Säkerhetspolicys och riktlinjer vid användning av behörighetskontrollsystem

(HS-IDA-EA-99-320)

Jenny Nilsson (a96jenni@ida.his.se)

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

Examensarbete på det systemvetenskapliga programmet under vårterminen 1999.

Handledare: Lennart Börjesson

Säkerhetspolicys och riktlinjer vid användning av behörighetskontrollsystem

Examensrapport inlämnad av Jenny Nilsson till Högskolan i Skövde, för Kandidatexamen (BSc) vid Institutionen för Datavetenskap.

990609

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: _____

Säkerhetspolicys och riktlinjer vid användning av behörighetskontrollsystem

Jenny Nilsson (a96jenni@ida.his.se)

Sammanfattning

Verksamheter som är beroende av information är idag av ett stort behov att skydda denna på ett säkert sätt. Ett sätt att skydda verksamheter från att t.ex. informationen hamnar i orätta händer är att använda ett sk behörighetskontrollsystem (BKS). Syftet med BKS är att skydda information så att den endast är tillgänglig för den som har rätt att ta del utav den.

För att säkerhetsarbetet skall fungera tillfredsställande med BKS, är det viktigt att personalen i verksamheten är medveten om syftet och de säkerhetspolicys och riktlinjer som finns i samband med BKS. Syftet med säkerhetspolicyn är att visa vilken betydelse säkerhetsarbetet har i verksamheten.

Den centrala delen av detta arbetet är den intervjuundersökning som ligger till grund för mitt resultat. Utifrån denna materialinsamling har jag försökt besvara min frågeställning ”Finns det någon medvetenhet hos personalen kring säkerhetspolicys och riklinjer vid användning av behörighetskontrollsystem?”. Resultatet och de slutsatser jag kommit fram till finns redovisade i denna rapport.

Nyckelord: Säkerhetspolicys och riktlinjer, Behörighetskontrollsystem (BKS)

Innehållsförteckning

1 Bakgrund

Vi lever i ett dynamiskt IT-samhälle där det är svårt att förutse vad som kommer att ske härnäst i utvecklingen. I och med datatekniken sker stora förändringar i samhället och hela vårt levnadssätt håller på att förändras skriver Freese och Holmberg (1993). Säkerhet och sårbarhet är därför viktigt att tänka på för att skydda oss mot hot och risker som växer fram i takt med att datatekniken utvecklas. Att utvecklingen går snabbt återspeglas tydligt genom att titta på vad som skett inom datorutvecklingens historia. Redan på 1500-talet började utvecklingen och sedan dess har utvecklingen fortsatt i snabb takt skriver Thavenius(1997).

Eftersom vi idag lever i ett informationssamhälle där det enligt Elgemyr och Mattson (1992) är kunskap och information som är verksamhetens konkurrensmedel, anser jag att det är viktigt att det finns en medvetenhet kring säkerhetsarbetet. En av anledningarna till det stora informationsflöde som florerar i dagens samhälle är utvecklingen och användningen av persondatorer.

För att skydda informationen i verksamheten kan det ibland räcka med enkla skyddsåtgärder såsom säkerhetskopiering, god ordning, utbildning etc. skriver Beckman (1990). Detta skulle kunna minska onödiga kostnader och öka effektiviteten inom verksamheten. I vissa fall krävs det dock säkrare behandling av informationen, som att exempelvis använda kryptering eller ett behörighetskontrollsystem för att obehöriga inte skall få tillgång till sådan information som klassificeras kvalificerat hemlig eller hemlig menar Statskontoret (1991).

För att ta fram de skyddsåtgärder som krävs i verksamheten för att få en tillfredsställande ADB-säkerhet och för att underlätta säkerhetsarbetet, kan säkerhetspolicys och riktlinjer utarbetas för vad som ska gälla i verksamheten. En säkerhetspolicy kan innehålla information om hur olika typer av information skall klassificeras, vad målet med säkerheten i verksamheten är och i vilken omfattning säkerhetsarbetet skall gälla. Det finns dock inga regler för hur säkerhetspolicys och riktlinjer för ADB-säkerheten skall se ut.

Många verksamheter är idag medvetna om den viktiga frågan då det gäller säkerhetsarbetet och har utarbetat säkerhetspolicys och riktlinjer för detta ändamål. Frågan är dock om personalen i verksamheten är medvetna om dessa policys och riktlinjer och om de i så fall utnyttjar dessa för att på så sätt skydda känslig information. Detta anser jag vara en mycket viktig fråga då jag anser att de säkerhetspolicys och riktlinjer som tagits fram måste vara integrerade i hela verksamheten för att effektivisera säkerhetsarbetet och motverka de hot som verksamheten kan utsättas för.

2 Introduktion

I detta kapitel kommer olika begrepp som är väsentliga att känna till då det gäller säkerhetsarbetet att beskrivas. För att ge en bild av hur utvecklingen av datatekniken ser ur kommer ett historiskt perspektiv ges över IT-utvecklingen. Jag kommer även att förklara varför säkerheten och sårbarheten i samhället har blivit så viktigt då det gäller att skydda en verksamhets information och vilka ekonomiska konsekvenser det kan innebära.

2.1 IT-utvecklingens historia

För att spegla den snabba utvecklingen inom datatekniken vill jag ge en övergripande bild över IT-utvecklingens historia. Redan på 1500-talet då det började krävas alltmer räknearbete vid tester av olika teorier började IT-utvecklingen menar Thavenius (1997). Babbage tog fram en s.k. differensmaskin som skrev ut resultatet av olika beräkningar, detta innebar att de felkällor som de matematiska tabellerna gett kunde undvikas. Utvecklingen fortlöpte och på 1800-talet kom det som påminner om dagens datorer, nämligen hålkortsmaskiner. Dessa maskiner låg sedan till grund för många företag som sedan slogs samman och kom att heta International Business Machine (IBM) (Thavenius, 1997).

