Åtkomstkontroll inom hälso- och sjukvården

- en kartläggning av nuvarande system

(HS-IKI-MD-04-103)

Dariusz Piotr Miettinen (a00darbu@student.his.se)

Institutionen för Kommunikation och Information
Högskolan i Skövde, Box 408
S-54128 Skövde, SWEDEN

Handledare: Rose-Mharie Åhlfeldt

Åtkomstkontroll inom hälso- och sjukvården - en kartläggning av nuvarande system

Examensrapport inlämnad av Dariusz Piotr Miettinen till Högskolan i Skövde, för Magisterexamen (M.Sc.) vid Institutionen för Kommunikation och Information.

2004-10-06

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: _____

Åtkomstkontroll inom hälso- och sjukvården - en kartläggning av nuvarande system

Dariusz Piotr Miettinen (a00darbu@student.his.se)

Sammanfattning

Detta arbete handlar om att kartlägga åtkomstkontrollen inom olika delar av dagens hälso- och sjukvård, nämligen primär-, sluten- samt hemvården. Arbetet handlar även om att undersöka om det finns alternativa lösningar på nuvarande problem när det gäller åtkomstkontroll inom hälso- och sjukvården.

Hälso- och sjukvården drivs av olika huvudmän och det kan finnas skillnader när det gäller hantering av åtkomsten till informationen mellan dessa delar.

Det är viktigt att ha hög datasäkerhet inom hälso- och sjukvården. En del av datasäkerheten är åtkomstkontroll. Resultatet av undersökningen som har gjorts inom olika delar av hälso- och sjukvården visar att, generellt sätt, både systemansvariga och användare är nöjda med hur dagens åtkomstkontroll ser ut. Ett problem som har framkommit i intervjuer är hantering av loggar. Loggarna kontrolleras manuellt. Utifrån litteraturstudie konstaterades att det finns olika verktyg som kan kontrollera loggar automatiskt. Litteraturstudien visar att även andra organisationer, både inom hälso- och sjukvården, men även utanför, hanterar loggar på ett manuellt sätt. Det finns dock organisationer som har effektiviserat kontrollen av loggar och hanterar denna automatiskt.

Nyckelord: Hälso- och sjukvård, datasäkerhet, åtkomstkontroll, behörighetskontroll.

Innehållsförteckning

1 Introduktion

En hög nivå av datasäkerhet inom informationssystem är viktig inom flera områden. Ett av dessa områden är hälso- och sjukvård. Där finns det stora mängder av känslig information (Poole et al., 1996).

Människor har ett behov av att hålla informationen om dem själva på ett sådant sätt att denna information inte blir åtkomlig för andra. Inom hälso- och sjukvården finns bl.a. samlad personlig information om alla de som någon gång besökt denna organisation för att få vård. Denna information kan användas på flera olika sätt och därför krävs det att organisationerna har starka kontrollmekanismer som skyddar denna information från att den används på ett felaktigt sätt (Sadan, 2001; Poole et al., 1996). Det finns olika hot som kan förekomma när det gäller datasäkerhet inom informationssystem och det finns olika sätt att skydda informationen mot dessa hot. Ett sätt är att ha en stark åtkomstkontroll inom organisationen (Connolly och Begg, 2002).

Det finns olika typer av åtkomstkontroll, t.ex. oberoende, obligatorisk och rollbaserad (Sandhu och Bhamidipati, 1999). Hälso- och sjukvården är en komplex organisation med många användare och stora mängder av information. För att kunna lösa vissa problem med åtkomstkontrollen kan rollbaserad åtkomstkontroll användas.

Första delen i detta arbete handlar om att kartlägga åtkomstkontrollen inom olika områden inom hälso- och sjukvården. De områden som valdes ut är primär-, sluten- och hemvården. Denna kartläggning begränsades till Skövdeområdet i västsverige. Kartläggningen ger en bild av hur åtkomst till information inom hälso- och sjukvården hanteras och kontrolleras i de olika delarna.

Andra delen handlar om att undersöka metoder och mekanismer som kan appliceras inom hälso- och sjukvården. Dessa synsätt och mekanismer undersöktes med hjälp av litteraturen, medan den första delen genomfördes genom ett antal intervjuer.

Arbetet börjar med att, i kapitel 2, ge olika definitioner på de begrepp som skall användas i de senare delarna av arbetet. Dessa begrepp innefattar bl.a. säkerhet inom informationssystem och inom hälso- och sjukvården. Andra begrepp som förklaras är olika typer åtkomstkontroll samt andra viktiga begrepp som behövs för att kunna förstå arbetets problemlösning.

I kapitel 3 ges en introduktion till arbetets problemområde. Beskrivning av problemområdet baseras på undersökningen av litteraturen. Ur detta problemområde definieras arbetets problemprecisering, med begränsningar och förväntade resultat.

I nästa del, nämligen kapitel 4, diskuteras de forskningsmetoder som kommer att användas för att lösa tidigare definierade problem. I detta arbete valdes intervjuer samt litteraturstudier som forskningsmetoder. Det diskuteras även varför dessa metoder lämpar sig bättre för att lösa arbetets problem. I denna del presenteras även arbetets genomförande, alltså hur hela arbetet har genomförts och varför.

I kapitel 6 presenteras all insamlat material. Först presenteras en sammanställning av alla intervjuer och i kapitel 7 finns efterföljande analyser av dessa intervjuer. Kapitel 8 handlar om resultatet av litteraturstudier. Arbetet avslutas med en

diskussion om resultatet, arbetets bidrag, funderingar kring utförandet samt förslag till framtida arbeten inom detta område.

Resultatet av detta arbete är att generellt är de intervjuade personerna nöjda med hur åtkomstkontrollen i deras organisationer ser ut i dagens läge. Arbetet påpekar vissa brister när det gäller hantering och kontroll av loggar. Dessa loggar hanteras manuellt och utan klara rutiner. Genom litteraturstudie framgick det att det finns mekanismer som kan kontrollera loggarna automatiskt, förutsatt att det finns vissa policies och riktlinjer för detta. Studier av flera andra organisationer, både inom och utanför hälso- och sjukvården, påvisade att kontroll av loggar sker mestadels manuellt. Det finns vissa som använder sig av automatiskt loggkontroll. Det finns även system som finns under utveckling där en sådan kontroll kan bli aktuell.

2 Bakgrund

I det här kapitlet definieras viktiga termer som förekommer senare i arbetet. Dessa termer är grundläggande för att kunna förstå arbetets innehåll.

2.1 Säkerhet inom informationssystem

Yialelis et al. (1996) anser att olika organisationer har ett starkt behov av att förvara ”känslig” information på ett säkert sätt. Vissa branscher är mer känsliga än andra, Hälso- och sjukvårdsmiljön är ett sådant område där behovet av stark kontroll över data är påtaglig. Därför krävs det att data förvaras på ett säkert sätt.

Enligt Pfleeger (1997) och Devargas (1995), är informationssystemsäkerhet ett område som kräver ständig utveckling. Andra områden och tekniska artefakter, såsom t.ex. bilar eller hus, har relativt god säkerhet, men informationssystem behöver bättre och starkare säkerhetsmekanismer. Det finns flera olika typer av mål när det gäller utveckling av säkerhet inom informationssystem:

- *Sekretess* (Confidentiality)- endast auktoriserade användare har tillgång till data och denna tillgång kontrolleras av olika typer av mekanismer. Med andra ord reglerar sekretessen tillgång till information utifrån förutbestämda regler och policies.
- *Integritet* (Integrity)- reglerar hur informationssystem skall bete sig så att data inte kan ändras, läggas till eller raderas av icke auktoriserade användare. Data som har förändrats av obehöriga användare kan orsaka stora problem för organisationen, i bästa fall kan den fortfarande användas, i värsta fall leder det till organisationens fall.
- *Tillgänglighet* (Availability)- En auktoriserad användare skall inte nekas tillgång till data. Data skall alltid vara tillgänglig för dessa användare.

Enligt SIS Handbok (2003) är även *spårbarhet* (accountability) ett viktigt mål när det gäller utveckling av säkerhet inom informationssystem. Med spårbarheten skall det vara möjligt att spåra olika aktiviteter som varje användare har utfört på systemet. För att kunna göra detta krävs det identifiering av användare samt loggning av alla händelser som sker inom systemet.

Det finns flera hot som kan uppkomma när det gäller säkerhet inom informationssystem. Connolly och Begg (2002) definierar fem olika typer av hot:

- *Förlust av personlig säkerhet* (Loss of privacy)- detta handlar om att förvara data om olika personer på ett säkert sätt, utan möjlighet för icke-auktoriserad användare att få tillgång till denna.
- *Förlust av integritet* (Loss of integrity)- om data är felaktig eller inte aktuell kan den orsaka störningar i det dagliga arbetet inom en organisation.
- *Förlust av tillgänglighet* (Loss of availability)- data skall vara tillgänglig för användare när de behöver den. Detta är relaterat till tekniska frågor samt frågor angående hur ett system är uppbyggt.
- *Förlust av sekretess* (Loss of confidentiality)- förlust av viktig, strategisk information kan få katastrofala följder för en organisation.

- *Stöld och bedrägeri* (Theft and fraud)- påverkar hela organisationen och resulterar ofta i att hemlig information blir tillgänglig för obehöriga personer.

Neumann (1995) påpekar att det finns tre grundläggande gap mellan vad som förväntas av informationssäkerheten och vad som erhålls i praktiken. Det första gapet är på teknologisk nivån och gäller skillnaden mellan vad ett system är kapabelt till med avseende på t.ex. åtkomstkontroll eller autenticitet och vad som förväntas av dessa system. Andra gapet gäller socialtekniska frågor, alltså skillnaden mellan policies inom ett informationssystem och regler som finns ute i samhället, t.ex. lagar angående databrott. Tredje och sista gapet gäller den sociala planen. Det innebär skillnaden mellan aktuella lagar och regler och hur människor beter sig i verkligheten.

Enligt Pfleeger (1997) kan informationssystem utsättas för tre olika typer av hot, nämligen hot mot hårdvara, mjukvara och data. Varje informationssystem innehåller hårdvaruenheter som kan bli förstörda på olika sätt, t.ex. kan de bli stulna eller brinna upp. Även mjukvaran i ett informationssystem kan bli förstörd, antigen avsiktligt eller oavsiktligt. Det tredje hotet, nämligen hot mot data, är en mer komplicerad fråga. Data kan bli ett begärligt föremål och kan användas på olika sätt av många människor, data har ett stort värde. Hemlig data kan läcka till konkurrenter och det kan orsaka enorma skador antigen för en enskild person eller för hela organisationen.

Yialelis et al. (1996) anser att distribuerade informationssystem är mer komplexa än centraliserade. Ofta finns det stora mängder av data och många användare utplacerade på olika ställen i ett distribuerat informationssystem. Med avseende på detta krävs det pålitliga säkerhetsmekanismer.

Enligt Berson (1996) är distribuerade system i stort behov av att ha bra säkerhetsmekanismer. En av dessa skall vara fungerande åtkomstkontroll, som hindrar ickeauktoriserad åtkomst till data. Denna teknik måste införas på operativ nivå inom organisationer som använder distribuerade informationssystem. Säkerhetsfrågor inom informationssystem är ofta sammankopplade med administration inom en organisation och kräver koordination mellan olika delar av systemadministrationen såsom system-, nätverks- och säkerhetsadministratörer.

Dawson et al. (2000) påstår att tillhandahållande av goda säkerhetslösningar är ett grundläggande krav för distribuerade system. Ingen organisation vill förlora kontrollen över data och exponera data för icke-behöriga användare. För att förbättra säkerheten inom distribuerade system krävs det policies och regler för hur data skall vara tillgänglig för användare och vilka användare som skall ha åtkomst till data. Regler och policies är viktiga frågor som organisationer måste försöka lösa innan ett system tas i bruk. Stegmann (1997) påpekar att det måste finnas en väldefinierad säkerhetspolicy inom varje större organisation. Dessa policies skall innehålla regler och tillvägagångssätt för hur känslig data skall skyddas samt hur den skall distribueras. Devargas (1995) påstår att säkerhetspolicy är grundläggande för varje informationssystem. Utan den är det omöjligt att ta ställning till vad som skall skyddas och hur.

2.2 Hälso- och sjukvården

Hälso- och sjukvårdslagen (HSL) är en ramlag som ger kommuner och landsting utrymme att utforma vården efter lokala behov. Den tillkom bl.a. för att göra patienternas ställning starkare. Hälso- och sjukvårdslagen säger:

”*Med hälso- och sjukvård avses i denna lag åtgärder för att medicinskt förebygga, utreda och behandla sjukdomar och skador. Till hälso- och sjukvården hör även sjuktransporter samt att ta hand om avlidna*” (Sjölenius, 1997).

Sjölenius (1997) påpekar att hälso- och sjukvården är uppdelad på tre olika områden, slutenvård, primärvård och hemvård. Dessa tre områden styrs av olika organ och kontrolleras av Socialstyrelsen. Enligt HSL är varje landsting ansvarigt för att tillgodose vårdbehov för sina invånare när det gäller sluten- och primärvård. Kommunernas ansvarsområde ligger i att förse sina invånare med särskilt stöd, bl.a. ålderdomshem, servicehus och hemvård. HSL säger att både lansting och kommuner bör samarbeta för att eliminera dubbelarbete och för att förse patienter med en bra vård.

2.2.1 Informationssäkerhet inom hälso- och sjukvården

Säkerhet bland informationssystem inom hälso- och sjukvården regleras med hjälp av etik, lagar och erfarenheter. Enligt SITHS- projektet, som är ett projekt om säker IT inom hälso- och sjukvården, finns det två huvudmodeller som reglerar åtkomst till data inom hälso- och sjukvården. Den ena är behörighetsmodellen, som kontrollerar användarnas åtkomst till data genom att använda policies och regler. Denna modell tillåter användare att få tillgång endast till data som specificeras av säkerhetsinstanser. Sådana instanser kan vara t.ex. systemadministratörer eller organisationens regelverk. En av fördelarna med att använda denna modell är att användarna inte får tillgång till någon annan data än den de behöver för att utföra sina arbetsuppgifter. En nackdel är att det ibland kan vara svårt att definiera vilka data användarna behöver. Den andra modellen, loggningsmodellen, tillåter användare att ha åtkomst till all data. Det finns inga begränsningar när det gäller åtkomst, men det finns mekanismer som kontrollerar användarnas aktiviteter i efterhand. Med hjälp av loggar kan varje enskild användare spåras tillbaka till alla genomförda aktiviteter. Denna modell kräver inte utveckling av behörighetsregler för användarna, alla har åtkomst till all data. En nackdel är att, p.g.a. att användarnas aktiviteter kontrolleras först efteråt kan skadan redan ha skett (Åhlfeldt, 2001).

Billum (1997) påpekar att anställda inom hälso- och sjukvården har ett ansvar när det gäller hanteringen av information om patienter. Sekretesslagen är ett viktigt instrument för att upprätthålla god säkerhet och för att skydda att patientuppgifter inte hamnar hos obehöriga. Andra lagar som skyddar mot utlämnandet av information om patienter är tryckfrihetsförordningen och patientjournallagen. I dessa står bl.a. vad som skall finnas i patientjournaler och hur sådan information skall hanteras.

Rindfleisch (1996) påpekar att känslig information om patienter levereras till andra intressenter såsom försäkringskassan eller diverse hjälpmedelstillverkare. Det finns sällan en uppföljning hur sådan information används av dessa intressenter. Det finns risker att sådan information kan användas till andra

ändamål än den var avsatt till från början, t.ex. affärsmässiga ändamål. Därför är det viktigt att dagens informationssystem inom hälso- och sjukvården uppfyller vissa krav, nämligen:

- Tillgänglighet- säkerhetsställer att uppdaterad information finns tillgänglig när den behövs och på den plats den behövs.
- Definition av parametrar- bestämmer och kontrollerar åtkomstgränser i ett informationssystem, både fysiskt och logiskt.
- Spårbarhet- säkerhetsställer att vårdgivarna är ansvariga för åtkomst till och användning av patientdata. Detta skall baseras på två principer, nämligen ”right to know” och ”need to know”.
- Rollbegränsad åtkomst- detta möjliggör att skapa åtkomst endast till den information som är grundläggande för att en anställd skall kunna utföra sitt arbete. Detta minskar även möjligheter till obehörig åtkomst till informationen.

Enligt Hutt et al. (1995) orsakar den mänskliga faktorn problem när det gäller informationssystemsäkerhet. Det finns två typer av problem, avsiktliga och omedvetna. Dessa handlingar kan medföra att data förstörs, ändras, stjäls eller läcker ut till obehöriga. För att minimera eller eliminera dessa problem krävs starka auktoriseringsmekanismer. Auktoriseringsmekanismer är mekanismer som fastställer åtkomsträttigheter för varje användare till de resurser som finns inom ett system.

Connolly och Begg (2002) påpekar att auktorisering, ibland även kallad åtkomstkontroll, är en viktig mekanism som inte bara specificerar användares åtkomst men också indikerar hur användare kan använda data.

2.3 Åtkomstkontroll

Enligt Burleson (1994) är åtkomstkontroll ett viktigt verktyg för att förbättra säkerheten inom informationssystem i distribuerade miljöer. Åtkomstkontroll hanterar användares rättigheter med hjälp av diverse policies och regler.

Europeisk säkerhetsstandard (ITSEC) framhäver när det gäller funktionaliteten hos ett informationssystem att det skall vara möjligt att reglera användarnas åtkomst till informationen samt deras rättigheter när det gäller att förändra data. Åtkomstkontroll skall även innefatta möjligheter att installera och underhålla listor med regler och användare samt ha kontrollmekanismer för dessa (Devargas, 1995).

