hur användare känner för att vara loggade utifrån den rapport som Furnell m fl. (2000) skrev. Användarna är positiva till att system loggas dels för att de ska få förtroende från patienterna för det arbete de utför och dels för sin egen säkerhet. Detta tyder på att användarna har förstått de skäl som finns för att logga system med känslig information.

Studien visar på att viss svårighet finns i att komma ihåg flera olika lösenord vilket gör att användare har enkla lösenord som är sammankopplade med anhörigas namn och några användare skriver ner sina lösenord för att inte glömma, vilket bekräftas av Furnell (2000). Enligt Dahlin och Arnesjö (1996) bör byte av lösenord i olika systemen ske minst en gång i kvartalet eller när någon råkat se användarens lösenord. Studien visar på att användarna inte får någon indikation från datorjournalsystemet att byte bör ske vilket kan göra att användarna glömmer denna åtgärd.

Resultatet från studien tyder även på att användarna påverkas på ett negativtsätt när avbrott sker i tillgänglighet till information i datorjournalen. Avbrott medför merarbete för personalen eftersom de är tvungna att utföra dubbelregistrering av patientinformation. Trots det är personalen positiv till datorjournalen och att tillgängligheten till information har förbättras gentemot att använda pappersjournal. Personalen behöver nu inte leta efter patienternas journaler utan den finns alltid

tillgänglig i datorn när de som har behörighet behöver journalen samt att utföra dokumentation inte tar längre tid än vid inskrivning i pappersjournal.

Användaren *påverkar* informationssäkerheten i datorjournaler bland annat genom att:

- *in- och utloggningsfunktionen inte fungerar på tillfredställande sätt*, exempelvis att användaren lämnar påloggad dator utan uppsikt när denne gör annat ärende, använder annan persons identitet och behörighet
- *information hanteras och registreras på felaktigt sätt*, exempelvis genom att användare lätt kan glömma utskrifter vid skrivare, att inte kontrollera att mottagare har behörighet att få tillgång till information, registrerar information på fel patient eller skickar patientinformation via fax utan att avidentifiera informationen
- *brister i och otillräcklig kunskap* om, exempelvis de program som används då ofta handhavande problem uppstår och att information registreras på flera ställen i datorjournalen. Rutiner för hur signering ska genomföras eller att användaren har enkla lösenord som exempelvis kan associeras till anhörig men även att lösenorden finns nedskrivna

Det krav som ställs på användare av datorjournal att logga in och ut med sin användaridentitet följs inte vid varje tillfälle. Användarna är inte alltid medvetna om de risker de tar när de inte loggar ut eller överlåter den egna identiteten till annan anställd. Attityden med att inte logga ut för att det är praktiskt omöjligt måste arbetas bort för att inte bristerna ska tillta. Utbildning bör vara till hjälp vid förändring av dåliga inloggningsrutiner men även ledningen bör se till att användarna får tid till att använda de säkerhetsrutiner som finns. Dessutom bör en enkel och säker in- och utloggningsrutin ställas som krav till systemleverantörerna, något som också Datainspektionen (1998) påpekar i sin rapport för att inte systemen ska bidra till olämplig användning av behörighetskontrollen genom ett långsamt och krångligt inloggningsförfarande.

Att systemen stödjer oavvislighet, exempelvis vid signering av aktivitet, är till hjälp men inte tillräckligt eftersom resultatet visar att rutiner saknas eller är ofullkomliga kring när personalen exempelvis ska registrera och signera någon annans patientanteckningar efter avbrott i datorjournalen. Att information inte finns tillgänglig när det är avbrott i datorjournalen är ett problem som kan få allvarliga konsekvenser. Smith och Eloff (1999) menar att brister i tillgängligheten och integriteten av patientdata kan leda till att liv förloras.

Vidare tyder resultaten på att en viss osäkerhet finns bland sjukvårdspersonal om vad de får och inte får göra vid hantering av patientinformation vilket gör att de hanterar information på ett felaktigt sätt. Den okunskap som användarna har vid att använda datorn och de program som arbetet kräver gör att informationssäkerheten påverkas. System bör därför ge tydlig indikation och stöd till användaren när denne gör någon felaktig handling för att på detta sätt påminna och uppmärksamma användaren på att något felaktigt skett.