Thavenius (1997) skriver om utvecklingen under andra världskriget då datorerna började användas för militärt bruk, t.ex. använde England datorer till att avkoda tyskarnas krypterade meddelande. Datorn de använde kallades Enigma. En engelsman, Turing, uppfann då en ny dator, Bombe, som i sin tur kunde knäcka Enigmas olika krypteringsnycklar. På 1940-talet skapades ännu en dator, ENIAC som inte behövde omprogrammeras som de tidigare datorerna behövt. En helt ny uppfinning var dock transistorn som medförde att datorerna blev allt mindre och billigare att producera (Thavenius ,1997).

Thavenius (1997) skriver att det under 1960-talet producerades en rad nya datorer som bestod av en färdig programvara, en central datorenhet, magnetbandsenheter, en operatörsenhet och en skrivare. På 1970-talet kom sedan de första persondatorerna. Enligt min mening har utvecklingen gått allt fortare sedan persondatorerna uppfanns. Persondatorerna har idag blivit en del av vårt vardagliga liv.

2.2 Säkerhet och sårbarhet

Användningen av persondatorerna och den stora informationsproduktion som dessa medfört, har lett oss in i vad Freese och Holmberg (1993) kallar informationsåldern. Informationsåldern innebär att datatekniken fått en allt större roll hos våra företag och myndigheter menar Gratte (1989). Information och kunskap har fått ett stort värde i samhället och i olika verksamheter då det blivit en av de mest betydelsefulla resurser som finns idag. Utvecklingen inom datatekniken har medfört att det ställs större krav på säkerheten och mer kunskap om sårbarheten, då utvecklingen skapar nya hot och risker samtidigt som den ger ett effektivare arbete inom företag, organisationer och myndigheter (Gratte, 1989).

Enligt Statskontoret (1989) är säkerhet inte alltid en självklarhet för alla i en verksamhet. För att komma till rätta med detta måste det ske en förändring hos personalens medvetenhet och engagemang då det gäller säkerhetsarbetet. Detta har blivit viktigare i och med den stora användningen av persondatorer, vilket innebär att

många personer kommer i kontakt med det ADB-stöd som används i verksamheten. Utvecklingen av persondatorer medför att information som kan skada verksamheten eller den personliga integriteten finns i mycket stor omfattning. Det är därför viktigt att skydda denna information mot de hot och risker en verksamhet kan utsättas för. För att kunna skydda informationen krävs det att personalen i verksamheten är medveten om vad säkerhet och sårbarhet innebär. Detta är viktigt för att kunna ställa krav på säkerheten och för att kunna ge svar på viktiga säkerhetsfrågor menar Statskontoret (1989).

2.2.1 Säkerhet

Vad innebär säkerhet? Det kan vara svårt att definiera begreppet säkerhet då det skall innefatta allt från driftsäkerhet till informationsskydd och brottsförebyggande arbete menar Elgemyr och Mattson (1992). I detta sammanhang kan säkerhet definieras på följande sätt:

> ”resultatet av alla de åtgärder som syftar till att skydda data, bearbetningen av dem, från oönskade händelser”
>
> (Statskontoret, 1989, sid 17)

Säkerhet i detta arbete, anser jag, är att skydda information mot oönskade händelser som på något sätt kan komma att påverka eller skada den personliga integriteten eller verksamheten. Viktigt att påpeka är att det dock inte finns någon garanti att all information kan skyddas till 100%.

Enligt Edlund et al, (1989) har det länge varit känt att skydda sig mot fysiska hot såsom t.ex. brand, stöld och sabotage. Skydd mot fysiska hot är idag därför relativt säkra, medan det ofta är sämre med säkerheten runt verksamhetens information. För att skydda sin information menar Freese och Holmberg (1993) att information bör säkerställas på likvärdigt sätt såsom produktionsutrustning, byggnader och kapital, eftersom informationen kan vara oersättlig om den skulle komma i orätta händer eller förstöras. Att skydda information och kunskap som en verksamhet besitter är viktigt då det är dessa faktorer som idag kommit att bli verksamhetens konkurrensmedel och överlevnad. Den betydelse som dessa faktorer fått innebär att det ställs högre krav på kvalitet och säkerheten hos verksamheter menar Elgemyr och Mattson (1992).

2.2.2 Sårbarhet

Enligt Freese och Holmberg (1993) har den snabba utvecklingen inom datatekniken liksom annan teknik lett till många positiva aspekter såsom ett snabbare och effektivare samhälle. Samtidigt har det svenska samhället allt eftersom tekniken utvecklats blivit databeroende och på så sätt sårbara mot bl.a. driftstörningar som kan orsaka stora kostnader för samhället. Datorer kan utsättas för en mängd oönskade händelser, där det många gånger inte går att räkna ut konsekvenser och eventuella kostnader skriver Gratte (1989). Exempelvis kan ett programfel i elförsörjningen påverka hela samhället p.g.a. att utvecklingen gjort vårt samhälle databeroende (Statskontoret, 1989).

Databeroendet visar sig tydligt då många av våra vardagliga sysslor påverkas av maskiner som utvecklats p.g.a. datatekniken. Datorerna styr vårt vardagliga liv, de hanterar bl.a. vissa delar av trafikljusen, sjukvården, energitillförseln och mycket mer skriver Freese och Holmberg (1993). Att dessa faktorer är beroende av datorisering är det inte alltid något som alla tänker på. Det svenska samhället är mer sårbart än andra länder då vårt samhälle är mer administrativt datoriserat och många av datorsystemen

som finns i Sverige samarbetar mer med varandra jämfört med andra länders datasystem skriver Freese och Holmberg (1993).

2.2.3 Ekonomiska konsekvenser

Att bygga upp en säkerhet för att minska sårbarheten i en verksamhet är ett kostsamt arbete. Gratte (1989) skriver att det är viktigt att det finns en balansgång mellan kostnader och säkerhet. Genom att ha en god säkerhet minskar förhoppningsvis skadekostnaderna.

Statskontoret (1991) skriver att sårbarheten i datasystem kan leda till allvarliga ekonomiska konsekvenser om inte säkerheten ses som en del av förvaltningen i verksamheten. För att avgöra en verksamhets kostnader är det viktigt att väga hur stora kostnader det kan bli för verksamheten vid exempelvis förlust eller obehörig åtkomst av information mot de kostnader datasäkerheten skulle stå för. En avvägning av dessa kostnader är extra viktiga vid nyanskaffning av utrustning och datasystem menar Freese och Holmberg (1993).