Elmasri och Navathe (2000) menar att auktoriseringssystem är ansvariga för att kontrollera att inga obehöriga kommer åt data. Det finns olika typer av åtkomstkontroll, t.ex. oberoende, obligatorisk och rollbaserad.

Smith och Eloff (1998) hävdar att åtkomstkontroll är ett av de viktigaste verktygen för att skydda känslig information. Åtkomstkontroll hanterar tilldelning och borttagning av användarens rättigheter till åtkomst av data och är nödvändigt, särskilt inom distribuerade system.

Ägarna till ett informationssystem kan använda åtkomstkontroll för att tillämpa de säkerhetspolicies och regler som finns inom en organisation. Dessa har som

uppgift att hålla icke auktoriserade användare borta från datan. Åtkomstkontroll kan användas i olika systemarkitekturer och på diverse abstraktionsnivåer, t.ex. databaser, nätverk, m. m. (Beznosov och Deng, 2000).

Barkley (1997) påpekar att åtkomstkontrollmekanismer kräver information om användare och objekt i ett informationssystem. Informationen om användarna skall innehålla bl.a. grupptillhörighet samt de roller som användaren är behörig att anta. Information om objekten skall innehålla rättigheter som dessa objekt kräver för att utföra olika operationer. Åtkomstkontrollmekanismer undersöker informationen om användare och objekt för att kontrollera om en viss användare är behörig att komma åt dessa objekt samt vilka operationer som denne användare kan utföra på objekten.

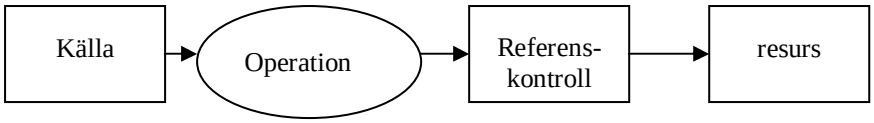

Fig.1. *Lampsons modell över åtkomstkontroll (1993).*

Lampson (1993) har skapat en modell över hur åtkomstkontroll fungerar, (Fig. 1). Denna modell innehåller fyra komponenter, nämligen källa, operation, referenshantering samt resurs. Med källa menas användare eller applikation. Denna kan utföra olika operationer, t.ex. skriva, läsa, exekvera, m.m., på olika resurser. Resurser eller objekt är olika delar av informationssystem eller databaser. Dessa delar kan innehålla data. Användaren eller applikationen måste ha rättigheter för att kunna utföra olika operationer. Referenskontrollen innehåller auktoriseringspolicies och regler som kontrollerar att källan har rättigheter för att utföra vissa operationer på resursen.

2.3.1 Oberoende åtkomstkontroll

Enligt Elmasri och Navathe (2000) handlar *oberoende åtkomstkontroll* (Discretionary Access Control, DAC) om tilldelning (grant) och borttagning (revoke) av användares rättigheter. Det finns två nivåer när det gäller tilldelning av rättigheter vid DAC:

1. Kontonivå- På denna nivå tas ingen hänsyn till relationer i ett informationssystem. Systemadministratören tilldelar rättigheter för varje konto beroende på användares arbetsuppgifter.
2. Relationsnivå- Här tas det hänsyn till de relationer som finns inom systemet. Rättigheter kontrolleras för varje relation eller fragment av systemet. Denna punkt är specifik för relationsdatabaser.

En grundläggande tanke bakom oberoende åtkomstkontroll är att det finns en ägare till varje objekt. Ägaren är vanligtvis den som har skapat objektet. Denne ägare bestämmer vilka subjekt som får ha tillgång till objektet. Policies för oberoende åtkomstkontroll är ägarbaserade och innehåller administration av åtkomsträttigheter för olika objekt. Det finns ett antal olika varianter av

oberoende åtkomstpolicies. Dessa skiljer sig från varandra genom tilldelning av olika grader av bestämmande för ägarna av olika objekt (Sandhu och Munawer, 1998).

Ett exempel på oberoende åtkomstkontroll är lösenord, men skapandet och användandet av lösenord räcker inte för att upprätthålla god säkerhet i alla organisationer. Därför krävs det ytterligare auktoriseringsmekanismer (Elmasri och Navathe, 2000).

2.3.2 Obligatorisk åtkomstkontroll

Obligatorisk åtkomstkontroll (Mandatory Access Control, MAC) är en annan typ av åtkomstkontroll, som kan användas ihop med DAC. MAC klassificerar både data och användare i säkerhetsklasser där det tillämpas olika rättigheter enligt policies och regler som finns för systemet (Elmasri och Navathe, 2000).

Enligt Dawson et al. (2000) baseras den obligatoriska åtkomstkontrollen på att skapa ett ramverk med åtkomstregler och klassificera både subjekt (dessa kan vara användare eller applikationer) och objekt (datakällor) i olika säkerhetsklasser eller säkerhetsnivåer. Dessa nivåer är uppbyggda på ett hierarkiskt sätt och nivån som finns över en annan dominerar denna, dvs. den övre nivån har åtkomst till den undre men inte tvärtom. Subjekten, i den obligatoriska åtkomstkontrollen, vet endast om vilken säkerhetsklass som dessa ingår i. Objektens säkerhetsramverk är inte känd för dessa subjekt.

Samarati och Jajodia (1999) påpekar att obligatorisk åtkomstkontroll innehåller åtkomstklasser. Varje sådan klass innehåller en säkerhetsnivå och ett antal kategorier. Varje säkerhetsnivå är ett element av en hierarkiskt uppbyggd arkitektur. Vanligtvis består obligatorisk åtkomstkontroll av dessa klasser: Top Secret (**TS**), Secret (**S**), Confidential (**C**) och Unclassified (**U**), där:

TS > S > C > U

Med andra ord ligger säkerhetsklassen **TS** överst i klasshierarkin. Sedan finns klassen **S**, klassen **C** och längst ner klassen **U**. Naturligtvis kan den obligatoriska åtkomstkontrollen byggas ut med flera säkerhetsklasser, beroende på organisationens behov.

2.3.3 Rollbaserad åtkomstkontroll

Rollbaserad åtkomstkontroll (RBAC) är generellt ansett som ett bra alternativ till både oberoende och obligatoriska åtkomstkontrollstyper. Åtkomstsrättigheterna i RBAC är associerade med roller (Fig.2). Organisationer definierar olika roller i samband med framtagning av organisationens säkerhetspolicies. Rollerna följer oftast organisationens struktur och arbetssätt. Användare av ett informationssystem kan erhålla medlemskap i en eller flera roller. Vanligtvis återspeglar rollerna olika funktioner inom en organisation. Användarnas åtkomst är baserat på deras yrken, kvalifikationer och ansvarsområden. Nya rättigheter kan lätt tilldelas utan större ingrepp i åtkomstmekanismerna, detsamma gäller vid ändring och borttagning av rättigheter. Varje roll kan tilldelas flera användare, dvs. återanvändas flera gånger. Tack vare att roller kan återanvändas anses RBAC som en kostnadseffektiv metod (Sandhu och Bhamidipati, 1999).

Barkley (1997) anser att rollbaserade åtkomstkontrollmodeller är helt oberoende av de systemmiljöer som de skall implementeras i, t.ex. kan de bli implementerade på nätverks-, operativsystems- eller databasnivån.

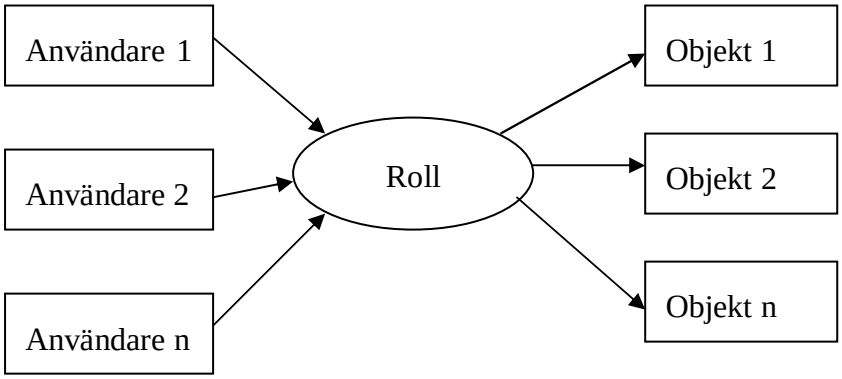

Fig.2. *Relationsfördelning av roller i RBAC (Stegmann, 1997).*

Poole et al. (1996) anser att RBAC från början har blivit utvecklat för att tillgodose industriföretagens behov. Huvudegenskap för RBAC är alla roller och inte klassificering av information. Varje roll har unika åtkomsträttigheter till delar av ett informationssystem. Stegmann (1997) menar att RBAC är en modell som kan tas fram med hjälp av observationer gjorda på anställdas funktioner i en organisation. Ofta följer dessa roller just användarnas ansvarsområden.

RBAC är en åtkomstkontrollmodell som lämpar sig för hälso- och sjukvården först och främst för att den kan återspegla organisationens struktur och att en roll kan användas för att förse flera användare med samma rättigheter (Stegmann, 1997; Bellettini et al., 2001).

RBAC är en av flera åtkomstkontrolltyper som kan användas för att skydda data i ett informationssystem. Denna typ är uppskattad p.g.a. att den reducerar åtkomstkontrollens komplexitet samt minskar administrativa kostnader när det gäller större informationssystem. RBAC-modellen stödjer även andra typer av åtkomstkontroll såsom t.ex. oberoende och obligatorisk åtkomstkontroll och är viktig när det gäller ökning av säkerhet där datoriserade informationssystem används (Bellettini et al., 2001).

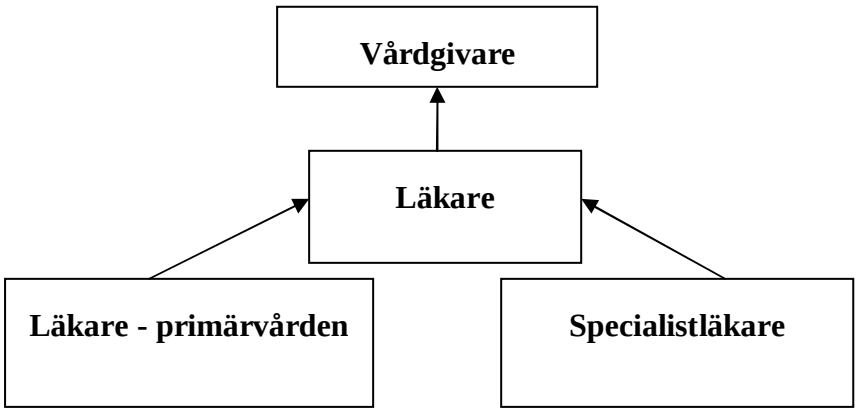

Fig.3. *Hierarkisk uppbyggnad av roller, ett exempel enligt Stegmann (1997).*

Roller som används i RBAC kan innehålla andra roller, denna uppdelning är uppbyggd på ett *hierarkiskt* sätt (Fig.3). Roller högre upp i hierarkier har tillgång till större mängder av data, t.ex. har rollen högst upp åtkomst till alla underliggande roller, medan rollen längst ner enbart har åtkomst till data inom just denna roll (Stegmann, 1997; Samarati och Jajodia, 1999).

Bertino (2003) hävdar att förutom de hierarkiska även finns *platta* arkitekturer för RBAC. Platt RBAC innehåller ett antal användare, roller, rättigheter och sessioner. Sessioner är instanser av kommunikation mellan användaren och systemet. Flera sessioner kan vara aktiva för en och samma användare samtidigt. Skillnaden mellan hierarkisk och platt RBAC är att i platt RBAC finns det inga extensioner av roller, roller innehåller inga andra roller.

Samarati och Jajodia (1999) anser att RBAC tillhandahåller åtkomst till data beroende på vilken typ av roll en användare har inom organisationen. En roll är definierad i organisationens säkerhetspolicies och är ett antal aktiviteter och uppgifter baserade på användarnas arbetsuppgifter. Rollerna identifierar de rättigheter som användare har för att kunna komma åt viss data, en roll kan vara t.ex. sjuksköterska, läkare eller sekreterare. Varje roll, inom RBAC, aktiveras genom en oberoende åtkomstmekanism. Det finns flera fördelar med att använda RBAC, en är att användarens identitet är separerad från dennes åtkomst till data. En annan fördel är att rollerna kan återanvändas, många användare kan erhålla en och samma roll. Ytterligare en fördel är att auktorisering av en roll är möjligt först när den är aktiv.

I större organisationer kan antalet roller växa upp till tusentals eller miljontals. Detta kan skapa stora problem för systemadministratörer som implementerar nya rättigheter och användare samt underhåller informationssystem. Regelverk för RBAC kan bli komplexa och svåröverblickliga. Det kan uppstå problem med att separera rollerna. En anställd kan inneha två olika roller som står mot varandra, t.ex. säljare och kund eller vårdgivare och patient. Då kan det uppstå konflikter när det gäller exekvering av vissa rättigheter, t.ex. en anställd kan även vara kund i företaget. Det kan även uppstå problem med rollernas företräde, alltså vilken roll som får exekveras först. RBAC:s största fördel är att flera användare kan signeras till en och samma roll utan att spårbarheten går förlorad. På detta sätt minskar det

administrativa arbetet. Detta arbete sker oftast centralt. Ytterligare ett steg för att minska belastningen är att decentralisera vissa delar av administrationen, men fortfarande ha övergripande ansvar när det gäller säkerhetspolicies centralt (Covington et al., 2001).

2.4 Mekanismer och synsätt

I denna uppsats används två viktiga begrepp när det gäller förbättringsförslag av åtkomstkontroll inom hälso- och sjukvården.

Det första begreppet är *mekanismer*. Med detta menas olika tekniska lösningar för att förbättra säkerheten och i synnerhet åtkomstkontrollen inom hälso- och sjukvården. Ett exempel på dessa är diverse mjukvaror som tillåter systemadministratörer att kontrollera användarnas åtkomst till data.

Det andra begreppet är *synsätt*. Synsätt är metoder, modeller eller tankesätt för att hjälpa organisationer att skapa säkrare informationssystem och hantera data och användare med avseende på åtkomstkontroll. Exempel på dessa är RBAC, DAC eller MAC.

3 Problemområde

I detta kapitel presenteras och förklaras problemområdet för denna uppsats. Här finns även själva problemet med begränsningar samt förväntat resultat.

Information om enskilda personer är en viktig del i många företags marknadsföringsarbete. Diverse data om privata personers vanor är ett viktigt verktyg, för många företag, för att kunna skaffa nya kunder. Sadan (2001) anser att i dagens samhälle är personlig data mycket eftertraktat för många organisationer. Olika företag använder dessa data inte bara i marknadsföringssyfte, utan också vid anställningar, för att få reda på om personerna är lämpliga. Personlig data används även för att kunna säga upp anställda.

Många människor vill hålla information om dem själva hemlig. Vissa av dem anser att all personlig information bör hållas hemlig, medan andra anser att viss information kan vara tillgänglig för andra och att det inte är farligt att exponera viss information. Inom hälso- och sjukvården finns det mycket data med hög grad av känslighet. Många länder i Västeuropa tillämpar synsättet att varje patient äger informationen om sig själv. För att säkerställa att ingen känslig information om en patient kommer ut i orätta händer, har landets politiker instiftat olika lagar som reglerar åtkomst till data samt lagar gällande publicering av personlig information (Sadan, 2001).

Poole et al. (1996) anser att hälso- och sjukvården är ett grundläggande område i nästan varje land i världen. Det finns stora mängder av känslig data i denna miljö, data om patienter, deras hälsa och deras medicinska historik, osv. Det finns behov av att hålla denna information hemlig då patienternas integritet är viktig. I början användes centraliserade informationssystem, men under senare tid är distribuerade system mer använda. Detta beror på att det inom dagens sjukvård krävs samarbete mellan olika avdelningar och organisationer. Distribuerade informationssystem inom sjukvården kräver starka auktoriseringsmekanismer, som värnar om patienternas integritet eller informationens sekretess. Patientjournaler måste skyddas så att en icke auktoriserad användare kan få åtkomst till dem. Säkerhetspolicies bör skapas inom varje organisation för att kunna bestämma åtkomst. För att skapa sådana policies bör en analys av organisationen och dess information göras. Oberoende åtkomstkontroll är den mest förekommande åtkomstkontrolltypen inom sjukvården. För att uppfylla alla krav som ställs på informationssystem inom hälso- och sjukvården genom diverse lagar måste mer kraftfulla åtkomstkontrollmekanismer appliceras. En sådan mekanism kan vara t.ex. MAC eller RBAC. Det som utmärker RBAC är att denna typ är mer flexibel än t.ex. MAC (Poole et al., 1996; Bleumer,1994; Yialelis et al., 1996).

En studie om åtkomstkontroll som är gjord på flera hemvårdcentraler i Skaraborg visar att säkerhetspolicies och framförallt policies som rör åtkomstkontroll inte är helt klara (Åhlfeldt, 2003). Olika yrkesgrupper har samma åtkomsträttigheter. Det finns ingen, eller obefintlig rollindelning inom olika nätverk och inga klara gränser när det gäller åtkomst till data. Den mest förekommande modell som används i denna miljö är loggningsmodellen med ett begränsat åtkomstområde. Användare har tillgång till all data, men deras aktiviteter kan kontrolleras efteråt

med hjälp av loggningslistor. Generellt, finns det bristfälligt stöd för kontrollrutiner av dataåtkomst. I vissa fall förekommer ingen kontroll av loggingslistor, i andra fall utförs en sådan kontroll manuellt och är slumpmässig (Åhlfeldt, 2003). Loggningsmodellen gör att användare kan komma åt data innan systemadministratörer hinner upptäcka det och skadan har då redan skett. Bristande kontroll av loggingslistor kan medföra att ett flertal icke auktoriserade användare får åtkomst till information utan att det upptäcks.