Resutatet visar även tydligt på att det erfordras en planerad och kontinuerlig utbildning inom hälso- och sjukvården om informationssäkerhet, risker, hotbilder och betydelsen av metoder och metoder för att ge förtroende för integriteten hos både patienter och personal. Säkerhet kan enligt Furnell, Warren och Evans (2001) endast erhållas om all personal med behörighet vet, förstår och accepterar nödvändiga

säkerhetsåtgärder. Lämplig säkerhetsutbildning och uppmärksamhet är nödvändig för att få personalen att förstå de följder deras handlande får mot säkerheten och genom förståelsen motverka onödiga risker (Furnell m fl., 2001; Björner 2000).

Enligt Furnell m fl. (2001) är många IT-användare nu medvetna om generell säkerhet, som hackning, virus och problem som orsakas av dessa. Kunskap om olika problem som kan uppkomma hjälper användare att lättare accepterar olika säkerhetsåtgärder, exempelvis ett inloggningsförfarande, vilka måste finnas i systemen (Furnell m fl., 2001).

Resultaten tyder på att användarna fortfarande är en stor riskfaktor vad gäller informationssäkerhet eftersom de krav som finns hur informationssäkerhet uppnås inte alltid efterföljs av användaren.

Användarna är i behov av kontinuerlig information och utbildning om informationssäkerhet för att de ska bli medvetna om de risker och hotbilder som finns vid hantering av känslig information. Funktionen för in- och utloggning bör i största möjliga mån stödja det arbetssätt som användarna har istället för att utgöra ett hinder. Vidare bör användarna bli medvetna om det ansvar som läggs på dem när de får behörighet till mer information än de behöver för att vårda de patienter de ansvarar för. För att bevara och förstärka patienternas förtroende bör hälso- och sjukvården sträva efter att erhålla informationssäkerhetsmedvetna användare.

7 Diskussion

I kapitlet förs en diskussion kring de resultat som framkommit under arbetet. Vidare kommer erfarenheter av arbetet och en kritisk granskning av det egna arbetet att diskuteras. Slutligen ges förslag på fortsatt arbete eller undersökning inom området.

7.1 Diskussion runt resultatet

Syftet med arbetet var bland annat att se om det skett någon förbättring vad gäller användarnas påverkan på informationssäkerheten utifrån vad Gratte (1996) skriver i sin rapport, där författaren anser att största delen av säkerhetsbristerna kan hänvisas till personalen. Den studie som gjorts i detta arbete bör kompletteras med ytterligare observationer och intervjuer med olika yrkesgrupper inom hälso- och sjukvården. Eftersom studien enbart berört en division och endast fem intervjuer har genomförts kan studien inte påvisa generella resultat som gäller för all personal inom hälso- och sjukvården.

Det förväntade resultat som arbetet förmodades få har visat sig vara förenligt med den verksamhet som studerades. Den litteratur som ligger till grund för problemområdet har visat sig relevant och utifrån dem har aktuella tankegångar tagits fram för att kunna förutsäga det resultat som studien sedan kom fram till.

7.2 Erfarenheter och kritisk granskning

Den tidsplan som utfärdades i ett tidigt skede av arbetet har följts i det närmaste, enbart mindre korrigeringar har gjorts. Att göra en tidsplan över arbetet har varit till stor hjälp vid genomförandet av studien och rapportskrivningen. Med hjälp av planen har kontroller gjorts, vad och när vissa arbetsuppgifter måste vara slutförda för att inte tidsbrist ska uppstå i slutet av arbetet.

Att genomföra en studie inom ett område som undertecknad inte har någon erfarenhet av kan vara både en fördel och nackdel. Nackdelen är att missuppfattningar kan uppstå när personalen och den person som utför studien inte har samma grundsyn om olika begrepp när de samtalar. Det har trots allt varit en fördel i detta arbete eftersom undertecknad har fått möjlighet att ställa många frågor till personalen och de har visat intresse för detta arbete. Personalen upplevdes uppskatta att någon person, som inte är insatt i deras arbete, är intresserad av deras verksamhet och vad de gör.