2.3 Behov av informationssäkerhet

I tidigare avsnitt har jag skrivit om betydelsen av att skydda information som flödar i olika verksamheter. I detta arbete kommer begreppet information att vara av stor betydelse varav det kan vara lämpligt att definiera detta begrepp. Begreppet information kan ha en mängd olika betydelser, för olika personer och vid olika situationer. Freese och Holmberg (1993, sid 21) definierar information i ADB-sammanhang på följande sätt:

> ”information är sammanställda och behandlade data, som presenteras på ett sådant sätt att den får ett meningsfullt innehåll.”

Jag anser att denna definition ger en övergripande och bra förklaring av begreppet information. Detta arbetet kommer att behandla hur säkerhetspolicys och riktlinjer används för att skydda känslig information, som på något sätt kan komma att skada den personliga integriteten om den exempelvis kommer i orätta händer. Freese och Holmberg (1993) nämner olika exempel på vad meningsfull information kan vara. Meningsfull information kan bl.a. vara data om försäljning, kunder, anställda, prognoser, bokföring, rutiner etc.

2.3.1 Skydd av information

För att ge ett bra skydd av information som är väsentlig för en verksamhet anser Freese och Holmberg (1993) att det krävs uppgifter som klargör följande punkter:

- Vem som äger informationen?
- Vilken information som vi har behov att skydda?
- Vilken säkerhetsgrad som krävs?

Enligt Freese och Holmberg (1993) är det ägarna av informationen som har ansvaret för att informationens trovärdighet upprätthålls och att kvaliteten och omständigheterna är som användarna förväntar sig. Det är vidare ägaren av t.ex. ett personregister som är ansvarig för att skyddet mot dessa uppgifter upprätthålls.

Olika typer av information bör ibland inte vara tillgänglig för alla personer på ett företag. Freese och Holmberg (1993) skriver att informationen exempelvis kan begränsas till speciella personalgrupper eller endast för personer i företagsledningen. Tillgängligheten av informationen bör vidare göras med avseende på informationens värde och viktighet för företaget.

Vilken säkerhetsgrad som behövs till olika typer av information bör också göras med hänsyn till hur relevant och värdefull informationen är för verksamheten. Information har fått ett helt nytt värde för de flesta verksamheter och idag är det en av de värdefullaste resurser en verksamhet har menar Gratte (1989).

2.3.2 Att skydda den personliga integriteten

Datatekniken har medfört stora risker då det gäller att skydda information som berör fysiska- och juridiska personer. Datalagen som till viss del trädde i kraft 1 juli 1973 är till för att skydda fysiska personer skriver Freese och Holmberg (1993). Datalagen stiftades för att skydda personer som registreras i personregister, datoriserade register. Aronsson (1995) skriver att personregister enligt datalagen är register, förteckning eller andra anteckningar som görs m.h.a. ADB och som då består av personuppgifter. Senare trädde kreditupplysnings- och inkassolagarna i kraft. Dessa lagar stiftades för att skydda även juridiska personer, d.v.s. företag, organisationer etc. Lagarna gäller inte bara datoriserade register utan även för manuella register.

En ny lag trädde i kraft den 24 oktober 1998, PUL (Personuppgiftslagen). Enligt Datainspektionen 1998 ligger EG-direktiv till grund för PUL som ersätter datalagen från 1973. PUL är liksom datalagen till för att hindra att den personliga integriteten kränks p.g.a. felbehandling av personuppgifter skriver Datainspektionen 1998.

Dataregister som behandlar personliga uppgifter kan trots lagstiftningen inte sägas vara säkra, då datakvalitén kan vara bristfällig och personer p.g.a. detta råkat illa ut menar Freese och Holmberg (1993).

Aronsson (1995) skriver att en verksamhet måste följa den lagstiftning som finns för att lagra uppgifter som berör den personliga integriteten, men vid felaktig användning av systemet eller andra hot och risker kan informationen gå förlorad eller skadas och på så sätt skada den personliga integriteten.

2.4 Hot och risker

För att ge en övergripande bild över hot och risker kommer ett fåtal exempel att presenteras i detta stycke. Det finns nämligen flera hot och risker som förekommer i samband med användningen av datorer.

Hot kan sägas vara avsiktliga, oavsiktliga hot, yttre eller inre hot menar Aronsson (1995). Freese och Holmberg (1993) framför att oavsiktliga hot är sådana som orsakats av den mänskliga faktorn, exempelvis feloperationer. Avsiktliga brott är däremot hot som på något sätt går att förhindra eller förebygga. Avsiktliga hot är ofta menade att skada verksamheten, dessa är ofta angrepp utifrån verksamheten d.v.s. yttre hot skriver Freese och Holmberg (1993). Inre hot är däremot sådana som orsakas av personer inom verksamheten, dessa kan vara avsiktliga eller oavsiktliga. Oftast är dessa dock oavsiktliga och förekommer p.g.a. den mänskliga faktorn.

Freese och Holmberg (1993) anser att vanligt förekommande hot exempelvis kan vara sabotage mot anläggningar eller utrustning. Andra hot som riktar sig mot

datorutrustning är bl.a. brand- och vattenskador, felaktig hantering av utrustningen, otillräcklig säkerhetskopiering och problem med bristfälliga behörighetskontrollsystem menar Aronsson (1995).

Andra förekommande hot är bl.a. hackers och datavirus. Freese och Holmberg (1993) skriver bl.a. om problemet med hackers d.v.s. personer som obehörigt bryter sig in i datorsystem utan att orsaka någon skada utan mer för att varna att det går att ta sig in i systemet. Aronsson (1995) anser att ett stort hot som ofta förekommer är de datavirus som existerar. Datavirus är enligt Aronsson (1995) en programdel eller olika kommandon som kopierar sig själv till andra program.

Att skydda sin information mot de hot som finns idag är mycket viktigt för alla verksamheter som på något sätt använder sig av ADB-stöd, då informationen är grunden till verksamheten skriver Aronsson (1995). Dessa skydd kan vara administrativa som att t.ex. ha utarbetade säkerhetspolicys och riktlinjer, men även ADB-tekniska skydd som exempelvis säkerhetskopiering, kryptering av information och behörighetskontrollsystem (se kap 4).