Ibland kan det finnas ett behov av att komma åt information som i vanliga fall inte är tillgänglig för användare. Behörighetsbegränsningar kan skapa problem med att kunna nå information utanför användarnas åtkomstområde. Enligt Smith och Eloff (1998) finns det problem med ”plötslig åtkomst” till data inom hälso- och sjukvårdsmiljön. Med ”plötslig åtkomst” menas åtkomst till data som användare vanligtvis inte har åtkomst till. Användare inom varje hälso- och sjukvårdsorganisation har tillgång till information som de behöver för att kunna utföra sina arbetsuppgifter, t.ex. krävs patientjournaler för att kunna se patientens tidigare behandlingar, sjukdomar, osv. Ibland kan användare behöva data som ligger utanför deras åtkomstområde. I dessa fall är det viktigt att ha mekanismer som möjliggör åtkomst till sådan data på ett säkert sätt. Hälso- och sjukvårdsmiljön har utvecklat starkt samarbete mellan olika avdelningar men också mellan olika organisationer. Distribuerade informationssystem gör detta möjligt. Personal som jobbar på olika avdelningar eller i andra delar av organisationen kan ibland behöva ha åtkomst till data som vanligtvis inte är tillgänglig för dem.

Ett annat problem som finns inom hälso- och sjukvården är att integration av olika aktörer skapar hot om att användare får tillgång till mer information än de behöver för att utföra sina arbetsuppgifter. Användare i många organisationer inom sjukvården, kommer åt diverse data genom inloggning på olika system, vilket kan skapa möjligheter till ickeauktoriserad åtkomst. Användning av loggningsmodellen inom hälso- och sjukvården medför ökad risk för ickeauktoriserad åtkomst till information samt orsakar mer administrativt arbete på lång sikt. På kort sikt minskas det administrativa arbetet genom att ingen behörighetstilldelning krävs, men på lång sikt skapar loggningsmodellen mer arbete genom att loggningslistor skall kontrolleras. För att säkerställa att information skyddas från ickeauktoriserad åtkomst samt att bibehålla datas integritet krävs det mer kraftfulla mekanismer (Jakobsson et al., 2002).

Enligt flera forskare, t.ex. Jakobsson et al. (2002), Smith och Eloff (1998) och Rindfleisch (1996), finns det problem när det gäller informationsåtkomst inom hälso- och sjukvården. Ibland finns det behov att komma åt information som vanligtvis inte är tillgänglig. Ibland har användare tillgång till mer information än vad som krävs för att utföra deras arbetsuppgifter. Det är svårt att definiera gränser för dataåtkomst, därför får användare ofta åtkomst till mer information än nödvändigt. Det är därför intressant att undersöka hur åtkomstkontroll fungerar inom olika organisationer inom hälso- och sjukvården. För att dels peka på de brister som finns och dels för att försöka ge förbättringsförslag om hur åtkomstkontroll kan förbättras m. h. a. olika mekanismer och metoder.

3.1 Problemprecisering

Målet med detta arbete är att:

Undersöka hur åtkomstkontrollen fungerar inom hälso- och sjukvården och utifrån denna undersökning studera hur olika problem, när det gäller åtkomstkontrollen, kan lösas eller minimeras.

- Undersöka hur dagens åtkomstkontroll fungerar inom hälso- och sjukvården.
- Granska och studera i litteraturen alternativa mekanismer och metoder som kan användas för att minska eventuella problem som finns i samband med åtkomstkontroll i de undersökta områdena idag.

3.2 Avgränsningar

Arbetet kommer att innefatta studier av tre olika vårdgivarorganisationer nämligen slutenvård, primärvård och hemvård. Detta görs för att erhålla ett bredare perspektiv för hur åtkomstkontroll fungerar i hälso- och sjukvården. Studierna kommer att utföras genom ett antal intervjuer inom varje organisation och kommer att innehålla intervjuer med både användare och systemadministratörer.

Nästa steg i detta arbete är att, med hjälp av litteraturstudier, undersöka om det finns metoder och mekanismer som kan hjälpa till att eliminera eventuella problem som finns inom de granskade områdena. Studierna kommer att fokusera på organisationer som har haft liknande problem och som har lyckats lösa dessa. Dessa metoder och mekanismer kommer att presenteras och diskuteras i detta arbete.

3.3 Förväntat resultat

Ett delproblem i detta arbete är att studera hur åtkomstkontroll fungerar inom hälso- och sjukvården. Enligt studier gjorda i Skaraborgsregionen, i västra Sverige används ofta loggningsmodellen för att kontrollera åtkomst till data inom hemvården (Åhlfeldt, 2003). Ett förväntat resultat av arbetet är att kartlägga hur åtkomstkontroll ser ut inom hemvården, primärvården samt slutenvården och om dessa organisationer använder samma typ av åtkomstkontroll. Ett annat förväntat resultat är att få klarhet i om användarna får åtkomst till tillräckligt mycket information för att kunna utföra sina arbetsuppgifter samt om användarna har tillgång till för mycket data. Detta arbete har också för avsikt att om det finns brister inom den nuvarande åtkomstkontrollen.

Ett annat delproblem i detta arbete är att undersöka i litteraturen om det finns metoder och mekanismer som kan användas för att lösa de problem som finns, enligt användare och systemansvariga inom hälso- och sjukvården, för att förbättra eller komplettera dagens åtkomstkontroll. Ett förväntat resultat är att hitta flera olika metoder och/eller mekanismer som kan tillämpas inom de undersökta områdena.

4 Metoder och genomförande

I detta kapitel presenteras de forskningsmetoder som kommer att användas i detta arbete samt motivering till varför de valts. Vidare beskrivs även de metoder som skulle lämpa sig för detta arbete, men som valts bort.

4.1 Litteraturstudie

En del i problempreciseringen som är beskriven i kapitel 3.1 är av sådan art att den bästa metoden för att lösa denna är litteraturstudier.

Enligt Berndtsson et al. (2002) finns det flera tekniker och metoder för att samla information. En av dem är litteraturstudien som är en viktig metod när det gäller att undersöka vad som finns skrivet inom ett visst område. Genom att studera litteraturen kan forskare skapa sig en bild av vad som, enligt andra forskare, är viktigt och aktuellt just inom det undersökta området. Detta arbete handlar bl.a. om att titta på olika åtkomstkontrollmekanismer och synsätt, därför kommer artiklar och publikationer att undersökas och läsas.

Patel och Davidson (1994) anser att det är avgörande för arbetet att hitta en bra strategi, när litteraturstudien skall genomföras. Det är viktigt att undersöka källor och författare för de vetenskapliga dokument, som ingår i arbetet. Deras trovärdighet skall fastställas. För att göra detta skall författaren undersöka om källorna som publicerar dessa artiklar är erkända och seriösa. Detta görs genom att undersöka om dessa källor tas med i andra vetenskapliga arbeten. Författarna skall kontrolleras på samma sätt. Vissa författare anses kunniga inom ett visst område och andra arbeten refererar till dessa författare. För att arbetet skall innehålla endast relevanta artiklar måste ställning till dessa tas utifrån problempreciseringen. I detta arbete kommer både författarna och källorna att kontrolleras m.h.a. att undersöka om dessa förekommer i andra arbeten samt om de anses trovärdiga bland andra forskare.

4.1.1 Validitet och tillförlitlighet

I detta arbete utforskas endast material som finns inom arbetets problemområde, dvs. material som handlar om rollbaserade metoder och mekanismer. Relevant material skaffas för att sedan kunna evalueras och diskuteras. Detta tillvägagångssätt kallas *validitet* (Patel och Davidson, 1994).

Det är viktigt att det anskaffade materialet är trovärdigt, att det kommer från tillförlitliga källor. Materialet i detta arbete hämtas från vetenskapliga artiklar samt från andra trovärdiga källor såsom böcker och tidsskrifter som andra artiklar refererar till. Med andra ord läggs det stor vikt vid artiklarnas *tillförlitlighet* (Patel och Davidson, 1994).

4.2 Intervjuer

Det andra delproblemet i detta arbete handlar om att undersöka dagens åtkomstkontroll inom hälso- och sjukvården. Patel och Davidson (1994) anser att intervjuer är en teknik som används för att samla in information. Berndtsson et al. (2002) anser att det finns två typer av intervjuer, *öppna* och *stängda*. Öppna intervjuer bygger på en diskussion mellan intervjuaren och den som intervjuas. Intervjuaren förbereder ett antal frågor, men har sedan friheten att ställa

följdfrågor beroende på erhållna svar. Stängda intervjuer följer på ett strikt sätt de frågor som intervjuaren har förberett innan. Det finns ytterligare en typ av intervjuer, som är en blandning av de två förstnämnda, som kallas semistrukturerad. Val mellan dessa två typer av intervjuer görs beroende på vad intervjuaren vill undersöka.

Patel och Davidson (1994) menar att när intervjufrågor skall framställas måste två aspekter tas i beaktning. Den första är hur mycket ansvar som intervjuaren skall få när det gäller frågeutformning och ordning på frågor. Den andra aspekten är hur mycket frihet den intervjuade personen skall ha när det gäller tolkning av frågor. Tolkning kan baseras på egna erfarenheter eller inställning till något.

En del av arbetets problemprecisering handlar om att studera dagens åtkomstkontroll inom hälso- och sjukvården. En lämplig metod för att få reda på det är intervjuer. Det är viktigt för arbetets resultat att undersöka detta problem från två perspektiv nämligen användarnas och systemadministratörernas perspektiv. Det finns viktig information som kan erhållas från administratörens sida, t.ex. information om systemets struktur och hur åtkomst tilldelas. Intervjuer med användarna skall skapa en bild av hur användaren upplever det nuvarande systemet och vilken grad av åtkomst till information varje användare har. För att erhålla relevant information är det viktigt att analysera och studera problemprecisering och utifrån den ställa frågor. Frågorna skall vara utformade på ett sådant sätt att både användare och administratörer kan besvara dem på ett bra sätt och att betydelsefull information erhålls för att kunna lösa problemet.

4.3 Alternativa metoder

Det finns även andra metoder som kan användas för att besvara problempreciseringen i detta projekt. En av dessa metoder är *fallstudie*. Berndtsson et al. (2002) påpekar att fallstudie kan användas för att undersöka ett problem på djupet. En viktig egenskap, som fallstudie har, är att studien kan genomföras på ett eller ett begränsat antal fall. Problemprecisering i detta arbete är av sådan art att det skulle vara möjligt att genomföra undersökning i form av en fallstudie. Största problemet med att använda fallstudien, i detta arbete, är att tre organisationer skall undersökas. Därför skulle det ta betydligt mer tid och kräva större resurser från både författare och de undersökta organisationerna, vilket inte var möjligt i detta fall då resurserna inte fanns.

En annan metod som kan användas i detta arbete är enkätundersökning. Patel och Davidson (1994) anser att enkätundersökningar är bättre än intervjuer när det gäller att få fram åsikter från ett större antal personer. Enkätundersökningar kan vara antingen stängda eller öppna. Vid stängda enkätundersökningar kryssar den intervjuade personen det alternativ som anses vara bäst. Vid öppna enkäter får den intervjuade besvara frågor med egna ord. Problemets art, i detta projekt kräver intervjuer. Under intervjuer kan det uppkomma frågor som intervjuaren eller den intervjuade kan besvara direkt. Det kan inte göras med enkätundersökningar.

Med hänsyn till problemprecisering som finns i kapitel 3.1, bedömdes intervjuer och litteraturstudie att vara mest lämpliga metoder för att genomföra detta arbete.

4.4 Genomförande

I denna del presenteras hur detta arbete har utformats och utförts med hänsyn på problemprecisering som finns i kapitlet 3.1.

Första fasen i detta arbete var att ta fram problemområdet och att utforma problemprecisering. Problemområdet togs fram med hänsyn till författarens forskningsintresse som är datasäkerhet och särskilt åtkomstkontroll. Utformningen av både problemområdet och problempreciseringen skedde m.h.a. undersökning av vad som finns skrivet inom detta området.

Nästa steg i arbetsprocessen var att undersöka vilka metoder som kan vara lämpliga för att kunna genomföra detta arbete. Flera olika metoder har studerats med avseende på den framarbetade problempreciseringen. Slutligen två metoder har tagits fram som användes för att lösa den framtagna problempreciseringen. Den första metoden var intervjuer, som hjälper att få inblick i hur åtkomstkontrollen ser ut i dagen hälso- och sjukvård. Den andra metoden var litteraturstudie, som möjliggör att hitta eventuella alternativa lösningar på vissa problem som finns inom hälso- och sjukvården när det gäller åtkomstkontroll.

Intervjuer är en bra metod när det gäller att samla in information (Patel och Davidson, 1994). Problempreciseringens art krävde ett antal intervjuer. Problempreciseringen spänner över flera olika områden inom hälso- och sjukvården, nämligen sluten-, primär- och hemvården. Då dessa organisationer styrs av olika huvudmän kan eventuella skillnader uppmärksammas. Arbetet begränsades till Skövdeområdet. För att genomföra intervjuer inom slutenvården kontaktades Kärnsjukhuset (KSS) i Skövde. Intervjuer inom primärvården gjordes på vårdcentralen i Timmersdala. För att undersöka hur åtkomstkontrollen fungerar inom hemvården undersöktes hemvården i Skövde kommun. Det uppstod problem med att hitta respondenter för intervjuer. Hög arbetsbelastning gjorde detta svårt. Det fanns även viss grad av misstänksamhet bland användare när det gällde att ställa upp på en intervju.

För att få inblick i både hur åtkomstkontrollen är uppbyggd samt hur den upplevs gjordes två typer av intervjuer inom varje organisation, en med användarna och en med systemansvarige. Inom varje organisation gjordes tre intervjuer, en med systemansvarige och två med användare. Varje intervju skickades tillbaka till respondenten för att denne skulle bekräfta att det som har skrivits ner blev sagt under intervjun.

Efter att alla intervjuer blev genomförda sammanställdes dessa för att kunna analyseras. Analys var ett viktigt steg i arbetsprocessen för utifrån analysen kunde problem med åtkomstkontrollen i hälso- och sjukvården hittas. Analysen pekade också på positiva sidor hos den nuvarande åtkomstkontrollen.

Nästa fas i arbetsprocessen var att, utifrån den tidigaregjorda analysen, undersöka i litteraturen om det finns alternativa sätt att kunna lösa de problem som finns i dagens hälso- och sjukvård, enligt användarna och systemansvariga, när det gäller åtkomstkontroll. Utifrån dessa problem analyserades litteratur, främst vetenskapliga artiklar.

Slutligen diskuterades arbetet med avseende på det som har framkommit både ur intervjuer men också från litteraturstudier. Arbetet granskades kritiskt. Under arbetets gång framgick det också andra aspekter som kan undersökas inom

problemområdet. Dessa antecknades i slutet som förslag till andra arbete inom detta området.

5 Sammanställning av intervjuer

I detta kapital presenteras en samanställning av genomförda intervjuer. Denna sammanställning är viktig för analysen av hur åtkomstkontrollen ser ut inom hälso- och sjukvården. Under varje fråga sammanställs de svar som har erhållits från varje undersökt del, nämligen från primär-, sluten- och hemvården.

5.1 Intervjuer med systemansvariga

Nedan presenteras en sammanställning av svar erhållna från ansvariga för system som används inom dessa tre delar av hälso- och sjukvården (bilagor: 1a, 2a och 3a):

1. **Hur ser Era system ut med avseende på åtkomstkontroll? Hur fungerar åtkomstkontrollen?**
   Primärvården: Varje vårdcentral har ett eget nätverk. Inom dessa nätverk finns olika program, t.ex. program med patientjournaler, som användare har åtkomst till.
   Slutenvården: Inom slutenvården finns sammanlagt 154 olika system fördelade på fyra sjukhus och ca 4700 användare. Behörigheter tilldelas på systemnivå beroende på vilka system som användare behöver komma åt.
   Hemvården: Inom hemvården används ett system som heter MagnaCura. Detta system används av olika yrkeskategorier inom omvårdnadsförvaltningen. Systemet förser organisationen med möjligheten att kontrollera åtkomsten till information.
   a. **Tillämpar Ni behörighetsmodellen eller får användare logga in sig och sedan har Ni möjlighet att kontrollera användarnas ”aktivitet” inom systemet?**
      Primärvården: Användare har olika behörigheter för att komma åt data. För att kontrollera användarnas aktiviteter används inloggningar. På loggningslistor kan ses vilket data användaren har tittat på. Denna kontroll kan genomföras i efterhand.
      Slutenvården: Det finns en form av behörighetsmodell. Rollindelningen sker lokalt, alltså inom varje system. Lokala IT-samordnare tilldelar nya användare roller beroende på deras arbetsuppgifter.
      Hemvården: MagnaCura skapar bilder för varje yrkesgrupp. Dessa bilder kan jämföras med roller. Bilderna begränsar användarnas åtkomst till informationen. Inom varje bild kan olika rättigheter skapas beroende på användarnas arbetsområde. Vissa användare kan t.ex. endast ha läsrättigheter medan en annan även kan skriva inom en viss bild.
   b. **Vilken autentisering använder ni i Era system? (ex. lösenord)**
      Primärvården: Autentisering som används inom primärvården är användarnamn och lösenord, som är personliga för varje användare. Användarna uppmanas att byta lösenord var 90:e dag.
      Slutenvården: Inom slutenvården används personliga användar-id samt lösenord. Lösenord består av fem tecken och är utan några krav på användning av siffror och bokstäver.

Hemvården: Användar-id samt lösenord används för att komma in i systemet. Dessa är personliga. Användarna uppmanas att byta lösenord med jämna mellanrum.