Att planera och bearbeta underlaget till observationerna och intervjuerna har visat sig vara en viktig del i studien för att erhålla det material som ska ligga till grund för resultatet. Tiden som togs i anspråk för att utföra underlagen har varit försvarlig vilket är en orsak till att observationerna och intervjuerna gav de resultat som framkommit.

Att respondenterna fick möjlighet att läsa igenom materialet gjorde att respondenterna kände förtroende dels för intervjuaren och dels för arbetet vilket gjorde att de utfrågade svarade ärligt på de känsliga frågor som fanns i intervjuunderlaget.

Att placera olika händelser och svar, som uppkommer vid observationer och intervjuer, i direkta fack vilket gjordes för bearbetning av materialet, skedde inte utan svårighet eftersom en händelse eller ett svar kan beröra fler av de funktioner som finns för att säkerställa informationssäkerhet. Om studien ska göras i ett annat

sammanhang kunde detta förfarande ses över och förändras för att inte dessa hinder ska uppstå. Att dela in materialet i olika kategorier har trots allt varit bra för att få överskådlighet över materialet.

7.3 Förslag på fortsatt arbete

För att få fram ytterligare fakta om hur användare av datorjournal i sjukhusmiljö hanterar informationssäkerhet bör en studie utföras vid datorer som används av enbart en användare. Detta för att se om deras förhållningssätt vid in- och utloggning och medvetenhet till informationssäkerhet och så vidare påminner om det resultat som framkommit under detta arbete.

En undersökning bör omgående göras för att studera om organisationen kan använda sig av smarta kort vid in- och utloggning för att underlätta för personalen i deras dagliga arbete och på så sätt skydda patientinformationen mot obehörig åtkomst.

Vidare är det intressant att undersöka varför organisationen skriver ut alla datorjournalanteckningar i en kopia, vilka sparas i arkiv, istället för att göra datakopior av journalen. Om det är av brist på kunskap, osäkerhet inför den nya tekniken eller om det är av ekonomiska orsaker att de gör på detta sätt.

Att studera informationssäkerhet mellan olika sekretessområden skulle vara av intresse för att granska om det finns brister i informationssäkerheten vid överföring av känslig information och kunna peka på förbättringar som behöver göras inom detta område.

Referenser

Alter, S. (1999) *Information systems a management perspective* (3:e upplagan). New York: Addison-Wesley Educational Publishers Inc.

Ask, L. (2002) Redovisning av material från observationer och intervjuer. Opublicerat material i Informationssäkerhet i datorjournal –en studie med användaren i fokus , Norra Kungsvägen 66a 522 31 Tidaholm, telnr: 0502-144 14.

Avison, D. E. & Fitzgerald, G. (1997) *Information Systems Development: Methodologies, Techniques and Tools* (2:a upplagan). Cambridge: McGraw-Hill International.

Barber, B. & Davey, J. (1996) Risk Analysis in Health Care Establishments. I: Barber, B., Treacher, A. & Louwerse, K. (Red:er.), *Towards Security in Medical Telematics Legal and Technical Aspects,* (s.120-124). Nederländerna: IOS Press.

Björner, O. (1999) *Begrepp för IT-säkerhet*, Rapport nr 2 från SITHS-projektet, 1999.

Björner, O. (2000) *Tjänster för att uppnå informationssäkerhet i hälso- och sjukvården*, Rapport nr 3 från SITHS-projektet, 2000.

Bourka, A., Polemi, N. & Koutsouris, D. (2001) An Overview in Healthcare Information systems Security. I: Patel, V. m fl. (Red:er.), *MEDINFO 2001*, (s.1242-1246). Amsterdam. IOS Press.

Collste, G. (1997) Vårdens datorisering ur etiskt perspektiv. I: Arensjö, B., Lagerstedt, M. & Nilsson, G. *IT i vården*, Sveriges Utbildningsradio AB, kapitel 4.

Dahlin, B. & Arnesjö, B. (1996) Datorjournalen. I: Petersson, G. & Rydmark, M. (Red:er) *Medicinsk Informatik*, Liber utbildning AB, kapitel 6.