2.5 Säkerhets- och riskanalys

Eftersom alla verksamheter små som stora kan utsättas för störningar är det viktigt att göra en bedömning över vilka risker verksamheten kan utsättas för och vilka kostnader dessa skulle medföra menar Aronsson (1995). Statskontoret (1989) framför att vid framtagandet av säkerhetspolicys och riktlinjer är säkerhetsanalysen en viktig del av säkerhetsarbetet. Säkerhetsanalyser och riskbedömningar ger underlag för att en verksamhet ska kunna bestämma vilka skyddsåtgärder de kan komma att behöva. Enligt Elgemyr och Mattson (1990) har en säkerhets- och riskanalys två syfte. Dess uppgift är dels att skydda sig mot att skada eller förlust av information inträffar och dels att begränsa skador av en oönskad händelse.

Enligt Aronsson (1995) brukar en säkerhetsanalys innehålla moment som att ge en beskrivning av olika hotbilder, konsekvenser som dessa kan medföra för verksamheten, eventuella skadekostnad vid en oönskad händelse och dessutom en bedömning av vilka skyddsåtgärder som kan vara relevanta för verksamheten.

Behovet av skyddsåtgärder är olika från verksamhet till verksamhet och dessutom beroende av vilket ADB-stöd som används i verksamheten menar Statskontoret (1989). Att göra en säkerhets- och riskanalys innebär dock inte att verksamheten kan förebygga och skydda sig mot alla eventuella hot som verksamheten skulle kunna utsättas för. Elgemyr och Mattson (1990) anser att en riskanalys har vissa begränsningar och brister, som att det exempelvis kan vara svårt att värdera och uppskatta vilka hot som kan komma att uppträda i verksamheten.

3 Säkerhetspolicy och riktlinjer

En väl utarbetad säkerhetspolicy i en verksamhet är mycket viktig för administrationen av säkerheten menar Statskontoret (1989). En säkerhetspolicy ökar medvetenheten och engagemanget av säkerhetsarbetet hos personalen i en verksamhet. I nedanstående avsnitt kommer jag att förklara varför det finns behov av säkerhetspolicy, hur en säkerhetspolicy kan dokumenteras, syftet med att ha en säkerhetspolicy och riktlinjer och vikten av ansvarsfördelningen mellan olika funktioner inom verksamheten.

3.1 Behov av säkerhetspolicy och riktlinjer

Enligt Statskontoret (1989) är behovet av säkerhetspolicys och riktlinjer beroende på verksamhetens krav och behov av säkerhet. Alla verksamheter som på något sätt använder ADB-stöd är dock i behov av att skydda sin information. Ett hjälpmedel för att nå önskad säkerhet kan nås m.h.a. säkerhetspolicys och riktlinjer.

3.2 Syfte med säkerhetspolicys och riktlinjer

Syftet med säkerhetspolicys och riktlinjer är att visa vilken betydelse säkerhetsarbetet har. Genom säkerhetspolicys och riktlinjer kan medvetenhet och engagemang i verksamheten skapas menar Aronsson (1995). Säkerhetspolicyns tanke är att ge en övergripande bild och inriktningen av målen med säkerheten. Syftet med respektive säkerhetspolicy och riktlinjer varierar naturligtvis då alla verksamheter har olika behov och krav av säkerhet.

I detta arbete gäller säkerhetsarbetet att skydda känslig information mot obehörig åtkomst, alltså säkerhetspolicys och riktlinjer för informationssäkerhet och behörighetskontrollsystem. Jag har valt detta då jag tror att många verksamheter har tagit fram säkerhetspolicys och riktlinjer för detta syfte men att de inte följs på ett riktigt sätt och p.g.a. det, kan känslig information som berör fysiska personer skada den personliga integriteten.

3.3 Dokumentutformning

Det är viktigt att vara medveten om att det inte finns någon standardiserad säkerhetspolicy som gäller för alla verksamheter, då alla verksamheter ser olika ut. De dokument som beskriver vilken säkerhetspolicy och vilka riktlinjer som ska gälla för verksamheten skall enligt Statskontoret (1989) spegla verksamheten. Aronsson (1995) ger ett exempel för hur en säkerhetspolicy skulle kunna se ut i en kommun. Följande punkter finns presenterade i denna:

- *Motivet för ADB-säkerheten* : uttrycker varför verksamheten har ett behov av en ADB-säkerhet.
- *Mål med ADB-säkerheten* : exempelvis vem som skall beröras av säkerhetsarbetet, bedömning av vilka skyddsåtgärder som kan krävas, och att uppföljning av exempelvis riskanalyser, skyddsåtgärder och utbildning skall ske.
- *ADB-säkerhetsnivå* : vilka krav som finns på säkerheten från lagar, intressenter och användare.
- *Ansvar och organisation* : dvs vem som ansvarar för vad inom ADB-säkerheten.

- *Omfattning och genomförande* : vad säkerhetspolicyn skall beröra för verksamheter och område. För genomförandet finns uppsatt vad som bör göras för att uppnå önskad säkerhetspolicy, däribland säkerhetsanalyser, skyddsåtgärder, utbildning och uppföljning.

Detta är endast ett exempel som åskådliggör vilka punkter som kan vara relevanta att ha med i en säkerhetspolicy och skall inte ses som en mall för en säkerhetspolicy, då det finns ett flertal sätt att ta fram en säkerhetspolicy.

Statskontoret (1989) skriver att dokumenten som behandlar säkerhetspolicyn och riktlinjerna inte får vara allt för detaljerade och inte heller för övergripande. Dokumenten ska bygga på verksamhetens inriktning, omfattning, förändrad hotbild, informations- och ADB-strategin etc. Omprövning av säkerhetspolicyn är således viktig då det kan ske förändringar av ovanstående faktorer som kan påverka verksamhetens säkerhetsarbete och medföra att förändringar av säkerhetspolicyn kan behövas.