2. **Vilka för- resp. nackdelar har denna hantering av åtkomstkontroll?**
   Primärvården: Enligt ansvarige för systemet fungerar nuvarande hantering av åtkomsten tillfredställande. Loggningslistor är ett viktigt verktyg för att kontrollera vilken information som användarna har kommit åt. Även patienter kan begära att få se loggningslistor för deras journaler. En nackdel med det nuvarande systemet är att endast hela moduler kan spärras för olika användare. Det går inte att spärra en del i en modul. En modul är en del av systemet, t.ex. program där finns alla patientjournaler, eller program med personaldata.
   Slutenvården: Autentisering anses som grundläggande mekanism för att identifiera användare inom ett visst system. Detta är viktigt för att kunna säkerställa deras identiteter. En nackdel med den nuvarande åtkomstkontrollen är avvecklingsrutiner. Det brister i kommunikationen mellan personalansvariga och systemansvariga. Systemansvariga har svårt att få reda på om en viss användare har slutat eller bytt arbetsuppgifter.
   Hemvården: Den största fördelen med att använda detta system är bilderna för olika yrkesgrupper, m.h.a. detta regleras åtkomst till informationen för olika användare. En annan fördel med att använda detta system är att åtkomst till informationen regleras på samma sätt inom hela organisationen. Spårbarheten är också en fördel när det gäller det nuvarande systemet. Loggningslistor gör det möjligt att spåra användare. En nackdel med att använda detta system är att vissa delar av systemet inte fungerar tillräckligt bra. Detta beror på det tekniska inom systemet och är på väg att åtgärdas.
   a. **Anser Ni att det finns andra metoder/sätt som kan vara mer lämpliga att använda?**
      Primärvården: Det nuvarande systemet anses mest lämpligt för tillfället.
      Slutenvården: Automatiska system anses vara mer lämpliga för att hantera åtkomstkontrollen. Dessa system skulle ge signal via personalsystem till behörighetssystem. Det finns ett möjligt problem som skulle uppstå med dessa system i dagens läge, nämligen att personalsystemen alltid måste vara uppdaterade. Det kan vara problematiskt med fördröjning av informationen inom organisationen.
      Hemvården: Det nuvarande sättet att hantera åtkomst till information anses vara tillfredsställande för organisationen.

3. **Vilka policies eller regler använder Ni er av för att säkerställa att en viss användare skall ha tillgång till en viss data?**
   a. **Hur vet Ni vilken data som en viss användare skall ha tillgång till?**
      Primärvården: Varje vårdcentral skapar egna policies gällande åtkomst till information. Dessa baseras på arbetsuppgifter, erfarenheter samt förtroende för personalen. Ofta har läkare och

sjuksköterskor samma bredd när det gäller åtkomst, men olika rättigheter (t.ex. skiva, läsa).
Slutenvården: Vårdchefen bestämmer vilka system som användare skall ha åtkomst till. Denna tillgång till informationen regleras alltså på systemnivån och inte på datanivån.
Hemvården: Det finns en arbetsgrupp som bestämmer utifrån gällande lagstiftning hur åtkomst till informationen inom denna organisation skall se ut. En systemadministratör känner till dessa bestämmelser och tilldelar behörigheten utifrån dessa. När en behörighet för en ny användare skall tilldelas erhåller systemadministratören information om denne användare. Utifrån denna information tilldelas användare en behörighet.

b. Vilken typ av information får Ni om användaren för att säkerhetställa att just han/hon skall ha tillgång till en viss data?
Primärvården: Vårdcentralchefen informerar systemansvarig vilken information som skall vara tillgänglig för varje användare eller användargrupp.
Slutenvården: Systemansvarige får tillgång till användarens personuppgifter samt uppgifter som berör vilka system som denna användare skall ha åtkomst till.
Hemvården: Varje ny användare anmäls till systemadministratören av chefen för enheten som användaren är anställd på. Uppgifter såsom användarens personnummer samt arbetsuppgifter skickas till systemadministratören.

4. Vad har Ni för procedur när Ni tilldelar en användare åtkomst till viss data?

a. Hur går Ni till väga rent praktiskt? Berätta steg för steg.
Primärvården: Åtkomsten tilldelas m.h.a. mallar som har skapats tidigare. För att tilldela nätverksrättigheter anmäls varje ny användare centralt till IT-enheten.
Slutenvården: Den nyanställdes närmaste chef eller IT-samordnare skickar ett underlag på vilka system som skall tilldelas denna användare. Efter att ha erhållit detta underlag tilldelas användaren användar-id samt lösenord. Till varje användare kopplas det rättigheter som denna har inom vissa system.
Hemvården: Varje användare registreras i systemet utifrån, av systemadministratören, erhållna uppgifter. Användaren tilldelas användar-id samt lösenord. Efter att ha fått dessa kan användaren börja använda systemet i sitt arbete.

b. Anser Ni att denna procedur är tillfredsställande och om inte hur skulle Ni vilja utveckla den?
Primärvården: Detta tillvägagångssätt anses tillfredställande inom den nuvarande organisationen.
Slutenvården: Rutinen vid tilldelningen av användar-id och lösenord för nya användare anses vara tillfredsställande därför att om det inte tilldelas ett användar-id då reagerar antigen användarens chef eller användaren själv på detta.

Hemvården: Denna procedur anses fungera tillfredställande inom denna organisation. Vad som också är viktigt är att användaren uppmanas att byta lösenordet med jämna mellanrum.

5. **Finns det någon rollindelning bland användare och i så fall vilka kriterier som styr denna uppdelning?**
   Primärvården: Det finns en rollfördelning bland alla användare inom organisationen. Denna indelning beror oftast på den yrkesgrupp som en användare tillhör. Rollfördelningen kan även bero på chefen på varje vårdcentral. Det är vårdcentralchefen som bestämmer vilka delar av systemet skall ingå i en viss roll.
   Slutenvården: Det finns rollindelning inom slutenvården. De roller som förekommer är: läkare, sjuksköterska, undersköterska, sjukgymnast, systemadministratör samt övrig personal. Denna indelning beror på användarnas yrkesroller.
   Hemvården: Det finns indelning inom detta system. Genom att systemet använder bilder kan olika användare delas in i olika grupper. Arbetsuppgifter styr huvudsakligen denna indelning.

6. **Anser Ni att det, i vissa fall, finns risk att användare kan behöva information som de i vanliga fall inte har åtkomst till? Om ja, hur kan de få tag på den?**
   Primärvården: Detta beror på varje vårdcentral. På vissa vårdcentraler har användare en bredare åtkomst än på andra. När ett sådant behov uppstår kan åtkomsten vidgas ut av systemadministratören. Det är vårdcentralchefen på varje vårdcentral som bestämmer om sådan åtgärd är nödvändig och vilken information som skall göras tillgänglig.
   Slutenvården: Generellt sett finns det inga behov av att användare skall komma åt information som ligger utanför dennes behörighetsområde. Detta beror på att användare är kopplade till de system som krävs av användarnas arbetsuppgifter och inte till data. På det sättet får användarna åtkomst till all den information som anses vara viktig för specifika användare. Den information som användarna kan sakna är informationen från andra delar inom sjukvården t.ex. primärvården. I dagens läge finns det ingen interaktion när det gäller informationssystem mellan sluten- och primärvården. Informationsutbytet mellan dessa får ske via post eller telefon.
   Hemvården: Användarna har tillfredställande åtkomst till informationen. Det har inte hänt någon gång att användare behövt komma åt information som inte funnits tillgänglig för dessa i vanliga fall. Om sådan situation skulle uppstå skulle arbets- och ledningsgruppen ta ställning till eventuell utökning av åtkomsten.

7. **Anser Ni att det kan finnas risk, generellt, för att användare får tillgång till mer information än de behöver för att utföra sitt arbete? (till exempel sådan information som inte berör behandling av en viss patient).**
   Primärvården: Det finns möjlighet att en användare kommer åt information som inte bör vara åtkomlig, men detta kan kontrolleras m.h.a.

loggningslistor. I dessa listor finns även tider under vilka användare har undersökt viss information. Dessa tider kan ge en indikation om ifall användaren kom åt informationen av misstag eller om denne gjorde det med avsikt. Personalen är väl medveten, genom utbildning, om vad som gäller vid åtkomst till information och vilken information de inte får se.
Slutenvården: Det kan finnas risk med att användarna får tillgång till mer information än vad som egentligen krävs för deras arbetsuppgifter. Detta beror just på att åtkomsten sker på systemnivå och inte på datanivå. En viktig aspekt är att t.ex. patientjournaler fortfarande finns i pappersformat. Detta innebär att dessa får läsas, i princip, av vem som helst utan att det kan spåras.
Hemvården: Användare har åtkomst till informationen inom alla distrikten. Detta beror på att användare arbetar på olika ställen. Därför är det viktigt att informationen finns tillgänglig. Eventuell begränsning av nuvarande åtkomst är inte nödvändig. Även om all information inte används dagligen är det viktigt att ha denna åtkomlig i de fall där användarna behöver den.

a. **Hur anser Ni att sådana risker kan reduceras?**
   Primärvården: Loggningslistor är ett bra instrument för att kunna kontrollera användarnas aktiviteter inom ett informationssystem.
   Slutenvården: Åtkomsttilldelning på datanivå skulle reducera dessa risker. När det gäller patientjournaler så pågår just nu ett projekt för att göra dessa journaler digitala. På det sättet minskar riskerna för obehörig åtkomst.
   Hemvården: All information som användarna har åtkomst till idag anses vara behövlig för dessa. Enligt organisationen finns det inga sådana risker.

8. **Hur anser Ni, att åtkomstkontroll skall se ut för att den skall uppfylla krav ställda från verksamheten, lagar samt användarkrav? Berätta hur en optimal åtkomstkontroll skall se ut enligt Er.**
   Primärvården: Det anses att det nuvarande systemet fungerar tillfredsställande för att klara av de krav som finns från organisationen samt lagstiftningen. Det finns dock vissa brister i systemet som bör åtgärdas. En av dem är att det borde vara möjligt att kunna spärra vissa delar i en modul och inte som det är idag att det endast finns möjlighet att spärra hela modulen. En annan brist är att vissa personliga inställningar i systemet borde göras endast av systemadministratören. I dagens system är det möjligt att en van användare själv kan ändra vissa inställningar i systemet så att vissa filer blir åtkomliga för denne.
   Slutenvården: Det optimala skulle vara en åtkomstmatris med följande parametrar: Roll, grupp, rättigheter och dataterm. Detta skulle innebära en förenkling av det administrativa arbetet. Det skulle fungera bra endast om antalet undantag inte skulle vara för stort. Problemet med en sådan lösning är att den inte går att implementera i många gamla system.
   Hemvården: Det nuvarande systemet anses uppfylla alla de kraven som ställs utifrån verksamheten och lagstiftningen. Olika delarna inom organisationen hålls skilda. Det finns dock en önskan om att dessa delar skall ha större åtkomst till varandras information.

5.2 Intervjuer med användare

I denna del presenteras intervjuer med användarna av system inom primär-, sluten- och hemvården (bilagor: 1b, 1c, 2b, 2c, 3b och 3c):

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   Primärvården: För att komma åt informationen som finns i systemet måste användarna logga in sig på nätverket. Personliga användar-id och lösenord används för detta. För att komma åt diverse program som finns i systemet måste användarna logga in på varje program. Användarna uppmanas med jämna mellanrum att byta sina lösenord.
   Slutenvården: Inom slutenvården finns det ett intranät som heter Fokus. För att komma in på intranätet måste användaren logga in sig m.h.a. ett användar-id och lösenord. Dessa är personliga för varje användare. Efter inloggningen kommer användaren åt sina personliga sidor med de inställningar som gjordes just för denna användare. För att kunna använda andra program som finns tillgängliga på användarnas personliga sidor måste varje användare logga in sig på varje program.
   Hemvården: Varje användare har ett personligt användar-id samt lösenord som används för att komma in på systemet. För att kunna använda de olika programmen som finns i systemet måste användarna logga in sig på dessa separat, alltså inloggning på dessa program sker varje gång programmet används av en användare. Användarna uppmanas att byta lösenord var 60:e dag.

2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   Primärvården: Användarna anser att åtkomsten till informationen fungerar tillfredställande, generellt sett. Åtkomst sker på ett snabbt sätt och det finns inga störningar. Behörigheten anses vara ett gott hjälpmedel för att kontrollera åtkomsten.
   Slutenvården: Enligt användarna fungerar åtkomsten till information tillfredställande med det nuvarande systemet. Ibland kan det uppkomma vissa komplikationer som avbrott eller andra fel. Användarna anser att dessa avbrott är acceptabla och menar att sådana typer av avbrott och fel uppkommer i de flesta datasystem.
   Hemvården: Åtkomsten till informationen fungerar tillfredställande, enligt användarna. Det finns inga svårigheter att nå den information som söks av användarna. Användarna anser att själva systemet har vissa brister, men dessa är acceptabla. Användarnas arbetsuppgifter kräver ofta åtkomst till informationen på flera olika platser, därför anses det att en bredare åtkomlighet till denna löser problem som uppkommer i det dagliga arbetet.

3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   Primärvården: Intervjuade personer hade behov av att komma åt patientjournaler, provsvar, information om olika läkemedel, tidsbokning

samt en allmän information om nya trender och metoder inom hälso- och sjukvården.
Slutenvården: Informationen som behövs för att användarna skall kunna utföra sina arbetsuppgifter är av olika slag. Användare behöver data rörande personal, t.ex. schemaläggning. En annan typ av data som behövs är information om patientbeläggning, blodgruppering, provsvar, information om läkemedel samt PM och annan information som erhålls via mail. Patientjournaler finns fortfarande i pappersformat.
Hemvården: Användarna behöver olika slags information. Information om diverse lagförändringar, sekretesslagen, tidigare information om patienter samt information om politiska beslut är några exempel på typer av information som behövs av användarna. Även information om patienter, läkemedel samt information rörande ändring av rutiner är viktig för användarna.

4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
Primärvården: Generellt anses att informationen är åtkomlig vid rätt tidpunkt samt att användarna erhåller rätt information. Det viktigaste, enligt användarna är att lära sig systemet för det är oftast det som är orsaken till störningarna. Eventuella ändringar i systemet meddelas personalen i god tid.
Slutenvården: Användarna anser att den information som krävs är tillgänglig vid rätt tidpunkt. Det finns inga problem med att komma åt den information användarna behöver vid olika tillfällen. De problem som kan uppkomma är av tekniska slag, alltså att det blir avbrott eller något annat fel i systemet och inte att det beror på åtkomsttilldelning av information.
Hemvården: Generellt anser användarna att informationen som erhålls är rätt och att den begärda informationen är åtkomlig vid rätt tidpunkt. Informationen är uppdaterad, på det sättet får användarna aktuell information. Det kan uppstå vissa problem ibland, men dessa är mer av tekniska slag och beror inte på åtkomstsvårigheter.

   a) Om Ni inte får rätt information i rätt tid, vad, anser Ni, att det beror på?

   Primärvården: -

   Slutenvården: -

   Hemvården: Den information som inte är rätt beror oftast på den mänskliga faktorn och inte på systemet. Detsamma gäller tidpunkten för åtkomligheten av viss information. Användarna anser att inte allt går att lösa via datasystem utan viss information måste inhämtas via t.ex. personliga kontakter. Informationen som ligger utanför hemvården, t.ex. i primär- eller slutenvården inhämtas via post eller telefon.

5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**

Primärvården: Användarna anser att åtkomsten till informationen är tillfredsställande och att den uppfyller de krav som ställs från verksamheten och lagstiftningen. Den information som finns tillgänglig för användarna anses vara tillräcklig för att användarna skall uppfylla sina arbetsuppgifter.
Slutenvården: Användarna finner att den åtkomst till information som finns för närvarande uppfyller de krav som ställs på den från både verksamheten och lagstiftningen. Användarna är medvetna om och följer de sekretessföreskrifter som finns när det gäller informationen inom hälso- och sjukvården.
Hemvården: Enlig användarna är den nuvarande åtkomsten till informationen tillräcklig. I vissa fall skulle en utökning kunna vara aktuell, men detta påverkar inte användarnas arbete i någon större grad.

6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
Primärvården: Användarna anser att det finns tillräckligt med information inom deras behörighetsområde. Den enda typen av information som dessa användare saknar är information om deras patienter som finns på andra ställen, t.ex. inom slutenvården. Enligt användarna skulle ett samarbete mellan olika delar av hälso- och sjukvården vara önskvärt.
Slutenvården: Information som finns tillgänglig för de intervjuade personerna anses vara tillräcklig. Användarna anser att den behörighet som har tilldelats dessa är tillfredsställande. Även om det ibland förekommer att användarna behöver någon information som ligger utanför deras behörighet så finns det olika sätt att få reda på denna information.
Hemvården: Det kan uppstå vissa problem med att få tag på information enligt de intervjuade personerna. Ett exempel på detta är gamla beslut. Användare får i dagens läge vända sig till andra instanser för att få tag på dessa beslut. Ett annat exempel är information mellan sjuksköterskor och biståndsbedömare. Det finns strikta regler för vilken information som skall vara tillgänglig. Sjuksköterskorna skulle vilja ha större insikt i vad biståndsbedömarna har ansett om olika patienter för att på detta sätt kunna förbättra rutinerna kring behandlingen av dessa.

7. **Om Ni saknar viss information hur agerar Ni för att få tag på denna?**
Primärvården: För att få reda på information om sina patienter tar användarna kontakt med andra delar av hälso- och sjukvården (t.ex. sjukhuset) och begär att denna information skickas till vårdcentralen. Överföring av denna information sker muntligen via telefon, post men också genom fax. Om en viss patient har tillhört en annan vårdcentral ber användarna patienten att flytta sina journaler till den nya vårdcentralen. Information som finns på jourcentralen är tillgänglig för användarna genom att en läkare kan komma åt den.
Slutenvården: Generellt anser användarna att det inte saknas någon information. Ifall det skulle förekomma kan användarna få tag på denna m.h.a. t.ex. telefonen.