Dahlin, B. & Ljungqvist, G. (1996) Från sökord till journalobjekt, Spri Statusrapport, 1996.

Datainspektionen, (1998) *Personregistrering vid sjukhus,* Datainpektionensrapport December 1998.

Datainspektionen, (2000) *Behandling av personuppgifter,* Datainpektionens småskrifter om PUL, 2000.

Davey, J. (2001) IT Security Training I: The ISHTAR Consortium. *Implementing Secure Healthcare Telematics Applikations in Europe* (s.149-166). Amsterdam, IOS Press, volym 66, kapitel 6.

Dowland, P.S., Furnell, S.M., Illingworth, H.M. & Reynolds, P.L. (1999) Computer crime and Abuse: A Survey of Public Attitudes and Awareness. *Computers and Security, 18,* 715-726.

Drazen, E. (1996) Inledning I: Drazen, E., Metzger, J., Ritter, J. & Schneider, M. (red:er) *Patient Care Information Systems -Successful Design and Implementation.* New York, Springer- Verlag.

Ejlertsson, G. (1996) *Enkäten i praktiken, En handbok i enkätmetodik.* Lund, Studentlitteratur.

Engström, S. (2002) Arbetsmiljö. Föreläsningsanteckningar i kursen Informationssystem inom vården, Högskolan Skövde 2002.05.02.

Faulkner, X. (2000) *Usability Engineering,* London: Macmillian Press Ltd.

Fisher, C. & Kingma, B. (2001) Criticality of data quality as exemplified in two disasters. *Information & Managment, 39* (2001), 109-116.

France, R. (2001) Security Of Electronic Health Care Records: A Clinical Perspektive I: The ISHTAR Consortium. *Implementing Secure Healthcare Telematics Applikations in Europe* (s.23-31). Amsterdam, IOS Press, volym 66, kapitel 2.

Furnell, S.M., Gaunt, P.N., Holben, R.F., Snaders, P.W., Stockel, C.T. & Warren, M.J. (1996) Assessing staff attitudes tiowards information security in a European healthcare establishment. *Medical informatics, 21,* 105-112.

Furnell, S.M., Dowland, P.S., Illingworth, H.M. & Reynolds, P.L. (2000) Authentication and supervision: A survey of User Attitudes. *Computers and Security, 19,* 529-539.

Furnell, S. M., Warren, M. J. & Evans, M. P. (2001) The ISHTAR World Wide Web Dissemination and Advisory Service for Healthcare Information Security I: The ISHTAR Consortium. *Implementing Secure Healthcare Telematics Applikations in Europe* (s.249-281). Amsterdam, IOS Press, volym 66, kapitel 9.

Gaunt, N. & Roger-France, F. (1996) Security Of The Electronic Helth Care Record – Professional Ad Ethical Implications. I: Barber, B., Treacher, A. & Louwerse, K. (Red:er.), *Towards Security in Medical Telematics Legal and Technical Aspects*, (s.10-22). Amsterdam: IOS Press.

Gratte, I. (1996) *Datorn i vården.* Falköping, Liber Utbildning AB.

Hälso- och sjukvårdsinstitutet. (1996) *Behörighet, säkerhet och sekretess – krav på system med patientinformation*, Spri Rapport 419, 1996.

Hälso- och sjukvårdsinstitutet. (1998) *Införandet av elektroniska patientjournaler – Förutsättningar och krav*, Spri Rapport 473, 1998.

Högskolan Skövde, (2002) *Föreläsningsinnehåll till kursen Informationssystem - Introduktion*, Box 408, 541 28 Skövde.

Kajbjer, K. & Lundmark, T. (1997) Kan vi standardisera informationshanteringen inom hälso- och sjukvården? I: Arnesjö, B., Lagerstedt, M. & Nilsson, G. *IT i vården*, Sveriges Utbildningsradio AB, kapitel 22.

Karlberg, A. & Arnesjö, B. (1997) Vårdinformationssystem. I: Arnesjö, B., Lagerstedt, M. & Nilsson, G. *IT i vården*, Sveriges Utbildningsradio AB, kapitel 8.