Statskontoret (1989) anser att det förutom ett policydokument bör finnas uppgifter om hur ADB-säkerhetsarbetet skall hanteras och vilka säkerhetskrav som gäller för verksamheten, exempelvis krav från gällande lagstiftning.

3.4 Ansvarsfördelning och organisation

Ansvarsfördelningen och organisationen kring säkerheten är när det gäller att ta fram säkerhetspolicys och riktlinjer mycket viktig anser Statskontoret (1989). När det gäller ansvaret finns det dels ett generellt ansvar som är kopplat till hela verksamheten, där ledningen har huvudansvaret och dels det särskilda ansvaret för säkerhetsarbetet där det är personer med specialkompetens som bär ansvaret skriver Statskontoret (1989).

Enligt Statskontoret (1989) skall ansvaret för säkerhetsarbetet dock ligga i hela verksamheten. Det är av stor vikt att alla berörda av säkerhetsarbetet känner till vilka säkerhetsföreskrifter som finns. Det finns olika ansvarsbegrepp som används vid säkerhetsfrågor och organisationen kring säkerheten. Exempel på ansvarsbegrepp kan vara verksamhetsansvar, systemägaransvar, systemansvar, användaransvar, ADB-funktionens ansvar, registeransvarig, ADB-säkerhetschef, ADB-säkerhetsansvariga, och ADB-säkerhetsorganisation. Jag vill inte gå in i detalj vad dessa begrepp innebär trots att de är viktiga vid säkerhetsarbetet, eftersom jag anser det vara en allt för detaljerad beskrivning för syftet med detta arbete.

3.5 Informationsklassificering

En del av säkerhetsarbetet vid framtagande av säkerhetspolicys och riktlinjer är att klassificera informationen i verksamheten skriver Statskontoret (1991). När en klassificering skall göras är det viktigt att vara medveten om att detta kan göras på olika sätt. Dataföreningen i Sverige (1997) har delat in klassificeringen i följande informationsgrupper:

- *Kvalificerat hemlig* - information som är av betydelse för rikets säkerhet, även information som berör den personliga integriteten kan klassas i denna grupp.
- *Hemlig* - information som kan skada verksamheten om det förekommer spridning av informationen.

- *Intern* - information som kan spridas fritt inom verksamheten, exempelvis interna meddelande.
- *Öppen information* - information som är tillgänglig för personer utanför den egna verksamheten.

En informationsklassificering är en nödvändighet för att kunna ge ett fullgott skydd i verksamheten. Brister som sker i informationshanteringen beror ofta på att inte någon klassificering av informationen gjorts. Aronsson (1995) menar att för att undvika brister i informationshanteringen bör informationsklassificeringen vara en del av utvecklingen av ett system. Klassificeringsarbetet kräver då kunskaper om bl.a. krav från lagstiftning, intressenternas behov av information och informationens innehåll och omfattning.

Dataföreningen i Sverige (1997) skriver att klassificeringen görs utifrån vad som skulle hända om informationen hamnar i orätta händer och vad detta skulle innebära för verksamheten. Särskilt viktigt i detta arbete är den information som klassificeras kvalificerat hemlig eller hemlig, d.v.s. sekretessbelagd eller integritetskänslig information. Då en verksamhet arbetar med denna typ av information finns ett behov av ett s.k. behörighetskontrollsystem (se kap 4) för att förhindra att obehöriga inte får tillgång av denna informationen.

4 Behörighetskontrollsystem

För att förhindra obehöriga att få tillgång av känslig information som en verksamhet besitter kan ett behörighetskontrollsystem vara till god hjälp. I nedanstående avsnitt kommer jag att beskriva vad ett behörighetskontrollsystem är, vad dess syfte är, vilka tekniska funktioner ett behörighetskontrollsystem kan tänkas ha för att ge ett tillfredsställande skydd och hur ansvaret och organisationen kan se ut kring ett behörighetskontrollsystem.

4.1 Vad är ett behörighetskontrollsystem?

Dataföreningen i Sverige (1997) anser att ett behörighetskontrollsystem (BKS) kan användas för att skydda information mot manipulering eller spridning i en verksamhet som exempelvis använder persondatorer. Enligt Statskontoret (1991) är ett BKS ett system som består av olika samverkande delar däribland ett aktuellt operativsystem, funktioner i operativsystemet som ska styra behörighetskontroll, ett program som stödjer behörighetskontrollen, behörighetsfunktioner i applikationer och administrativa rutiner.

Enligt Statskontoret (1991, sid 17) är ett behörighetskontollsystem följande:

> ”ett system som kan kontrollera behörighet och som skall skydda information så att den endast är tillgänglig för den som har rätt att ta del av den”

Ovanstående definition stämmer bra överrens med min uppfattning om vad ett BKS har för uppgift, därför valde jag just denna definition.

4.2 Syfte med BKS

Enligt Statskontoret (1991) har ett BKS tre huvudsyfte:

- Skydda verksamheten mot avsiktliga eller oavsiktliga brott
- Skydda informationen mot obehörig åtkomst
- Skydda medarbetare genom att förhindra denne mot oavsiktligt missbruk av systemet

Med användning av ett BKS skall detta enligt Statskontoret (1991) försvåra eller förhindra obehörig användning av ADB-system, åtkomst till information/datorprogram, manipulering av information och radering av information.

Enligt Dataföreningen i Sverige (1997) skall systemet förhindra personal att genomföra ett oavsiktligt brott och även förhindra att personal anklagas för obehörigt tillträde av verksamhetens IT-system. Dessutom kan BKS användas för uppföljning av funktioner som finns i verksamhetens system.

4.3 Tekniska funktioner i BKS

För att få ett tillfredsställande BKS bör det ha följande tekniska funktioner menar Statskontoret (1991).

- Identifiera och verifiera användare av det befintliga IT-systemet.
- Systemet bör kunna reglera vilka rättigheter som respektive användare har till IT-systemet och viss information.
- Reglera vilka resurser en användare får tillgång till, exempelvis skrivare, program etc.
- Systemet bör kunna registrera vad en användare genomför för typer av aktiviteter i verksamhetens IT-system. Ett annat ord för detta är loggning.
- Systemet skall ha möjlighet att spärra användaridentiteter.
- Kryptering av lösenord.
- Definiera vilka/vilken terminal som användaren får ha tillgång till.