Hemvården: Ibland kan det uppstå problem med att få fram viss information. För att ta reda på denna ringer användare till andra användare inom hemvården eller andra delar inom hälso- och sjukvården. Informationen kan även skickas i pappersformat. Användarna använder sig även av böcker och Internet för att ta reda på information.

8. **Kan Ni ibland uppleva att viss information som Ni har tillgång till är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   Primärvården: Användare upplever inte att någon del av den information som finns tillgänglig är överflödig eller ej nödvändig. Däremot anser användarna att det finns information som inte används dagligen, men att denna hantering av information underlättar ifall den skulle behövas någon gång. På detta sätt klarar användare av olika situationer som kan uppstå. Användarna anser att även om informationen finns tillgänglig så innebär det inte att de läser denna.
   Slutenvården: Användarna upplever att det är svårt att avgöra om det finns för mycket information eller vilken information som skulle kunna klassas som överflödig. Även om användarna inte använder all information dagligen så anses det vara bra att ha tillgång till den information som finns i nuläget. Användarna upplever att det finns stora mängder av information tillgängligt. Denna tillgång kan ibland upplevas som nästan för mycket.
   Hemvården: Enligt användarna finns det mycket information som är tillgänglig för dessa, bl.a. information som rör andra förvaltningar, m.m. Generellt anser användarna att även om all information inte behövs dagligen så är det viktigt att ha tillgång till denna ifall den skulle behövas. Användarna tycker att den information som inte behövs ändå skall finnas tillgänglig för dessa. Varje användare skall själv avgöra om och när denne skall läsa denna information. Användarna anser också att de bilder som har skapats för varje användargrupp skall styra deras åtkomst till informationen.

9. **Hur anser Ni att en åtkomstkontrollmekanism skall fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   Primärvården: Användarna anser att den nuvarande åtkomstkontrollen uppfyller de krav som ställs på systemet från både verksamheten och lagstiftningen. Autentisering med personliga användar-id och lösenord ses som tillräckligt för att kontrollera att inga obehöriga kommer åt informationen. Även gruppindelning bland användare anses fungera i syfte att förhindra obehörig åtkomst till information.
   Slutenvården: Nuvarande åtkomstkontroll till information anses som tillräcklig. Användarna tycker inte att det skall finnas fri tillgång till all information utan att det skall finnas någon typ av begränsning. I de fall när det uppkommer störningar eller om det krävs behörighet till ytterligare någon information kan användare vända sig till IT-enheten och få den behörighet som krävs.
   Hemvården: Användarna upplever att den nuvarande behörighetskontrollen fungerar tillfredsställande. Det uppkommer

meningsskiljaktigheter bland användare när det gäller att ändra behörighetsgränser. Sjuksköterskor anser att det är viktigt med insyn till andras arbetsområden för att deras arbete skall bli ännu effektivare, medan biståndsbedömarna tycker inte att andra bör få insikt i deras uppgifter om patienter. Större tillgänglighet skulle innebära större risk att informationen hamnar i fel händer.

6 Analys av intervjuer

I detta kapitel analyseras de svar som har erhållits m.h.a. intervjuer i tre områden inom hälso- och sjukvården.

6.1 Åtkomst till information

Generellt får användarna i de undersökta delarna inom hälso- och sjukvården tillfredställande åtkomst till den information som behövs i deras arbete. För att kunna utföra sina arbetsuppgifter anser användare att det är nödvändigt att ha tillgång till stora mängder av information, både när det gäller patienter men även information som berör andra delar inom dessa organisationer. Ett vanligt argument som förekommer när det gäller åtkomst till informationen är att även om all information inte behövs dagligen så är det lämpligt att ha tillgång till denna ändå. Användarna anser att användarna själva får avgöra om viss information skall läsas av dessa. Inga användare anser att åtkomsten till information bör minskas eller göras strängare. Vissa upplever att åtkomsten är på gränsen till för stor, men att det är svårt att avgöra vilken information som skulle kunna tas bort.

Enligt de systemansvariga är användarna inom de undersökta delarna av hälso- och sjukvården medvetna om de lagar som finns när det gäller informationshantering inom hälso- och sjukvården. Användarna är även medvetna om att alla deras aktiviteter kan spåras m.h.a. loggningslistor. Just spårbarheten är ett viktigt instrument för systemansvariga när det gäller åtkomstkontrollen.

När det gäller systemen så fungerar dessa tillfredställande enligt användarna i de undersökta delarna av hälso- och sjukvården. Ibland uppkommer det vissa tekniska problem och det kan orsaka störningar i arbetet. Dessa störningar anses acceptabla. Generellt anser användarna att den erhållna informationen är rätt, alltså att användarna får den information som eftersöks av dessa och att åtkomsten sker vid rätt tidpunkt, alltså utan onödiga fördröjningar.

6.2 Behörighet

Det finns viss behörighetsindelning i de undersökta delarna inom hälso- och sjukvården. Denna indelning skiljer sig mellan dessa delar med undantag för åtkomsttilldelning av nätverksrättigheterna. Nätverksrättigheter tilldelas i de undersökta delarna av hälso- och sjukvården i samband med att användare erhåller sina användar-id och lösenord till systemet.

Inom primärvården bestämmer vårdcentralchefen på varje vårdcentral användarnas åtkomsträttigheter, därför kan dessa rättigheter variera från fall till fall. I vissa fall får användarna en större frihet att komma åt informationen, i andra tillämpas en strängare kontroll med större begränsningar. Det som styr vårdcentralschefens beslut när det gäller tilldelning av åtkomsten till information är tillit och tidigare erfarenheter av personalen. Det finns rollindelning inom primärvården, men rättigheterna inom dessa roller varierar mellan olika vårdcentraler.

Inom slutenvården ligger det övergripande ansvaret av behörighetstilldelning hos vårdchefen. Det finns sex huvudroller som gäller inom alla system, nämligen

läkare, sjuksköterska, undersköterska, sjukgymnast, administratör samt övrig personal. Dessa roller styr åtkomsten till informationen. Det förekommer klara brister i rutiner gällande avveckling av användare, dvs. när en användare slutar eller byter arbetsuppgifter. P.g.a. bristfällig kommunikation mellan personalavdelningen och IT-enheten kan dessa användare fortfarande äga sina gamla användar-id och lösenord och på så sätt komma åt information som inte längre skall vara tillgänglig för dessa.

Inom hemvården bestäms åtkomsträttigheter av en arbetsgrupp som granskar vilken information som är nödvändig för varje yrkesgrupp. Systemet inom hemvården arbetar med bilder där varje bild motsvarar en arbetsgrupp. Bilderna är generella och gäller i alla delar av organisationen, t.ex. har en sjuksköterska åtkomst till all information som motsvarar sjuksköterskans nivån på alla ställen inom organisationen. Dessa bilder kan jämföras med roller. Om en användare kommer åt information som ligger utanför dennes arbetsuppgifter skall detta rapporteras till systemansvarige. På detta sätt får systemansvarige reda på att användaren kom åt informationen av misstag.

I vissa system finns det klara brister när det gäller personliga inställningar för användarna. Enligt systemansvariga kan datorvana användare gå in och ändra vissa inställningar själva. På detta sätt har dessa användare en möjlighet att kunna läsa viss information som inte var avsedd för dessa användare från början.

Det som är gemensamt för primär-, sluten- och hemvården är att alla har en form av autentisering för sina användare. Varje användare måste uppge sitt användar-id och lösenord innan åtkomsten till informationen beviljas. Användarna uppmanas att byta ut sina lösenord efter viss tid. Detta tidsintervall varierar i de olika delarna av hälso- och sjukvården och ligger mellan 60 och 90 dagar. Användarna i de undersökta delarna upplever att denna form av autentisering är tillräcklig för att förhindra icke auktoriserade användare att komma åt informationen. Även systemansvariga i dessa områden anser att autentisering bidrar till en ökad kontroll av icke auktoriserad åtkomst till information. De undersökta områdena inom hälso- och sjukvården tillämpar loggningslistor som ett kontrollinstrument när det gäller åtkomst. Det finns dock inga klara regler för hur dessa listor skall kontrolleras och vad som är viktigt att kontrollera. Dessa kontroller sker slumpvis och görs av systemansvariga.

6.3 Informationsutbytet mellan de undersökta delarna

De tre undersökta delarna av hälso- och sjukvården använder distribuerade informationssystem. Informationens tillgänglighet för användarna sker via nätverk. Varje del har ett eget nätverk som inte är integrerat med de andra. Inom primärvården har varje vårdcentral eget lokalt nätverk. Informationsutbytet mellan primär-, sluten- och hemvården sker inte m.h.a. informationssystem utan med hjälp av telefon, fax eller via posten. Detta arbetssätt innebär viss fördröjning av informationen. Informationen är inte tillgänglig direkt när användarna behöver den, t.ex. om en sjuksköterska inom primärvården behöver någon information från slutenvården om en viss patient måste denna sjuksköterska ringa och begära denna information. Användarna i de olika delarna av hälso- och sjukvården anser att det finns ett behov av att utbyta informationen med varandra och att det borde effektiviseras.

7 Alternativa lösningar

I detta kapitel diskuteras m.h.a. litteraturstudie alternativa lösningar på de problem som enligt användarna och systemansvariga finns inom de tre undersökta organisationerna inom hälso- och sjukvården.

7.1 Kontroll av loggningslistor

Enligt intervjuer gjorda inom de tre delarna av hälso- och sjukvården så förekommer manuell hantering av loggningslistor. Loggningslistor kontrolleras oregelbundet och utan klara direktiv om vad som skall eftersökas.

Inom litteraturen finns ett antal olika verktyg som kan kontrollera loggningslistor och även bevaka att obehöriga inte kommer åt informationen som finns inom organisationen.

Det finns verktyg som arbetar i realtid d.v.s. undersöker systemet medan det används och indikerar eventuella obehöriga åtkomster direkt till administratören (t.ex. RealSecure). Dessa kan användas i både Unix- och Windowsmiljöer. Dessa verktyg består ofta av tre olika delar, nämligen nätverksbaserad mekanism, hostbaserad mekanism samt en modul för systemadministration (Allen et al., 2000).

Den nätverksbaserade mekanismen körs på alla arbetsstationer (datorer) inom ett distribuerat system och har som uppgift att kontrollera att ingen obehörig användare tar sig in i nätverket. Denna mekanism övervakar all trafik som sker inom ett nätverk eller delar av det. Om en obehörig användare upptäcks kan denna mekanism utföra olika åtgärder. En av dessa åtgärder kan vara att koppla ner förbindelsen för just denna användare, en annan åtgärd kan vara att skicka ett meddelande till systemadministratören. Olika åtgärder kan definieras vid installationen av detta verktyg (Allen et al., 2000).

Hostbaserad mekanism installeras på varje dator i ett nätverk och är ett komplement till den föregående mekanismen. Denna mekanism analyserar loggar genom att använda olika mönster och avvikelser från dessa samt känner igen obehöriga aktiviteter. När det förekommer en obehörig aktivitet kan denna mekanism stänga av användarens processer och blockera användarens konto. Den sänder även information till systemadministratören med upptäckta intrång.

Modulen för administration är ett gränssnitt där systemadministratör kan konfigurera de två ovanstående mekanismerna. Alla meddelanden som skickas från dessa mekanismer hamnar i denna modul. Denna modul lämpar sig för de flesta nätverkstyper och systemhanteringsmiljöer (Allen et al., 2000).

Enligt Allen et al. (2000) finns det verktyg som kan användas för att övervaka ett system när det gäller obehörig användning utifrån (t.ex. Computer Misuse Detection System). Detta verktyg stödjer kontroll av användarnas aktiviteter inom ett nätverk samt upptäcker intrång utifrån. Dessa verktyg kan generera analytiska rapporter över alla aktiviteter inom ett nätverk.

Dessa verktyg använder statistiska analyser för att kunna skapa beteendemönster som avviker från det fördefinierade och kan föra statistik om användarnas inloggningstider, vilka applikationer som användes, samt antalet filer som blev öppnade, ändrade eller borttagna.

Profiler av aktiviteter inom ett nätverk kan skapas. Dessa profiler undersöks med avseende på beteendeavvikelser jämfört med de fördefinierade profilerna. Om det förekommer avvikelser så rapporteras dessa till systemansvariga via varningssignaler (Allen et al., 2000).

7.2 Hantering av loggar hos andra organisationer

Posten Sverige AB använder sig av ett åtkomstutfärdarssystem som loggar olika händelser, sparar och kontrollerar dessa. Systemet loggar flera olika händelser, bl.a. skapande av konton för administratörer, initiering av transaktioner (t.ex. certifikatbegäran eller utlämning av certifikat), information om säkerhetskopiering, beställningsinformation, datum och tid för loggar, m.m. (Posten Sverige AB, 2003).

Loggar inom Posten Sverige AB undersöks minst en gång per vecka. Detta görs för att kunna upptäcka obehörigt intrång. Kontrollen görs dels manuellt och dels automatiskt. Vissa loggar kan kontrolleras m.h.a. systemet, medan andra måste kontrolleras av behörig personal. Alla loggar skyddas mot obehöriga ingrepp genom logiska mekanismer som finns i åtkomstutfärdarssystemet. En gång per månad verifieras och konsolideras loggarna av, till detta, bemyndigad personal. Varje logg förses med tidstämpel och säkerhetskopieras (två kopior). För att öka ytterligare säkerheten placeras dessa kopior i separata loggarkiv som är fysiskt placerade på olika ställen. Alla loggar sparas i 15 år (Posten Sverige AB, 2003).

Nordeas utfärdarsystem skapar loggar på olika händelser som uppkommer i systemet, bl.a. skapande av användarkonton, transaktioner (typ av transaktion, vem begärde transaktionen samt tidpunkt), referens till kortbeställning, kortnummer, certifikatnummer, m.m. Enligt Nordea granskas loggarna regelbundet. Även på Nordea tidstämplas alla loggar för att skydda dessa mot obehöriga förändringar. Det skapas två kopior på varje logg och varje kopia bevaras på åtskilda ställen. Loggar sparas för att kunna avläsas under sju år (Nordea, 2004).

Landstinget i Halland har ett vårdadministrativt system Swedestar. Detta system används vid Sjukhuset i Varberg. När det gäller detta system så finns det ingen automatisk kontroll av loggar. Kontrollen sker manuellt. Uppföljning sker genom att använda en utvald tidbok. För närvarande finns det cirka 70 olika tidböcker. Varje vecka skrivs det ut loggar på en utvald patient i en utvald tidbok. Endast dessa loggar kontrolleras. Urvalsmetoden vid utskrifter är den att en tidbok väljs ut, sedan plockas den tredje patienten i den aktuella tidboken ut och loggningsuppgifter skrivs ut (Aronsson och Jacobsson, 2004).

Landstinget i Halland kommer även att implementera ett patientadministartionssystem Elvis (PAS/Elvis) som även hanterar åtkomstkontroll och administrerar loggarna. Detta projekt skall genomföras vid Länssjukhuset i Halmstad. Till skillnad från det äldre PAS loggas i PAS/Elvis aktiviteter som utförs när det gäller en utvald patient. Loggar skapas för varje åtkomst till en viss patientinformation. På det sättet kan systemansvariga kontrollera vem som har kommit åt informationen om vissa patienter. Loggarna sparas centralt, i en databas. Endast systemadministratörer kan komma åt dessa loggar. Genom att PAS/Elvis fortfarande är under utveckling och även om detta system skall implementeras i verksamheten inom kort så finns det inga verktyg

sam kan användas för att kontrollera dessa loggar automatiskt (Aronsson och Jacobsson, 2004).

8 Diskussion

I detta kapitel förs en diskussion om arbetets resultat, om hur själva arbetsprocessen gick till samt kritisk granskning av arbetet. Här presenteras även arbetets bidrag. Slutligen ges flera olika förslag till framtida arbeten inom detta område.

8.1 Diskussion kring resultatet

I denna del diskuteras arbetets resultat. Först diskuteras resultatet framtaget m.h.a. intervjuer. Sedan diskuteras resultatet av litteraturstudier.

8.1.1 Åtkomstkontroll inom hälso- och sjukvården

Utifrån den gjorda undersökning kan konstateras att både användare och systemansvariga är nöjda med den åtkomstkontroll som finns i deras system idag. Detta kan bero på att systemen är relativt driftsäkra. System går inte ner så ofta utan användarna kan komma åt informationen vid behov. Det finns inte heller några problem med att komma åt all information användarna behöver tack vare den breda åtkomst som förekommer inom undersökta organisationer.

För att kunna ha en effektiv åtkomstkontroll i olika system inom hälso- och sjukvården måste det finnas klara policies och rutiner för denna. Under arbetets gång märktes att de olika organisationerna har vissa problem med åtkomstkontrollen p.g.a. bristande rutiner och policies. Inom primärvården finns grundläggande behörigheter, men innehållet i dessa behörigheter varierar mellan olika vårdcentraler. Vårdcentralchefen får godtyckligt tilldela åtkomst till informationen beroende på dennes erfarenheter av personalen. Inom hemvården finns vissa policies som bestäms av en arbetsgrupp inom varje kommun. Detta innebär att det kan finnas stora skillnader när det gäller åtkomstpolicies mellan olika kommuner. Inom slutenvården finns policies som bestämmer åtkomst till informationen, men det brister i andra rutiner, bl.a. när det gäller avskaffning av användarkonton.