Lagerlund, B. (1997) Informationssäkerhet. I: Arnesjö, B., Lagerstedt, M. & Nilsson, G. *IT i vården*, Sveriges Utbildningsradio AB, kapitel 6.

Lagerlund, B. (1999) *Informationssäkerhet i vårdprocessen: Krav beskrivna i generella användningsfall utifrån vårdscenarion*, Rapport1 från SITHS-projektet, 1999.

Leffler, J & Odelhög, Ö. (2001) *Stategier för effektiva och samverkande IT-stöd i sjukvården.* Carelink rapport 1/2001.

Lyckéus, L., Wahlgren, L. & Lindqvist, R. (1998) *HSA-pilotprojektet säkerhet och sekretess*, Delprojekt från Spri I, 58015, 1998.

Metzer, J. & Teich, J. (1995) Designing Acceptable Patient Care Information Systems. I: Drazen, E., Metzger, J., Ritter, J. & Schneider, M. (red:er) *Patient Care Information Systems -Successful Design and Implementation* (s.83-132). New York, Springer- Verlag, kapitel 4.

Meyer, F., Lundgren, P-A., Moor, G. & Fiers, T. (1998) Determination of user requirements for the secure communication of medical record information. *International Journal of Medical Informatics, 49,* 125-130.

Nationalencyklopedin. (2002) Tillgänglig på Internet: http://www.ne.se/jsp/search/article.jsp?i_art_id=150881 [Hämtad den 02.05.07].

Nilsson, G. (1997) Kan omvårdnad datoriseras och varför? I: Arnesjö, B., Lagerstedt, M. & Nilsson, G. *IT i vården*, Sveriges Utbildningsradio AB, kapitel 20.

Patel, R. & Davidson, B. (1994) *Forskningsmetodikens grunder, Att planera, genomföra och rapportera en undersökning.* Lund, Studentlitteratur.

Petersson, G. & Rydmark, M. (1996) Medicinsk Informatik inom vård och utbildning. I: Petersson, G. & Rydmark, M. (Red:er) *Medicinsk Informatik,* Liber utbildning AB, kapitel 1.

Schneider, M. & Reed, W. (1996) Developing a Patient Care Information System Strategy I: Drazen, E., Metzger, J., Ritter, J. & Schneider, M. (red:er) *Patient Care Information Systems -Successful Design and Implementation* (s.133-162). New York, Springer- Verlag, kapitel 5

SFS 1980:100. *Sekretesslagen,* Justitiedepartementet L6 1980, Omtryckt SFS 1992:1474.

SFS 1985:562. *Patientjournallagen,* Socialdepartementet 1985, Sveriges Riksdag.

SFS 1998:204. *Personuppgiftslagen,* Justitiedepartementet L6 1998, Sveriges Riksdag.

SFS 1998:544. *Vårdregisterlagen,* Socialdepartementet 1998, Sveriges Riksdag.

SFS 1982:763 *Hälso- och sjukvårdslagen,* Socialdepartementet 1982, Sveriges Riksdag.

Sjölenius, B. (1996) Lagar, regler och etik. I: Petersson, G. & Rydmark, M. (Red:er) *Medicinsk Informatik,* Liber Utbildning AB, kapitel 4.

Smith, E. & Eloff, J. H. P. (1999) Security in health-care information systems-current trends. *International Journal of Medical Informatics, 54,* 39-54.

Sågänger, J. & Utbult, M. (1998) *Vårdkedjan och informationstekniken*, Teldok rapport 119.

Västra Götalandsregionen, (2000) *Informationssäkerhetspolicy: Vad är informations-säkerhet för Västra Götalandsregionen?*, diarienr. 541-2001(7), 2000.

Åhlfeldt, R-M. (2002) Säkerhet och sårbarhet. Föreläsningsanteckningar i kursen Informationssystem inom vården, Högskolan Skövde 2002.05.23.