Detta är några av de funktioner som Statskontoret (1991) anser ett BKS bör ha för att systemet skall fungera på ett tillfredsställande sätt. För att systemet sedan skall användas och fungera på tänkt sätt måste regler för hur de administrativa rutinerna skall skötas finnas tillgängliga.

Om en verksamhet rör sig med information som berör fysiska personer, dvs personuppgifter som exempelvis är sekretessbelagda kan användningen av ett BKS vara ett krav gentemot lagar och förordningar skriver Dataföreningen i Sverige (1997).

4.4 Ansvar och organisation

Enligt Dataföreningen i Sverige (1997) måste det finnas ett tydligt ansvar och organisation vid användningen av ett BKS, detta skall innebära att användaren av behörighetskontrollsystemet har rätt behörighet vid rätt tidpunkt. Dataföreningen i Sverige (1997) menar att det måste finnas dokumenterade regler för vilket ansvar som gäller för behörighetskontrollsystemet, användarna av systemet ska ha utbildning av hur det fungerar och kontroller bör göras av arbetsledningen för att kunna visa vad som gäller vid ett eventuellt missbruk av systemet.

Systemägare

Beroende på vilken verksamhet det rör sig om har olika personer olika ansvarsområde definierade. Enligt Dataföreningen i Sverige (1997) måste det finnas en systemägare som bl.a. har till uppgift att hantera vilka personer som har rättigheter till vad i systemet. Systemägarens uppgift är också att eventuellt kunna delegera administationsuppgifter till behörighetsadministratören och göra uppföljning och kontroll av behörigheten.

Operativ chef

Dataföreningen i Sverige (1997) anser även att det bör finnas en operativchef som bestämmer vilken person som har en viss funktion i arbetet exempelvis vem som är tillåten att attestera, vem som får betala ut i ett ekonomisystem osv. Operativchefens uppgift är att ändra eller bestämma behörigheten exempelvis vid nyanställning, när någon i personalen får ändrade arbetsuppgifter eller om någon avslutar sin anställning,

vidare är det operativchefens uppgift att informera vilka regler som gäller med en viss behörighet och göra uppföljning av de olika behörigheter som delats ut.

Behörighetsadministratör

Behörighetsadministratören är den person som främst har till uppgift att göra det praktiska administrativa arbetet. Behörighetsadministratörens uppgifter kan enligt Dataföreningen i Sverige (1997) bl.a. vara att registrera användarna i BKS, ge operativ chefen uppgifter om nya registreringar, arkivera beslut från operativ chefen angående behörighet till viss person. Behörighetsadministratören skall även ha en rådgivande funktion, ge användaren en allmän beskrivning hur systemet fungerar exempelvis information kring lösenordskrav, krav på tidsintervall mellan lösenordsbyte, vad som kan hända vid misslyckad inloggning etc.

4.5 Exempel på säkerhetspolicys och riktlinjer i samband med BKS

En verksamhet som använder sig utav ett BKS, bör enligt min mening sätta upp säkerhetspolicys och riktlinjer för detta ändamål. Information och utbildning är sedan en viktig del av arbetet för att nå ut till användarna av systemet och öka deras medvetenhet kring syftet med systemet.

Att personalen är medveten kring säkerhetspolicys och riktlinjer i samband med behörihetskontrollsystem är enligt min mening nedanstående definition:

> om personalen tagit del utav någon säkerhetspolicy muntligt eller skriftlig och har denna i åtanke vid användandet av behörighetskontrollsystemet.

Denna definition är nödvändig för att kunna besvara problemställningen. Definitionen gör det lättare att avgöra om personalen är medveten eller inte om säkerhetspolicys och riklinjer.

Jag har inte hittat så mycket material kring detta område, endast ett exempel från Lunds kommun, hur de satt upp sina säkerhetspolicys och riktlinjer för användningen av ett BKS. Enligt Drätselkontoret (1998) skall Lunds kommuns säkerhetspolicys och riktlinjer för BKS hantera följande funktioner:

- *Identifiering* : En standard har satts upp över hur användaridentifieringen skall skötas.
- *Behörighet tilldelning* : beskriver hur ansökan om behörighet skall hanteras och vilka rutiner som gäller för olika typer av klassificerad information.
- *Autenciering (personlig identifiering)* : hur användarna skall identifiera sig inom servern på kommunnätet och vid distansarbete. Det finns även uppsatt en rad regler över lösenordskrav.
- *Behörighet borttagning* : hur behörigheten skall hanteras då någon slutar sin tjänst eller får ändrade arbetsuppgifter.

Jag bör påpeka att ovanstående punkter endast är ett exempel över hur säkerhetspolicys och riktlinjer för ett BKS skulle kunna se ut. Det finns olika behov och säkerhetskrav i olika verksamheter och därför finns det inte någon standard över hur säkerhetspolicys och riktlinjer skall se ut.

4.6 Problem med BKS

Trots fördelarna ett BKS medför med att hindra obehörig åtkomst av information kan det finnas en del problem med denna uppgift. Att ge rätt person rätt behörighet i små organisationer går bra, men detta kan vara ett problem i organisationer som har en stor geografisk spridning. Det är mycket svårt att hindra obehörig tillgång av information i en sådan organisation om det t.ex. finns personer som utger sig själva att vara någon annan menar Dataföreningen i Sverige (1997). Att vara medveten om problemet med felaktig behörighetstilldelning är en sak men att hitta en praktisk lösning kan vara svårt.

Ett annat viktigt problem är enligt Dataföreningen i Sverige (1997) att användaren kan tycka att användningen av ett BKS är påtvingat. Många användare försöker därför att kringgå systemet vilket kan leda till allvarliga konsekvenser. Det är därför viktigt att användarna får information och utbildning kring syftet och behovet av systemet. BKS är ju dels till för att skydda användarna så att de inte blir misstänkta att ha missbrukat systemet.

Jag anser liksom Dataföreningen i Sverige (1997) att detta är svåra problem att komma tillrätta med. Säkerhetspolicys och riktlinjer för detta ändamål tror jag dock skulle kunna underlätta arbetet om användarna blir tillräckligt underrättade om hur behörighetskontrollsystemet fungerar och skall användas.