För att förbättra åtkomstkontrollen inom hälso- och sjukvården bör varje organisation skapa klara regler och policies. Detta skulle göra det enklare för systemansvariga att tilldela åtkomst för användarna. En annan viktig fördel med utveckling av sådana policies är att det skulle underlätta att hantera processtänkandet inom hälso- och sjukvården. Klara policies inom organisationer skulle kunna innebära att en användare på en behörighetsnivå skulle ha likvärdig behörighet som en annan användare i en annan del av organisationen.

I dagens hälso- och sjukvård väljer organisationerna att tillämpa en bredare åtkomst till informationen för sina användare. Detta kan grundas i att organisationerna hanterar människoliv och inte vill riskera att göra fel p.g.a. bristande information.

De undersökta organisationerna inom hälso- och sjukvården lägger stor vikt vid spårbarheten. Dessa organisationer anser att det är viktigt att kunna spåra användarnas aktiviteter i systemet. Spårbarheten är en viktig egenskap när det gäller åtkomstkontroll, men för att kunna spåra användare på ett effektivt sätt måste det finnas klara rutiner för detta. Vissa av organisationerna använder sig av manuell kontroll av loggningslistor. Det finns inga bestämda tidsintervaller för

sådana kontroller och det är inte helt klart vilken information som skall undersökas. Inom slutenvården finns fortfarande pappersbaserade patientjournaler. Spårbarheten kan anses som obefintlig när det gäller dessa journaler. För att effektivisera arbetet med att spåra användarnas aktiviteter bör automatiska mekanismer anskaffas. Dessa mekanismer bör förses med klara regler för vilken information som skall letas efter samt hur ofta sökningar skall genomföras.

Slutenvården har 154 olika system fördelade på fyra sjukhus (bilaga 3a). Inom denna organisation arbetar ca 4700 anställda. Komplexiteten försvårar arbetet med att skapa en kraftfull åtkomstkontroll. Vissa av dessa system kan inte integreras med varandra och drivs på olika sätt. En fråga som kan ställas är om denna organisation behöver så många system. Om inte alla dessa system behövs, hur kan dessa system avvecklas utan att viktig information går förlorad?

Ett annat resultat i detta arbete påpekar att det inte finns någon interaktion av informationssystem mellan de olika organisationerna inom hälso- och sjukvården. I dagens läge, när patienterna vårdas på olika ställen, behövs ett sådant samarbete. Det är viktigt att tänka i processer vid patientvården. Processen börjar när en patient kommer in i systemet och avslutas när denna patient friskförklaras. Visserligen finns informationsutbyte mellan dessa organisationer, men detta sker via telefon, post eller fax. Datorisering av detta utbyte skulle innebära effektivisering av personalens arbete samt snabbare åtgärder vid behandling av patienter.

Hälso- och sjukvården bekostas med offentliga medel. Ekonomin är ansträngd, vilket gör den till en viktig faktor när det gäller utveckling av informationssystem och åtkomstkontrollen i dessa. Ledningen för de undersökta organisationerna måste dagligen ställa frågan om vad som skall prioriteras. Därför kan arbetet med att skapa effektivare åtkomstkontroll prioriteras lägre än t.ex. vård av patienter.

8.1.2 Alternativa metoder

Problem med att kontrollera inloggningslistor är inte unikt för hälso- och sjukvården. Även inom andra områden kontrolleras dessa listor manuellt och utan klara direktiv. En sådan organisation är Riksskatteverket. Där kontrolleras dessa listor på begäran från ansvarig chef. Det finns inga möjligheter att kontrollera samtliga loggar då antalet transaktioner är för stort (Riksrevisionsverket, 1999). Även inom hälso- och sjukvård i andra regioner förekommer det liknande problem som i det undersökta området. I Halland kontrolleras loggar manuellt efter ett förutbestämt urval (Aronsson och Jacobsson, 2004).

Flera andra organisationer försöker lösa problem med kontroll av loggar i sina system. Problemet är att i flera fall finns det mekanismer som möjliggör detta, men det saknas klara rutiner och policies för vad som skall undersökas. Komplexa organisationer hanterar stora mängder av transaktioner. Det finns ett stort antal användare och stora mängder av data som hanteras varje dag. Genom att kontrollera endast ett visst antal transaktioner kan dessa organisationer inte vara säkra på att obehörig åtkomst till data inte förekommer i deras system. Aronsson och Jacobsson (2004) påpekar att det är viktigt att ha klara regler och rutiner för vad som skall kontrolleras och hur. Att ta fram policies när det gäller kontroll av loggar är en arbetsam process. Det är viktigt att ta reda på vad systemen skall leta

efter, men det är även viktigt att skapa rutiner kring själva kontrollen, alltså med vilka tidsintervaller kontrollen skall utföras och hur.

När det gäller verktyg för att utföra kontroll av loggar så finns det ett antal av dessa på marknaden. En del av dem ingår i större åtkomstkontrollapplikationer, andra kan införskaffas separat och implementeras i organisationens befintliga system. Det finns två olika huvudtyper av mekanismer för kontroll av loggar, en som arbetar i realtid och en som kontrollerar loggarna med jämna intervaller. Organisationen måste ta ställning till vilken typ är mer lämplig i deras system. Realtidsmekanismer kräver större resurser genom att dessa arbetar hela tiden.

Generellt finns det ett flertal mekanismer som kontrollerar system mot intrång utifrån. Utifrån den lästa litteraturen kan konstateras att kontrollmekanismer är byggda mer för att skydda mot obehörig åtkomst utifrån än mot obehörigt inträde som kan ske inom organisationen.

För att utveckla värdefulla mekanismer för att kontrollera loggar kan datautvinningstekniker tänkas användas. Det gäller att hitta information som är viktig för att ge svar på om de uppställda åtkomstpolicies efterföljs. Denna kontroll kan jämföras med datalager (data warehouse) där det ställs frågor m.h.a. olika verktyg (t.ex. OLAP) för att få de svar som söks. Samma princip skulle kunna anpassas till kontroll av loggar. Verktygen skulle analysera loggar och utifrån dessa analysera m.h.a. policies som finns inom organisationen om någon obehörig åtkomst har skett, både av interna användare men också av personer eller applikationer utifrån.

8.2 Arbetets bidrag

Detta arbete berör åtkomstkontroll inom hälso- och sjukvården. Arbetets problemprecisering, som finns under kapitlet 3.1, fokuserar på två område. Dels på att kartlägga hur åtkomstkontroll fungerar inom hälso- och sjukvården, dels på att i litteraturen undersöka metoder och mekanismer som kan tillämpas för att kunna åtgärda de problem som finns inom hälso- och sjukvården utifrån den tidigare gjorda undersökningen.

Arbetet bidrar till en bättre förståelse för hur åtkomstkontrollen inom hälso- och sjukvården fungerar och ger en sammanställning på hantering av åtkomst till informationen inom tre olika delar av hälso- och sjukvården. Arbetet bidrar även med att diskutera alternativa mekanismer som kan bidra till att minska de problem som finns, när det gäller åtkomstkontroll, inom de undersökta områdena idag.

Tidigare arbeten inom problemområdet, exempelvis Åhlfeldt (2003), berör säkerheten inom hälso- och sjukvården i stort, där åtkomstkontrollen bara är en del av undersökningen. Andra arbeten riktar in sig på ett område inom hälso- och sjukvården, medan detta sammanställer tre olika områden. Många arbeten om åtkomstkontrollen har för avsikt att skapa generella modeller (Yao et al., 2001; Covington et al., 2001; Bertino, 2003), som kan användas inom olika områden. I detta arbete fokuseras det på att studera de typer som förekommer i hälso- och sjukvården.

Arbetet framhäver även olika mekanismer som kan användas för att åtgärda de problem som finns i de tre undersökta organisationerna när det gäller åtkomstkontroll. Utifrån litteraturstudien skapas en bild av hur kontroll av loggar,

som är ett problem enligt den gjorda undersökningen, fungerar i andra organisationer inom hälso- och sjukvården samt i andra branscher.

8.3 Diskussion kring arbetet

Arbetet påbörjades med att ta fram ett problemområde och problemprecisering. Första steget var att förstå problemområdet. För att göra detta användes litteraturen. Arbetet med att anskaffa litteraturen upplevdes som svårt. Det finns stora mängder av artiklar och böcker om säkerheten och åtkomstkontrollen, men det finns en begränsad mängd av litteratur som berör åtkomstkontrollen inom hälso- och sjukvården. Det som finns behandlar huvudsakligen hälso- och sjukvården i andra länder. Den svenska hälso- och sjukvårdsmodellen skiljer sig från andra, därför var det svårt att jämföra denna med hälso- och sjukvården i andra delar av världen.

Arbetet med att ordna fram intervjuer upplevdes som svårt. En av orsakerna till detta var svårigheten att få fram intresserade personer inom organisationerna. Det var besvärligt att få tag på personer i chefsställning, särskilt inom primärvården. Kontakter togs med olika vårdcentraler i Skövdeområdet både per telefon och personligen utan att dessa resulterade i intervjuer. Slutligen svarade en vårdcentral positivt. Ofta förekom brist på tid som huvudorsak till varför de övriga vårdcentraler inte kunde ställa upp på intervjuer. Intervjuer skedde på plats, svaren antecknades och renskrevs direkt efteråt. Efter att intervjuarna har blivit redigerade skickades dessa tillbaka via e-mail för validering. De intervjuade personerna var hjälpsamma och tillmötesgående. I början av vissa intervjuer kunde författaren uppleva en viss misstänksamhet mot detta arbete. En av dessa personer ville inte att dennes namn skulle förekomma i arbetet, detta var av personliga skäl.

Det förekom vissa svårigheter när det gäller anskaffning av vissa artiklar eftersom artiklarna varken fanns tillgängliga på Internet eller på biblioteket.

Generellt upplevdes arbetet som intressant och stimulerande. Hälso- och sjukvården är ett intressant område med komplexa informationssystem som kräver stark auktorisation och hög säkerhet när det gäller information.

8.3.1 Kritisk granskning av arbetet

Det gjordes endast nio intervjuer inom de tre organisationer. För att få en ännu mer rättvis bild av hur åtkomstkontrollen fungera och upplevs borde fler intervjuer göras, särskilt när det gäller användarna.

Alla intervjuer gjordes inom Skövdeområdet. Det innebär att de resultaten som arbetet har tagit fram gäller endast detta område. För att få en klarare bild av hur åtkomstkontrollen inom hälso- och sjukvården i Sverige fungerar generellt borde en mer omfattande undersökning göras, där flera andra regioner skulle ingå.

När det gäller litteraturstudier, hittades ett fåtal artiklar som beskrev hur kontroll av loggar fungerar bland andra hälso- och sjukvårdsorganisationer samt andra branscher. För att skapa en klarare bild av hur det fungerar i andra organisationer kunde en undersökning i form av intervjuer göras. Detta kunde inte genomföras p.g.a. arbetsbelastning hos dessa organisationer samt arbetets begränsade tidsresurser.

8.4 Förslag till framtida arbete

Ett förslag till framtida arbetet inom detta område är att undersöka hur olika organisationer inom hälso- och sjukvården tar fram sina policies när det gäller åtkomst till informationen. Primär-, sluten- och hemvården drivs av olika huvudmän varför det kan skilja mellan dessa delar av hälso- och sjukvården när det gäller framtagning av åtkomstpolicies.

Ett annat förslag till framtida arbete är att undersöka olika mekanismer som kan generera tillfällig åtkomst till informationen. Det finns rollbaserade mekanismer som möjliggör sådan åtkomst. Det arbetet kan innehålla undersökning om dessa mekanismer kan implementeras inom hälso- och sjukvården och på det sättet ”krympa” användarnas nuvarande åtkomst till informationen.

Ytterligare ett förslag till arbete är att undersöka om nivåbaserad åtkomstkontroll (Multilevel Access Control) kan användas inom hälso- och sjukvården och vilka konsekvenser av en sådan implementering skulle bli inom detta område.

Många olika organisationer använder åtkomstkontroll i sina system för att hantera användarnas åtkomlighet till information och applikationer. Ett förslag till framtida arbete är att undersöka och jämföra hur olika organisationer i olika branscher, t.ex. banker, polisen och militären, har löst åtkomstkontrollen och vilka problem som uppstår inom dessa organisationer när det gäller åtkomstkontroll.

Referenser

Allen, J., Christie, A., Fithen, W., McHugh, J., Pickel, J. och Stoner, E. (2000) *State of the practice of intrusion detection technologies*. Technical Report CMU/SEI-99-TR-028. Springfield: National Technical Information Service.

Aronsson, R. och Jacobsson, L. (2004) *Landstinget i Halland- Säkerhet och intern kontroll i vårdinformationssystem*. Tillgänglig på Internet: http://www.lthalland.se/dynamaster/file_archive/040526/85ff9364ba49da9b45a11c904366800a/V%C5RDINFOSYSTEM.pdf [Hämtad: 2004.07.13].

Barkley, J. (1997) Comparing simple Role Based Access Control models and Access Control Lists. *Proceedings of Third ACM Workshop on Role-Based Access Control*. New York: ACM Press.

Bellettini, C., Bertino, E. och Ferrari, E. (2001) Role Based Access Control Models. *Information Security Technical Report*, vol. 6, Nr.2, s. 21-29.

Berndtsson, M., Hansson, J., Olsson, B. och Lundell, B. (2002) *Planning and Implementing your Final Year Project with Success!* London: Springer-Verlag.

Berson, A. (1996) *Client/server architecture* (2:a upplaga). New York: McGraw-Hill.

Bertino, E. (2003) RBAC models- concepts and trends. *Computers & Security*, vol.22, s. 511- 514.

Beznosov, K. och Deng, Y. (2000) Engineering Access Control in Distributed Applications. I: S. K. Chang (red.), *Handbook of Sofware Engineering and Knowledge Engineering*, vol.1. World Scientific Publishing co., Inc.

Billum, S. (1997) *Sekretessprövning, handledning för personal inom vård och omsorg*. Stockholm: Nordstedts Juridik AB.

Bleumer, G. (1994) Security for Decentralized Health Information Systems. *International Journal of Bio-Medical Computing*, vol. 35, s. 139-145.

Burleson, D. K. (1994) *Managing Distributed Databases-building bridges between database islands*. New York: John Wiley & Sons, Inc

Connolly, T. och Begg, C. (2002) *Database Systems - A Practical Approach to Design, Implementation, and Management* (3:e upplaga). Essex: Pearson Education Limited.

Covington, M. J., Moyer, M. J. och Ahamad, M. (2001) Generalized Role-Based Access Control for securing future applications. *Proceedings of 23rd National Information Systems Security*, Baltimore.

Dawson, S., Qian, S. och Samarati, P. (2000) Providing security and interoperation of heterogeneous systems. *Distributed and Parallel Databases, vol.8*, s. 119-145. Norwell: Kluwer Academic Publishers.

Devargas, M. (1995) *The total quality management approach to IT security*. Cambridge, USA: Blackwell Publishers Inc.

Elmasri, R. och Navathe, S.B. (2000) *Fundamentals of Database Systems* (3:e upplaga). Reading, Massachusetts: Addison-Wesley Publishing Company.

Hutt, A. E., Bosworth, S. och Hoyt, D. B. (1995) *Computer Security Handbook* (3:e upplaga). New York: John Wiley & Sons, Inc.

Jakobsson, U., Parner, G., Hertin, U. och Eriksson, Y. (2002) *Analys av förutsättningar för en sammanhållen IS/IT- strategi för Stockholms läns landsting*. Tillgänglig på Internet: http://www.hsn.sll.se/hsnprotokoll/hsn/2002/2002-06-19/. [Hämtad : 2004.03.10].

Neumann, P. G. (1995) *Computer related risks*. Reading, Massachusetts: Addison- Wesley Publishing Company.

Nordea (2004) *Nordeas Policy & CPS för e-legitimation*, version 1.0. Tillgänglig på Internet: http://www.nordea.se/nordeacertifikat/resurs/medcert.pdf [Hämtad: 2004.07.05].

Lampson, B. W. (1993) Authentication in distributed systems. I: S.Mullender, *Distributed systems* (2:a upplaga, s. 543-553). Wokingham: ACM Press.

Patel, R. och Davidson, B. (1994) *Forskningsmetodikens grunder* (2:a upplaga). Lund: Studentlitteratur.

Pfleeger, C.P. (1997) *Security in computing* (2:a upplaga). New Jersey: Prentice-Hall International, Inc.

Poole, J., Barkley, J., Brady, K., Cincotta, A. och Salamon W. (1996) *Distributed Communication Methods and Role-Based Access Control for Use in Health Care Applications*. Tillgänglig på Internet: http://hissa.ncsl.nist.gov/rbac/poole/ir5820/nistir5820.htm [Hämtad: 2004.02.27].

Posten Sverige AB (2003) *Certifikatpolicy och CPS för Postens Elektroniska ID-handling på kort*, version 1.1. Tillgänglig på Internet: http://digitalid.postnet.se/pdf/CP-CPS-SMIME-ORG-v1.pdf [Hämtad: 2004.06.30].

Riksrevisionsverket (1999) *IT-säkerhet på Riksskatteverket*. Tillgänglig på Internet: http://www.riksrevisionen.se/templates/OpenDocument.aspx?documentid=3316 [Hämtad: 2004.07.06]

Rindfleisch, T. C. (1996) Privacy, confidentiality, information technology, and Health Care. *Proceedings of the Second Information Network for Health Officials Conference, Atlanta.*

Sadan, B. (2001) Patient data confidentiality and patient rights. *International Journal of Medical Informatics*, vol.62, s.41-49. Elsevier Science Ltd.

Samarati, P. och Jajodia, S. (1999) Data Security. *Wiley Encyclopedia of Electrical and Electronics Engineering*. Johan Wiley & Sons.

Sandhu, R. och Munawer, Q. (1998) How to do Discretionary Access Control using roles. *Proceedings of Third ACM Workshop on Role-based Access Control*. New York: ACM Press.