Överstyrelsen för civilberedskap (ÖCB), (1993.242), FA 22, *Grundsäkerhet för samhällsviktiga datasystem hos beredskapsmyndigheter.*

Observation av informationssäkerhet på _____ Bilaga 1

Dag:_____ Klockan:_____

Kategorier	Uppkomna situationer															
Autentisering																
Inloggning: Använder eget ”loggin” till nätverket																
Använder annans identitet																
Använder grupp-identitet																
Loggar in i datajournal																
Loggar in i annat program																
Lösenord sparad: i minnet																
Lösenord sparad: på lapp																
Utloggning: Loggar ut																
Loggar inte ut																
Kontroll av identitet på patient																
Kontroll av identitet av mottagare: Vid e-post																
Vid telefonkontakt																
Behörighetstilldelning Har tillgång till information																
Har inte tillgång till information																
Sekretess Lämnar ”påloggad” arbetsstation för kortare stund																
Integritet **Data Inskrivning** från: Lapp																
Ur minnet																
Utskrift: Gå och hämta																
Inom räckhåll																
Ändring: Signera																
Enbart ta bort																
Oavislighet																

Observation av informationssäkerhet på _____ Bilaga 1

Dag:_____ Klockan:_____

Kategorier	Uppkomna situationer															
Använder e-post:																
Skicka e-post: utan patientinfo																
Skicka e-post: Med patientinfo																
Ta emot e-post: utan patientinfo																
Ta emot e-post: Med patient info																
Spårbarhet																
Känslig information som loggas:																
Ruta som kommer upp?																
Använder Internet																
Arbetsbelastning																
Stressad																

Anteckningar:_____

Bilaga 2 Information inför observation/intervju

Jag heter Lena Ask och är student på Högskolan i Skövde. Jag går systemvetenskapligt program och under våren gör jag mitt examensarbete som berör datoranvändning inom vården. Jag kommer att studera informationssäkerhet i datajournaler och har fått möjlighet att vara med på er avdelning.

I mitt arbete kommer observationer och efterföljande intervjuer att ligga till grund för det slutliga resultatet. Jag är därför tacksam att få studera er avdelning och de personer som kommer att medverka i min studie. Er medverkan är viktigt för att jag skall kunna få en inblick i hur det är att arbeta med datajournaler och kunna studera informationssäkerhet vid användning av datajournalsystem.

Materialet kommer att behandlas helt konfidentiellt och det är därför endast jag som vet vilka som medverkat i undersökningen. De band som kommer att användas under intervjuerna kommer efter avslutad bearbetning att förstöras. I min slutrapport kommer jag inte heller att ange någon vid namn och materialet kommer därför inte kunna spåras till er, avdelningen eller till sjukhuset.

Om ni undrar över något hör gärna av er till mig.

Ser fram emot att få arbeta med er.

Vänliga hälsningar

Lena Ask

SVP 3, Högskolan i Skövde

Telnr: 0502-14414

E-mail: a99lenas@student.his.se

Bilaga 3 Intervjufrågor

Intervjufrågor	System-administratör	Sjuk-sköterskor
Inledande frågor:		
Hur lång tid har du arbetat inom avdelningen och vad består dina arbetsuppgifter av?	X	X
Vad är din erfarenhet, även privat, av att använda datorer?		X
Vilka strategier finns för att försäkra att de stränga informationskraven som lagen ställer efterföljs?	X	
Utbildning och information:		
Har du fått någon utbildning i informationssäkerhet från landstinget?		X
Har användaren fått någon utbildning i informationssäkerhet från landstinget?	X	
Finns det någon rutin för att utveckla eller följa upp informationssäkerheten i landstinget?	X	
Finns det något existerande utbildningsprogram i organisationen för att utbilda vårdpersonal i informationssäkerhet?	X	
Vilka kunskaper har du fått angående säkerhetspolicy i landstinget?		X
Vilka kunskaper har användaren fått angående säkerhetspolicy i landstinget?	X	
Följer organisationen upp och utvecklar policyn? Om ja hur ofta?	X	
Fanns det någon specifik strategi för utbildning i säkerhetsfrågor när datorisering av systemen introducerades?	X	
Hur får du reda på författningar eller andra regler i organisationen så att du kan använda dig av dem i ditt arbete? Är de nödvändiga/tillräckliga i ditt tycke?		X
Hur sprids författningar eller andra regler i organisationen så att de anställda kan använda sig av dem i sitt arbete? Är de nödvändiga/tillräckliga i ditt tycke?	X	
På vilka sätt anser du att du påverkas av kraven på informationssäkerhet?		X
På vilka sätt anser du att användarna påverkas av kraven på informationssäkerhet?	X	
Autentisering:		
Hur kontrolleras en ny patients identitet?	X	X
Vilka grundregler för identifiering av vårdtagare finns i organisationen?	X	X
Hur kontrollerades er identitet, vid anställning?		X
Hur kontrolleras er identitet, vid inloggning?	X	X
Autentisering och behörighet:		
Har du någon gång använt någon annans användarnamn/inloggning?		X
Har du tillåtit någon använda ditt användarnamn/inloggning?		X
Finns det några rutiner för att kontrollera att användarna använder sin egen användaridentitet och inte lånar ut den?	X	
Vad är din åsikt om ut- och inloggning?		X
Hindrar det dig i ditt arbete?		