4.6.1 Ett exempel från verkligheten på problem med BKS

För att visa vilka problem som finns med säkerhetsarbetet vill jag ge en övergripande förklaring av ett exempel som jag tagit del av på Internet. Detta är ett exempel från Datainspektionens hemsida (Datainpektionen ,1998). Datainspektionen (1998) skriver att det på sjukhus behandlas mycket integritetskänslig information, d.v.s. patientuppgifter som kan skada den personliga integriteten om de kommer i orätta händer eller felbehandlas. Enligt information från Datainspektionens hemsida, har datainspektionen genomfört olika inspektioner för att undersöka hur integritetsskyddet fungerar vad gäller patientuppgifter, finns det en del slarv i säkerhetsarbetet vad gäller inloggningsrutiner och placering av den fysiska utrustningen. Datainspektionen (1998) skriver att det exempelvis förekommer att bildskärmar är placerade så att patienter kan ta del av informationen och att det även förekommer att servrar är felaktigt placerade. Detta är några av de brister som Datainspektionen funnit. Jag har dock endast tagit del av en sammanfattning över detta problem. Det finns rapporter som bekräftar vilka brister som finns vad gäller säkerhetsarbetet på sjukhus.

5 Problembeskrivning

I dagens samhälle är det enligt min mening viktigt att vara medveten om hur stor betydelse säkerheten av information har, då den kan komma att skada den personliga integriteten om den kommer i orätta händer eller på något sätt skadas. Säkerhetsarbetet är dock inte alltid något självklart, trots att säkerheten borde vara en del av verksamheten (Aronsson, 1995).

För att skydda integritetskänslig information använder många verksamheter säkerhetspolicys och riktlinjer för att på så sätt ta fram en handlingsplan och vilka skyddsåtgärder som kan komma att behövas. Jag anser att detta är särskilt viktigt inom den offentliga sektorn eftersom det finns mycket integritetskänslig information hos dessa verksamheter.

En av de skyddsåtgärder som kan vara lämpligt vid integritetskänslig information, är enligt Dataföreningen i Sverige (1997) ett behörighetskontrollsystem (BKS). BKS är ett bra skydd för att förhindra obehörig åtkomst av integritetskänslig information. Ett BKS ger ett gott skydd om det används på ett riktigt sätt efter utsatta säkerhetspolicys och riktlinjer menar Statskontoret (1991).

Finns det tydliga säkerhetspolicys och riktlinjer vad gäller användningen av BKS? Har information kring säkerhetspolicys och riktlinjer nått ut till användarna? Hur ansvarar användarna för att obehöriga inte skall få tillgång till integritetskänslig information? Utnyttjas säkerhetspolicyn och riktlinjerna i det syfte som är tänkt?. Detta är några relevanta frågeställningar som kan vara av intresse i detta arbete.

Min problemformulering är följande:

- Finns det någon medvetenhet hos personalen kring verksamhetens säkerhetspolicys och riktlinjer, vid användning av behörighetskontrollsystemet?

5.1 Avgränsning

I min undersökning kommer jag endast att beröra integritetskänslig information d.v.s. sekretessbelagd och hemlig information. Undersökningen kommer även att vara inom den offentliga sektorn, då jag anser det vara där som integritetskänslig information finns tillgänglig. Inom den offentliga sektorn kommer jag att begränsa mig till vårdcentraler inom Skövde kommun.

5.2 Förväntat resultat

Jag förväntar mig att arbetet kommer att ge en inblick i hur viktigt det idag är med säkerhetsarbetet kring säkerhetspolicys och riktlinjer. Jag hoppas även att arbetet kommer att ge kunskap kring hur information och utbildning av säkerhetspolicys och riktlinjer når ut till personalen.

6 Möjliga metoder och metodval

I detta avsnitt kommer jag att beskriva vilka möjliga metoder som finns för min undersökning. Metoder är till för att samla in material som förhoppningsvis ska ge svar på den definierade problemställningen. Beroende på arbetets karaktär lämpar sig olika metoder bäst för olika sorters undersökningar.

Det finns olika metoder som kan användas för insamling av material, antingen i en sorts kombination med varandra eller var för sig. En kombination av olika kvalitativa metoder ger enligt Repstad (1999) ett bredare material, vilket ger en säkrare grund att tolka materialet på. Det är dock beroende på syftet med arbetet som avgör om det är lämpligt med en kombination av olika metoder, eller att endast använda en metod.

Med varje metod finns det en rad fördelar och nackdelar, dessa ska jag diskutera i nedanstående avsnitt för att slutligen komma fram till den metod eller de metoder som är lämpligast för mitt arbete. Patel och Davidson (1994) beskriver olika metoder som kan användas. De som jag skulle kunna använda mig av i detta arbete är följande:

- Litteraturstudie
- Survey undersökning

Litteraturstudie och survey undersökning verkar relevanta för mitt arbete då jag vill göra en kvalitativ studie. Enligt Repstad (1999) innebär en kvalitativ studie att undersökningen oftast är avgränsad till särskilda miljöer, för att ge en helhetsbild av det som studeras. Patel och Davidson (1994) skriver att målet med en kvalitativ undersökning är att kunna förstå och analysera helheter.

Vid bearbetningen och analysen av det insamlade materialet vid en kvalitativ undersökning arbetar man oftast med textmaterial, t.ex. material som framställts genom intervjuer skriver Patel och Davidson (1994).

Litteraturstudier och survey undersökning kan vara lämpliga metoder i detta arbete då jag vill ha material om personalens medvetenhet kring säkerhetspolicys. En kvalitativ undersökning ger mig en djupare kunskap, än en kvantitativ undersökning skulle gjort. Enligt Patel och Davidson (1994) ger en kvantitativ undersökning ett fragmenterat informationsunderlag jämfört med en kvalitativ undersökning.