Sandhu, R. och Bhamidipati, V. (1999) Role-based administration of user-role assignment: The URA97 model and its Oracle implementation. *Journal of Computer Security*, vol.7, s.317-342. IOS Press.

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

Sjölenius, B. (1997) *Hälso- och sjukvård i kommunerna inför 2000-talet*. Falköping: Kommentus Förlag.

Smith, E. och Eloff, J.H.P (1998) Security in healthcare information systems - current trends. *International Journal of Medical Informatics*, vol.54, s.39-54.

Stegmann, C. (1997) *A framwork for authorisation policies*. Msc dissertation, Institut Eurécom, Sophia Antipolis, France.

Yao, W., Moody, K. och Bacon, J. (2001) A model of OASIS Role-Based Access Control and its support for active security. *Proceedings of Sixth ACM Symposium on Access Control Models and Technologies*. New York: ACM Press.

Yialelis, N., Lupu, E. och Sloman, M. (1996) Role-Based for Distributed Object Systems. *IEEE Fifth Workshop on Enabling Technology*. Washington: IEEE Computer Society.

Åhlfeldt, R-M. (2001) *Information Security in Home Healthcare - Personal Integrity and Secrecy*. Msc dissertation, Department of Computer Science, University of Skövde.

Åhlfeldt, R-M. (2003) *Analys av existerande system – säkerhet*, VITA Nova, rapport 4. Tillgänglig på Internet: http://www.carelink.se/files/doc_2004611104300.pdf [Hämtad: 2004.02.24].

Bilagor

Bilaga 1a – **Intervju med systemansvarige, primärvården**

Bilaga 1b – **Intervju med användare 1, primärvården**

Bilaga 1c – **Intervju med användare 2, primärvården**

Bilaga 2a – **Intervju med systemansvarige, slutenvården**

Bilaga 2b – **Intervju med användare 1, slutenvården**

Bilaga 2c – **Intervju med användare 2, slutenvården**

Bilaga 3a – **Intervju med systemansvarige, hemvården**

Bilaga 3b – **Intervju med användare 1, hemvården**

Bilaga 3c – **Intervju med användare 2, hemvården**

Bilaga 1a. **Intervju med systemansvarige, primärvården** 1 (2)

1. **Hur ser Era system ut med avseende på åtkomstkontroll? Hur fungerar åtkomstkontrollen?**
   – *Varje vårdcentral har ett eget nätverk, all information ligger på en server. Inom nätverket ligger olika program, t.ex. journalprogrammet Profdoc.*
   a. **Tillämpar Ni behörighetsmodellen eller får användare logga in sig och sedan har Ni möjlighet att kontrollera användarnas ”aktivitet” inom systemet?**
      – Olika användare har olika behörigheter för att komma åt informationen. Dessa användare kommer åt endast den information som tilldelas dem. Vi använder oss också av inloggningar som sparas och kan kontrolleras i efterhand.
   b. **Vilken autentisering använder ni i Era system? (ex. lösenord)**
      – Vi *använder oss av användarnamn och lösenord. Varje användare får ett eget användarnamn och lösenord när han eller hon anställs, sedan så uppmanas de att byta lösenord var 90:e dag.*
2. **Vilka för- resp. nackdelar har denna hantering av åtkomstkontroll?**
   – *Jag tycker att det fungerar bra. Det finns loggar så att man kan kontrollera vem som har tittat på vad. Även själva patienterna kan kontrollera vem som har varit och tittat i deras journaler. En nackdel kan vara att man inte kan spärra delar i en modul utan kan endast jobba med hela moduler.*
   c. **Anser Ni att det finns andra metoder/sätt som kan vara mer lämpliga att använda?**
      - *Jag tycker att den nuvarande fungerar bra.*
3. **Vilka policies eller regler använder Ni er av för att säkerställa att en viss användare skall ha tillgång till en viss data?**
   a. **Hur vet Ni vilken data som en viss användare skall ha tillgång till?**
      – Vårdcentralchefen bestämmer vilken information som skall vara tillgänglig för varje användare eller användargrupp, exempelvis så har användarna på vårdcentralen i Hjo tillgång till all information, förutom information som kuratorn och psykologen har skrivit. Läkare och sjuksköterskor har samma tillgång till informationen, rättigheterna kan däremot regleras, t.ex. en sjuksköterska kan inte skriva i vissa delar av systemet, men det kan en läkare. Vårdcentralchefens beslut baseras på arbetsuppgifter men också på förtroendet.
   b. **Vilken typ av information får Ni om användaren för att säkerhetställa att just han/hon skall ha tillgång till en viss data?**
      – Vi får information från vårdcentralchefen om vad som skall vara tillgängligt för varje användare eller användargrupp.
4. **Vad har Ni för procedur när Ni tilldelar en användare åtkomst till viss data?**
   a. **Hur går Ni till väga rent praktiskt? Berätta steg för steg.**

Bilaga 1a. **Intervju med systemansvarige, primärvården** 2 (2)

– Vi tilldelar åtkomst genom att använda oss av mallar som finns tillgängliga. När det gäller nätverksrättigheter så anmäls varje ny användare centralt till IT-enheten.

   b. **Anser Ni att denna procedur är tillfredsställande och om inte hur skulle Ni vilja utveckla den?**
   – **Nej**, *jag tycker att det fungerar bra som det är. Vi har vissa mallar som vi följer.*

5. **Finns det någon rollindelning bland användare och i så fall vilka kriterier som styr denna uppdelning?**
   – Ja, det finns en viss rollindelning. Denna indelning beror på vilken yrkesgrupp en användare tillhör, men också vilken åtkomst till information skall en användare ha enligt vårdcentralchefen.
6. **Anser Ni att det, i vissa fall, finns risk att användare kan behöva information, som de i vanliga fall inte har åtkomst till? Om ja, hur kan de få tag på den?**
   - Det är nog olika från fall till fall, t.ex. i Hjo behöver de inte mer information genom att de har åtkomst till nästan allt, men på andra vårdcentraler kan vårdcentralchefen be systemadministratören att lämna ut ytterliggare vissa rättigheter till olika användare.
7. **Anser Ni att det kan finnas risk, generellt, för att användare får tillgång till mer information än de behöver för att utföra sitt arbete? (till exempel sådan information som inte berör behandling av en viss patient).**
   – Visst finns det risk att personal kommer åt ”fel” information, men man kan kontrollera detta m h a loggningslistor. Där finns det även tider för hur länge en användare har kollat på något. Av dessa tider kan man dra slutsatser om användare har varit där av misstag eller inte. Personalen är välmedveten om att de kan spåras.

   a. **Hur anser Ni att sådana risker kan reduceras?**
   - loggningslistor är ett bra hjälpmedel.

8. **Hur anser Ni, att åtkomstkontroll skall se ut för att den skall uppfylla krav ställda från verksamheten, lagar samt användarkrav? Berätta hur en optimal åtkomstkontroll skall se ut enligt Er.**
   – Den nuvarande åtkomstkontrollen fungerar bra, enligt mig. Det som kunde ha varit bättre är att man kunde spärra information mer på modulnivå, alltså att man kunde spärra delar av en modul och inte behöva spärra hela modulen. En annan sak som kunde förbättras är att vissa s.k. ”personliga inställningar” borde flyttas över till journalsystemets underhållsdel och regleras av systemadministratören för att få ännu bättre säkerhet.

Bilaga 1b. **Intervju med användare 1, primärvården** 1 (2)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – Vi har gemensamt nätverk, som vi måste logga in oss på. För att göra det använder vi oss av användarnamn samt lösenord, lösenord byts med jämna mellanrum. Jag skriver in mitt användarnamn och lösenord, sedan är jag inne på nätverket, detsamma gäller de olika program som jag arbetar i, t.ex. patientjournalsystemet, osv.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   – Tillgång till diverse information fungerar bra, utan några som helst problem. Åtkomsten sker på ett snabbt sätt. Man kan komma inte bara åt det som berör själva patienter, men kan även komma åt senaste information inom sjukvården, som är upplagt på Västergötlandsregionens hemsidor. Det gör att man kan ta del av nya trender, metoder, m.m.
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   – För att kunna utföra våra arbetsuppgifter måste vi få tag på, framförallt informationen om patienter, alltså patientjournaler. Anna, viktig information som vi måste ha är alla provsvar, information om olika mediciner och även tidsbokning.
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   – Jag tycker att vi får rätt information, på snabbt och effektivt sätt. Om vi söker efter något specifikt så hittar vi detta omgående, det är inga problem. Det viktigaste är att lära sig systemet, kan man det så är det inga som helst problem.

   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**

   -
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   – Ja, jag tycker åtkomsten till informationen är tillräcklig och uppfyller de krav som vi har samt även kravställda utifrån lagstiftningen. Det mesta inom sjukvården är sekretessbelagt, alla som jobba vet om det och följer detta. Vi kommer åt all information vi behöver, så att nuvarande åtkomst till information uppfyller även våra krav.
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – Den information som vi saknar är information som finns på andra ställen än hos oss. Vi skulle behöva ibland komma åt information om våra patienter som finns lagrad på Kärnsjukhuset. Om patienten har varit på andra vårdcentraler så har vi inte heller tillgång till denna information. Det skulle behövas lite mer samarbete mellan olika parter för att man skulle få tillgång till deras information om patienter.

Bilaga 1b. **Intervju med användare 1, primärvården** 2 (2)

7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**
   – *Om vi behöver någon information om en utav våra patienter från KSS ringer vi eller meddelar de på ett annat sätt att de skall skicka den till oss. Om en patient har tidigare varit hos en annan läkare, ber vi patienten att hans gamla läkare skickar över information via post eller fax. Fax är mindre lämpligt, för att man kan skicka informationen till fel nummer.*
8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – *Nej, jag ser ingen information som är överflödig eller inte nödvändig. Visst finns det information som vi inte använder dagligen, men den kan behövas någon gång och då är det bra att ha tillgång till den. Man vet aldrig vilken information man kan behöva i olika lägen, därför är det viktigt att ha så mycket information som möjligt. Det underlättar att kunna klara av olika situationer på ett bra sätt.*
9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   - *Jag anser att det nuvarande systemet fungerar bra. Vi har våra lösenord, så att ingen annan kommer åt informationen. Det syns var vi har varit och tittat, detta kan kontrolleras efteråt. Det finns viss gruppindelning så att läkare kan komma åt all information, även information som finns på Jourcentralen, läkarsekreterare kan skriva i alla patientjournaler men inte signera dess och vi sjuksköterskor kan skriva i alla journaler men signera bara våra egna. Jag anser att detta system fungerar bra.*

Bilaga 1c. **Intervju med användare 2, primärvården** 1 (2)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – Vi har användarnamn och lösenord för att komma åt informationen. Lösenord får vi byta ut med jämna mellanrum. För att komma åt diverse information så måste jag logga in mig på det lokala nätverket, sedan måste man även logga in sig på i de övriga programmen.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   - *Åtkomst till information fungerar väldigt bra. Systemet är lätt att jobba med, det är endast den mänskliga faktor som kan strula, t. ex. bortglömda lösenord till program som används mindre ofta. Genom att det finns olika behörighetsroller så kommer man inte åt all information, bara den man behöver.*
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   – *För min del så behöver jag åtkomst till patientjournaler och den information som finns om patienter. Dokument som kommer utifrån skannas och läggs in i patientjournaler, man ser även om en viss patient har någon annan läkare. Man kan se om patienten är listad hos oss eller inte, man ser dock inte på vilken annan vårdcentral han/hon är listad.*
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   – *Jag tycker att jag får all den information jag behöver. Genom att systemet fungerar bra så får man snabba svar ifrån det. Behöver man åtkomst till något annat får man ta kontakt med IT-avdelningen och om något strular så ringer man supporten. Vi har väldigt få driftsstörningar. Vi får också reda på om något har ändrats på våra informationsträffar och via mail och telefon.*
   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**
      -
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   – *Ja, jag får tillgång till all den information jag behöver. När det gäller säkerheten så har vi användarnamn och lösenord och det är bra. Det enda risk som kan uppstå är att man går ifrån dator utan att logga av, då kan en annan komma åt informationen som tillhör mitt konto. Vi använder et kortkommando för utloggning som kräver lösenord för nyinloggning.*
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – *Jag har tillgång till allt jag behöver i mitt arbete. Behöver vi någon information från t.ex. Kärnsjukhuset, så ber vi dem skicka den till oss. Läkare har även tillgång till jourcentralens information.*
7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**

Bilaga 1c. **Intervju med användare 2, primärvården** 2 (2)

– Jag känner att, i vissa fall, skulle jag behöva information från jourcentralen. Information från KSS får vi in med hjälp av telefon eller posten. Om vi får in en ny patient, ber vi honom eller henne att flytta sina journaler från den gamla centralen i till oss.

8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – *Man behöver inte alltid all information som man har tillgång till, man tittar bara på det som man behöver och väljer själv det man vill läsa. Men ibland kan vi behöva just specifik information och då är det bra att ha tillgång till denna.*
9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   – *Jag tycker att den nuvarande kontrollen fungerar bra och tycker att det skall finnas personliga inloggningar till nätverket och inte generella.*

Bilaga 2a. **Intervju med systemansvarige, slutenvården** 1 (3)

1. **Hur ser Era system ut med avseende på åtkomstkontroll? Hur fungerar åtkomstkontrollen?**
    a. **Tillämpar Ni behörighetsmodellen eller får användare logga in sig och sedan har Ni möjlighet att kontrollera användarnas ”aktiviteter” inom systemet?**
    – Vi använder en form av behörighetsmodellen. Rollindelningen sker för varje system lokalt. IT-samordnarna tilldelar nya användare de roller som motsvarar deras arbetsuppgifter. Idag har vi 154 olika system inom slutenvården i vår region. Dessa system är fördelade på 4 sjukhus samt 4700 anställda och fungerar inom både sluten- och öppenvården.
    b. **Vilken autentisering använder ni i Era system? (ex. lösenord)**
    – Vi har personliga användar-id samt lösenord som uppmanas att bytas var 60:e dag. Lösenord består av fem tecken, utan några som helst föreskrifter när det gäller användning av siffror och bokstäver.
2. **Vilka för- resp. nackdelar har denna hantering av åtkomstkontrollen?**
    – Autentisering är grundläggande för att identifiera varje användare inom systemet, det måste vi ha för att säkerställa användarnas identiteter. Via dessa erhåller användarna åtkomst till viss mängd av information. En nackdel är att våra avvecklingsrutiner inte fungerar tillräckligt bra. Det är svårt att få reda på om användarna har slutat eller förflyttats.
    a. **Anser Ni att det finns andra metoder/sätt som kan vara mer lämpliga att använda?**
    – Automatiska system (som ger signal via personalsystem till behörighetssystem) skulle förbättra situationen, men detta innebär att statusen på personalsystemen alltid måste vara aktuella vilket i sin tur kan vara problematiskt, med tanke eftersläppning i informationen
3. **Vilka policies eller regler använder Ni er av för att säkerställa att en viss användare skall ha tillgång till en viss data?**
    a. **Hur vet Ni vilken data som en viss användare skall ha tillgång till?**
    – Vårdchefen bestämmer vilka system som en viss användare får ha åtkomst till. Detta regleras inte på datanivån utan på systemnivån.
    b. **Vilken typ av information får Ni om användaren för att säkerhetställa att just han/hon skall ha tillgång till en viss data?**
    – Vi får den anställdes personuppgifter samt uppgifter om vilken information han eller hon skall ha tillgång till.
4. **Vad har Ni för procedur när Ni tilldelar en användare åtkomst till viss data?**

Bilaga 2a. **Intervju med systemansvarige, slutenvården** 2 (3)

   a. **Hur går Ni till väga rent praktiskt? Berätta steg för steg.**
   – När en person anställs skickar dennes närmaste chef eller IT-samordnare ett underlag på vilka system som skall vara tillgängliga för denna person. Användaren tilldelas en användar-id samt lösenord, som denne får byta vid senare tillfälle. Sedan tilldelas användaren rättigeter till de system som denna skall ha tillgång till.
   b. **Anser Ni att denna procedur är tillfredsställande och om inte hur skulle Ni vilja utveckla den?**
   – Rutinen vid början av en anställning är tillfredställande eftersom en anställd/chef alltid reagerar om inloggning inte finns.