Vad är din åsikt om access och kontroll av behörighet i existerande system?		X
Dokumenteras beslut av tilldelad behörighet?	X	
	X	
Behörighet, Lösenord:		
Ger systemet bekräftelse när byte av lösenord bör ske eller får ni användare göra detta när ni anser det befogat?	X	X
Hur upplever du som användare att byta lösenord? Hur ofta?		X
Hur många lösenord måste du komma ihåg för ditt arbete?		X
Hur upplever du att det är att komma ihåg ditt/dina lösenord?		X
Har du någon gång diskuterat med kollega och/eller skrivit ned ditt lösenord?		X
Tror du ditt lösenord är tillräckligt säkert eller är det enkelt och skulle gå att lista ut?		X
Har du någon gång använt ett lösenord bestående av anhörigs namn eller liknande?		X
Sekretess:		
Finns det några rutiner i organisationen som påverkar vilka personer som ska ha access till information i datorjournalen?	X	X
Är dessa rutiner eller regler tydliga?	X	X
Hur kontrollerar organisationen att de upprätthålls?	X	
Hur förhindras obehöriga accessen i datorjournalen?	X	X
Kan skyddet förbättras? Ska skyddet förbättras?	X	X
Används e-mail eller fax till att föra information till andra vårdinrättningar? Är informationen krypterad?	X	X
Oavvislighet:		
Kontrolleras mottagaren att den är behörig att få tillgång till informationen?	X	X
Hur länge kan aktiviteter vara osignerade i datorjournalen?	X	X
Spårbarhet:		
Loggas känslig information i systemet?	X	X
Hur kontrolleras och hanteras loggen?	X	X
Har du fått någon information om vilken data som sparas i loggfilen?		X
Hur uppfattar du att systemen loggas?		X
Anser det befogat att logga systemen, varför?		X
Integritet:		
Är det svårt att komma ihåg information om en patient när du arbetar med många olika patienter när du sedan skall föra in detta i datorjournalen?		X
Finns det olika rättigheter för att läsa, skriva och ta bort och vet du som användare på vilket sätt du får ändra på inskriven data?		X
Finns det olika rättigheter för att läsa, skriva och ta bort och vet användaren på vilket sätt han/hon får ändra på inskriven data?	X	
Hur sparas data?	X	
Är den tillgänglig eller sparas den i en separat lagringsenhet?	X	
Kan obehöriga få tillgång till information som skrivs ut på skrivare?	X	
Hur ofta skrivs kopior ut från datorjournal som sparas i arkiv?	X	

Hur ofta görs back up på datorjournalen?	X	
Blandade frågor:		
Hur upplever du det är att hantera känsliga uppgifter?		X
På vilket sätt påverkas du när det blir avbrott i datorjournalen?		X
På vilket sätt påverkas informationssäkerheten när det blir avbrott i datorjournalen?		X
Tillgängligheten av systemet: kan du genomföra dina arbetsuppgifter på ett tillfredställande sätt?		X
Anser du att kraven i ditt arbete är rimliga? Varför?		X
Hur är arbetsförhållandet på avdelningen, vad gäller stress, för höga och för låga krav?		