5. **Finns det någon rollindelning bland användare och i så fall vilka kriterier som styr denna uppdelning?**
   – Det finns rollfördelning inom våra system. Vi har sex olika roller som vi kan tilldela en användare. Dessa roller är: läkare, sjuksköterska, undersköterska, administratör, sjukgymnast samt övrig personal. Det som styr denna indelning är de arbetsuppgifter eller yrkesroller som varje användare har.
6. **Anser Ni att det, i vissa fall, finns risk att användare kan behöva information, som de i vanliga fall inte har åtkomst till? Om ja, hur kan de få tag på den?**
   - Både ja och nej. Visst kan det uppkomma tillfälle när en användare kan behöva information som ligger utanför dennes behörighet, men det händer nog sällan. Genom att användarna får behörigheter på systemnivån så få de automatiskt åtkomst till den information som ligger där. Därför, generellt sett, får de tillgång till all den informationen för att kunna utföra sina arbetsuppgifter. Sedan kan det finnas tillfälle där användarna behöver informationen utifrån, t.ex. från en vårdcentral. Då kan det uppstå problem för, i dagen läge, har vi inga integrerade system med primärvården. Denna form av informationsinhämtning får ske på konventionella sätt.
7. **Anser Ni att det kan finnas risk, generellt, för att användare får tillgång till mer information än de behöver för att utföra sitt arbete? (till exempel sådan information som inte berör behandling av en viss patient).**
   – Genom att användarna får åtkomst på system- och inte på datanivån kan det uppkomma tillfällen där de får tillgång till mer information än de behöver för att kunna utföra sina arbetsuppgifter. Vi i slutenvården/öppenvård har fortfarande patientjournaler i pappersformat. Det är också en viktig del i åtkomsten till information. Skall man hårdra detta så kan vem som helst kunna läsa en patientjournal utan att vi kan kontrollera detta. Just nu håller vi på med ett projekt som har som mål att införa digitala datajournaler, så förhoppningsvis skall vi kunna förbättra åtkomstkontrollen inom detta område.
   a. **Hur anser Ni att sådana risker kan reduceras?**

Bilaga 2a. **Intervju med systemansvarige, slutenvården** 3 (3)

8. **Hur, anser Ni, att åtkomstkontroll skall se ut för att den skall uppfylla krav ställda från verksamheten, lagar samt användarkrav? Berätta hur en optimal åtkomstkontroll skall se ut enligt Er.**
   – *Det optimala vore en åtkomstmatris med följande parametrar: Roll, grupp, läs/skriv, dataterm. Detta innebär att, för att underlätta administration inte får vara en större mängd undantag, kan möjligtvis vara något rigid***.** *Problemet är att i gamla system går detta inte att implementera,*

Bilaga 2b. **Intervju med användare 1, slutenvården** 1 (2)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – Vi har intranät som heter Fokus. För att komma åt komma in i systemet måste jag logga in mig. Först loggar jag in mig på min personliga sida, sedan kan jag även logga in mig på olika program som finns tillgängliga.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   – För min del så får jag den information jag behöver för att utföra mina arbetsuppgifter. Själva systemet fungerar bra för det mesta. Det kan uppkomma fel eller avbrott, men det gör med de flesta system. Sedan vi har fått nya datorer så går det hyfsat snabbt också.
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   - Jag behöver information om personalen för bl.a. schemaplanering och diverse annat. Annars så behöver man svar från laboratorium, information om beläggningen för att kunna lägga in nya patienter. Vi har inga patientjournaler inlagda i systemet, dessa är fortfarande i pappersformat. Övrig information som är tillgänglig är den via mail och PM.
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   – Ja, det är inga problem. Jag får information som jag behöver för att utföra mina arbetsuppgifter utan några större problem.
   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**
      -
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   – Ja, det tycker jag. Genom personliga koder kan man komma åt den information man är behörig till. Vi är även medvetna om sekretessen.
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – Nej, jag tycker att jag får tillgång till den information jag behöver. Det är inga problem med att jag inte åt någon information som krävs för att utföra mitt jobb. Visst händer det att man saknar något ibland, men det går alltid att få tag på detta på ett eller annat sätt.
7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**
   – Om jag saknar någon information så använder jag telefonen för att få reda på denna.
8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – Svårt att säga, man får väldigt mycket information genom systemet så det är svårt att avgöra. Men visst all information är kanske inte nödvändig, men åt andra sidan är det svårt att urskilja vilken som behövs och vilken inte.

Bilaga 2b. **Intervju med användare 1, slutenvården** 2 (2)

9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   – *Jag vet inte riktigt, jag har de behörigheter jag behöver. Om man saknar något så kan man alltid be den som sköter om datorsystemet att IT-avdelning fixar det.*

Bilaga 2c. **Intervju med användare 2, slutenvården** 1 (1)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – Vi har ett intranät, som heter Fokus. För att komma in på det så måste man använda sitt användarnamn och lösenord. Sedan har vi olika program som man måste logga in sig på för att kunna använda dessa.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   – Det fungerar bra, inga problem. Visst kan det uppkomma vissa störningar ibland, men det är inga problem.
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   – Den information som behövs här är information om personalen, schemaläggning, aktuella händelser. Även informationen om blodgruppering och patientbeläggning är viktig. Vidare så behöver vi informationen från apoteket när vi skall beställa läkemedel, mail, osv.
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   – Ja, det tycker jag. Ibland kan det uppkomma problem, men dessa beror oftast på den tekniska biten.
   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**
      -
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   - *Ja, jag får all den information jag behöver för att kunna göra mitt jobb.*
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – Det finns inga problem alls. Jag har de behörigheter jag behöver och kommer åt den information som krävs för att jag skall kunna göra det jag skall.
7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**
   - *Jag saknar ingen information, men om det skulle hända så är det bara att lyfta på luren och ringa så löser man detta.*
8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – Snubblande nära. Egentligen så får jag inte för mycket information, men det är på gränsen. Man kan behöva viss information vid en viss tidpunkt, men ibland kan det kännas att man skulle klara sig utan en hel del. Det är svårt att avgöra.
9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   – Det fungerar bra som det är idag. Man skall inte ha en naturlig åtkomst åt all information. Det krävs att man begränsar tillgången till information, därför är den nuvarande åtkomstkontroll bra.

Bilaga 3a. **Intervju med systemansvarige, hemvården** 1 (3)

1. **Hur ser Era system ut med avseende på åtkomstkontroll? Hur fungerar åtkomstkontrollen?**
   – Vi har ett system som heter MagnaCura. Det är flera olika yrkeskategorier inom omvårdnadsförvaltningen som använder sig av detta system, bl.a. biståndsbedömare, sjuksköterskor, arbetsterapeuter, sjukgymnaster, ekonomer, enhetschefer, m.fl. Genom att använda systemet har vi god kontroll på vilka som skall ha åtkomst till vilken data.
   a. **Tillämpar Ni behörighetsmodellen eller får användare logga in sig och sedan har Ni möjlighet att kontrollera användarnas ”aktivitet” inom systemet?**
      – Systemet arbetar med bilder, varje yrkesgrupp har vissa bilder som de får tillgång till, eller som de är behöriga till. Utanför de tilldelade bilderna har användare ingen åtkomst. Sedan finns det olika rättigheter som tilldelas varje användare, t.ex. läsa, skriva eller radera. Om an användare har t.ex. skrivrättigheter till en viss bild, betyder det inte att han eller hon har även raderingsrättigher till samma bild.
   b. **Vilken autentisering använder ni i Era system? (ex. lösenord)**
      – Varje användare har ett användar-id och lösenord, som bytts med jämna mellanrum. Varje gång användare skall komma in i systemet får de logga in sig.
2. **Vilka för- resp. nackdelar har denna hantering av åtkomstkontroll?**
   – Den största fördelen är att man tilldelar användarna bilder till vilka de har åtkomst till. På det sättet har man koll på vilka delar av systemet som skall användas av vissa användare. En annan fördel är att all åtkomst hanteras på samma sätt inom hela verksamheten genom att man använder detta system. Ytterligare en fördel är att man även kan spåra användarnas aktiviteter inom varje bild, som de har tillgång till. En nackdel är att vissa funktioner inte fungerar fullt ut, men dataföretaget har lovat att åtgärda detta.
   a. **Anser Ni att det finns andra metoder/sätt som kan vara mer lämpliga att använda?**
      – Jag anser att system som vi använder fungerar tillfredställande för vår verksamhet och vi är nöjda med detta system.
3. **Vilka policies eller regler använder Ni er av för att säkerställa att en viss användare skall ha tillgång till en viss data?**
   – Jag vet vilka som skall ha tillgång till vilken data och det är jag som sätter upp rättigheter och tilldelar användarna bilder. Sedan har vi en arbetsgrupp som diskuterar vilka regler som skall gälla vid åtkomst till data. En viktig punkt är också de lagar som finns när det gäller att skydda information och individen.
   a. **Hur vet Ni vilken data som en viss användare skall ha tillgång till?**
      – Jag får information om vilka arbetsuppgifter vederbörande skall ha inom verksamheten. På så vis kan jag tilldela henne eller honom de bilder som behövs för att utföra dessa uppgifter. Det finns även en gruppindelning man kan göra beroende på just arbetsuppgifter, t.ex.sjuksköterskor.

Bilaga 3a. **Intervju med systemansvarige, hemvården** 2 (3)

   b. **Vilken typ av information får Ni om användaren för att säkerhetställa att just han/hon skall ha tillgång till en viss data?**
   – Varje enhetschef som har anställt en ny medarbetare meddelar mig detta. Jag får uppgifter om denne person, t.ex. namn, personnummer samt vilka arbetsuppgifter som denna person skall utföra.

4. **Vad har Ni för procedur när Ni tilldelar en användare åtkomst till viss data?**
   a. **Hur går Ni till väga rent praktiskt? Berätta steg för steg.**
   – Varje ny användare registreras i systemet utifrån de uppgifter som jag har fått av enhetscheferna. Användare tilldelas ett användar-id samt en lösenord, dessa uppgifter meddelas användare. När denne har fått dessa uppgifter kan hon eller han börja använda systemet i sitt arbete. Användaren uppmanas att byta lösenord med jämna mellanrum.
   b. **Anser Ni att denna procedur är tillfredsställande och om inte hur skulle Ni vilja utveckla den?**
   – Denna procedur fungerar bra, jag lägger in en ny användare after att samråd med enhetschef som har anställt denne användare. Jag kopplar användare till bilder som denne behöver för att utföra sina arbetsuppgifter. Byte av lösenord medför också en ökat säkerhet.
5. **Finns det någon rollindelning bland användare och i så fall vilka kriterier som styr denna uppdelning?**
   – Det finns en indelning, där man delar in användare i olika grupper inom verksamheten. Man kan även säga att vi har rollindelning beroende på arbetsuppgifter. Det som styr denna indelning är arbetsuppgifter som användarna i en viss yrkesgrupp skall utföra.
6. **Anser Ni att det, i vissa fall, finns risk att användare kan behöva information, som de i vanliga fall inte har åtkomst till? Om ja, hur kan de få tag på den?**
   – Än så länge har det inte förekommit att an användare skulle behöva information som de inte har åtkomst till, de har åtkomst till all information som de kan tänkas behöva. Om sådan situation skulle uppstå så skulle vi nog ta en diskussion i arbetsgruppen hur vi skall hantera detta och eventuellt gå vidare till ledningsgruppen med denna fråga.

Bilaga 3a. **Intervju med systemansvarige, hemvården** 3 (3)

7. **Anser Ni att det kan finnas risk, generellt, för att användare får tillgång till mer information än de behöver för att utföra sitt arbete? (till exempel sådan information som inte berör behandling av en viss patient).**
   – *Användarna har tillgång till information i alla distrikt. Detta beror på att under helgerna får de arbeta på olika ställen. Jag tycker inte att användarna har tillgång till för mycket information hos oss. De kan komma åt den information som de behöver. Jag anser inte att man kan ytterligare begränsa åtkomst för att även om viss information inte används just då så kan den behövas vid något tillfälle och då finns den redan tillgänglig för användaren.*
   a. **Hur anser Ni att sådana risker kan reduceras?**
      – Jag anser att det inte finns sådana risker för information som finns tillgänglig för varje användare i vår verksamhet är behövd av dessa användare. Det finns ingen onödig eller överflödig information.
8. **Hur, anser Ni, att åtkomstkontroll skall se ut för att den skall uppfylla krav ställda från verksamheten, lagar samt användarkrav? Berätta hur en optimal åtkomstkontroll skall se ut enligt Er.**
   – *System som används i vår verksamhet passar oss alldeles utmärkt. Vi har ett gemensamt gränssnitt, som ser ut på precis samma sätt för hela verksamheten. Men de olika delar i verksamheten hålls separat och regleras med olika lagar, t.ex. socialtjänsten är separerad från biståndfunktionen och vårdfunktionen. Det som man skulle kunna utveckla är att man hade lite större insikt till andra funktioner. En önska är att, t.ex. en sjuksköterska skall kunna se antal lagda timmar hos bistånd, osv. Med andra ord det skulle behövas lite mer iteration mellan olika funktioner.*

Bilaga 3b. **Intervju med användare 1, hemvården** 1 (2)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – För att komma in i systemet så måste jag logga in mig med mitt användarnamn och lösenord. Även för att kunna använda vissa program krävs det separat inloggning. Vi har personliga koder till detta. Vi uppmanas att byta dessa koder efter 60 dagar. Genom att man använder olika datorer så är det viktigt att ha personlig användarnamn och lösenord.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   – Åtkomsten fungerar bra. Det finns inga svårigheter att nå den information man söker, men man måste veta var man skall söka. Själva systemet har vissa brister, men de är acceptabla.
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   – Jag behöver information om lagförändringar, sekretesslagen, vad politiker anser om vissa saker, tidigare information om berörda personer. Med andra ord det är ett brett område som jag håller reda på, därför behöver jag information som rör flera olika saker.
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   - Generellt får jag rätt information vid rätt tidpunkt.
   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**
      – Ibland kan det vara problem att få all information. Allt går inte lösa med hjälp av en dator.
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   – Jag skulle vilja ha mer åtkomst till viss information som vi i dagens läge inte har åtkomst till. Annars tycker jag att den nuvarande är tillräckligt.
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – Som jag har sagt tidigare så skulle jag även behöva tillgång till annan information än den jag har tillgång till idag. Ett sådant exempel är gamla domar, som rör mitt arbetsområde. Idag måste jag gå via kommunen för att få fram denna information. Kommunen bestämmer själva vilka utdrag ur domar de skall ta hem. Sådan process är tidskrävande
7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**
   – För att få tag på den information jag söker måste jag ringa dem som har denna information eller som kan ta fram den. Annars så söker jag mycket på Internet och i böcker och tidsskrift.

Bilaga 3b. **Intervju med användare 1, hemvården** 2 (2)

8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – *Självklart så har vi tillgång till mycket information, bl.a. andra förvaltningar, osv. Vi använder inte all information jämnt, men den är bra att ha när vi skulle behöva den. Vi behöver inte läsa den information vi inte behöver för våra arbetsuppgifter, men det är bra att den finns där ifall vi skulle behöva den.*
9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   – *Behörighetskontrollen fungerar bra idag. Det finns förslag att andra, t.ex. sjuksköterskor, skall gå in och läsa visa delar i våra system men jag tycker inte att man skall släppa ut för mycket information. Det kan vara känsligt.*

Bilaga 3c. **Intervju med användare 2, hemvården** 1 (2)

1. **Vad måste Ni göra för att kunna komma åt information som finns lagrad inom systemet? Berätta, steg för steg, hur Ni gör.**
   – För att komma åt systemet måste jag logga in mig. Jag har en personlig användar-id och ett lösenord. Jag uppmanas att byta lösenord med jämna mellanrum.
2. **Hur upplever Ni att åtkomst till information fungerar utifrån Era arbetsuppgifter?**
   – Jag tycker att åtkomsten till information fungerar bra. Man kommer åt den information man behöver för att kunna göra mitt jobb. Genom att man kan jobba på flera olika ställen har vi åtkomst till lite olika information beroende på vilka ställen vi jobbar på. Det tycker jag är bra, för på det sättet är informationen tillgänglig oavsett vilket område vi jobbar på.
3. **Vilken typ av information behöver Ni för att kunna utföra Era arbetsuppgifter?**
   – Jag behöver informationen om våra patienter, om de läkemedel som finns tillgängliga samt informationen om vad som har hänt inom verksamheten, t.ex. nya rutiner eller liknande.
4. **Får Ni rätt information vid rätt tidpunkt, så att Ni kan utföra Era arbetsuppgifter så effektivt som möjligt?**
   – Jag tycker att jag får den information jag behöver. Systemet fungerar bra så jag får tag på denna information snabbt och smidigt. Information som jag har tillgång till är uppdaterad. Ibland kan det uppkomma tekniska fel och då blir tillgången begränsad, men det händer inta ofta.
   a. **Om Ni inte får rätt information i rätt tid, vad anser Ni att det beror på?**
      – Om jag inte får tag på rätt information beror det oftast på att den informationen finns någon annanstans t.ex. i primär-, sluten- eller öppenvården. Dessa drivs av olika huvudmän och är inte kopplade ihop.
5. **Anser Ni att nuvarande åtkomst till information är tillräcklig och att den uppfyller de krav, utifrån verksamheten och lagstiftningen, som finns för att skydda information?**
   – Jag anser att den nuvarande åtkomsten till information är tillräcklig och att den uppfyller de krav som ställs på den utifrån verksamheten och lagstiftningen.
6. **Anser Ni att det finns problem med att Ni får tillgång till för lite information och i så fall vilken typ av information saknar Ni tillgång till?**
   – Enligt min åsikt så skulle vi behöva mer information från biståndsbedömare om olika patienter. Som det ser ut idag så har vi ingen information från deras sida. Våran och deras information är skilda och vi kan inte komma åt det. Jag har hört att det kan bli så att i framtiden får vi en del av deras information. En annan typ av information som vi ibland skulle behöva är information från t.ex. sluten- och öppenvården.

Bilaga 3c. **Intervju med användare 2, hemvården** 2 (2)

7. **Om Ni saknar viss information, hur agerar Ni för att få tag på denna?**
   – *Vi får kontakta de ställen där det finns den önskade informationen och be de antigen skicka denna i pappersformat eller tar vi den direkt via telefonen.*
8. **Kan Ni ibland uppleva att viss information, som Ni har tillgång till, är överflödig eller ej nödvändig för Era arbetsuppgifter?**
   – *Nej. Det är bra att ha tillgång till informationen. Jag kanske inte använder all information jämt men om det skulle uppstå en situation där jag skulle behöva viss information, då är det bra att ha tillgång till denna. Sedan har vi ju bilder som bestämmer vilken information vi får komma åt.*
9. **Hur anser Ni att en åtkomstkontrollmekanism ska fungera för att den skall uppfylla krav ställda från användare, verksamheten respektive lagstiftning?**
   – *Jag tycker att det nuvarande systemet fungerar bra. Det är viktigt att ha bestämda behörigheter till informationen och inte ha tillgång till all information. Sedan tycker jag att det är bra att ha användar-id och lösenord. På det sättet kommer ingen obehörig ha tillgång till informationen.*