6.1 Litteraturstudier

Litteraturstudier är en bra metod för att skapa sig en kunskapsbas om ett specifikt ämne. Vid en litteraturstudie är det viktigt att kritiskt granska allt material som används och eventuellt jämföra olika författares synpunkter. Enligt Bell (1993) är det viktigt att endast använda relevant litteratur för studien. Metoden är väldigt tidskrävande eftersom det oftast är nödvändigt att gå igenom en hel del litteratur, för att sedan välja ut det som är relevant för syftet med arbetet. Material som kan användas är böcker, artiklar, forskningsrapporter etc.

Fördelar och nackdelar

En litteraturstudie är en bra metod då det oftast finns relativt mycket information om de flesta ämnen. Bra med metoden är också att det ofta finns mycket referenser till litteraturen, där det går att hitta ytterligare material inom det område man söker. En litteraturstudie ger dessutom kunskaper inom det område som studeras.

Nackdelar är dock att det är en relativt tidskrävande metod. Det kan vara svårt att få tag i önskad litteratur, då den kan vara utlånad på biblioteket. Det är dessutom tidskrävande att gå igenom litteraturen och svårt att verkligen fånga in det som är väsentligt för syftet med arbetet. Det gäller att inte ta med för mycket eller för lite av det material som kan vara av intresse i arbetet. Det kan även vara svårt att få fram litteratur inom nya forskningsområden.

6.2 Survey undersökning

Enligt Bell (1993) är syftet med en survey undersökning att genom intervjuer eller enkäter få fram information. Denna information skall sedan analyseras och då ge ett mönster av svaren som sedan kan jämföras. Enligt Bell (1993) ger en survey undersökning svar på frågorna vad, när och hur medan det kan vara svårare att få svar på frågor om varför.

Undersökningen görs på en större avgränsad grupp som kallas population skriver Patel och Davidson (1994). Om undersökningen görs på hela undersökningsgruppen kallas detta för en totalundersökning. En stickprovsundersökning kan göras med hjälp av ett slumpmässigt urval, om det inte finns möjlighet till att genomföra undersökningen av hela populationen. Det är viktigt att undersökningsgruppen specificeras noggrant så att det verkligen är den avsedda gruppen som är med i undersökningen.

6.2.1 Enkätundersökning

En enkätundersökning fungerar oftast så att enkäter skickas ut eller överlämnas till önskad svarsgrupp. Respondenterna fyller således i enkäterna och skickar eller lämnar tillbaka dem. Det finns även enkätundersökningar där intervjuaren är på platsen och kan vägleda och förtydliga eventuella frågeställningar som kan verka oklara skriver Patel och Davidson (1994).

Dahmström (1991) menar att vid användning av enkäter används en standardiserad intervju (se avsnitt 6.2.2). Enkätundersökningen bygger på att samma frågor ställs till ett antal personer, där det oftast redan finns fördefinierade svarsalternativ som respondenten således kan välja mellan. Detta innebär att det vid intervjutillfället inte finns något utrymme för några ytterligare svar, och alltså kan ingen ny information tillföras undersökningen.

Olika typer av enkätundersökningar kan genomföras. Enligt Trost (1994) finns det två enkätundersökningar som det brukar göras skillnader mellan, postenkäter och gruppenkäter.

Postenkäter

Trost (1994) skriver att en undersökning med postenkäter genomförs så att enkäterna skickas ut per post. Vissa företag vill skicka enkäterna över den interna posten och på så sätt spara in pengar vid materialinsamligen. Nackdelar bör dock övervägas, som

t.ex. att respondenten inte kan besvara enkäten på arbetsplatsen kanske p.g.a. att andra anställda kan ta del av dennes svar.

Gruppenkäter

Trost (1994) anser att gruppenkäter är vanligt där det finns många respondenter på samma plats, vilket gör det lätt att nå respondenterna med frågeformuläret. Vid denna typ av enkätundersökning finns ofta personen som sköter undersökningen på plats och kan förklara eventuella oklarheter. Trost (1994) skriver också att det är viktigt att intervjupersonen försöker motivera respondenterna, för att få respondenterna att medverka i undersökningen.

Fördelar och nackdelar

En enkätundersökning var till en början aktuell för min undersökning, men eftersom det finns en stor risk för bortfall och inga följdfrågor eller öppna frågor är möjliga beslutade jag mig för att inte använda denna metod. Det finns också begränsade möjligheter att ge förklaringar till respondenten om någon av frågorna verkar oklara.

Denna metod skulle kunna användas för att få ett större och bredare underlag för min undersökning. Enkäter skulle kunna skickas ut till hela personalen på vårdcentralerna och då kunna få ett stort materialunderlag. Undersökningen skulle kunna ge mig ett bra underlag förutsatt att bortfallet av respondenter inte är för stort. Enkäterna skulle dock inte ge mig lika bra svar på öppna frågor, då det inte finns möjlighet att förklara oklarheter i samband med undersökningen. Vid en enkätundersökning skulle det dessutom inte finnas något utrymme för eventuella följdfrågor till respondenten, vilket jag ansåg vara av stor vikt i min undersökning.

Vid en eventuell enkätundersökning skulle kvantiteten av underlaget ha blivit stort, men p.g.a. att intervjuaren eventuellt inte skulle kunna finnas på plats vid “intervjun” kan kvaliteten av materialet bli sämre, då vissa frågor eventuellt kan verka oklara. Dessa frågor kan då inte diskuteras och utredas.

6.2.2 Strukturerade och standardiserade intervjuer

En intervju kan vara upplagd på en rad olika sätt. En intervju kan vara av hög eller låg grad av strukturering skriver Patel och Davidson (1994). Graden av strukturering på intervjun avgör respondentens utrymme att fritt svara på frågor utifrån sin egen inställning eller erfarenheter skriver Patel och Davidson (1994). En helt ostrukturerad intervju ger respondenten fritt utrymme att besvara frågorna, medan en strukturerad intervju begränsar respondentens ”svarsutrymme”.

Vid hög grad av strukturering kan enkäter med fasta svarsalternativ användas, eller så kan intervjuer användas där målet är att göra en kvantitativ analys av materialet. Låg grad av strukturering kan således användas vid en enkätundersökning eller vid intervjuer med öppna frågor.

Enligt Patel och Davidson (1994) avgörs graden av standardisering i en intervju av hur frågorna formulerats av intervjuaren, dvs frågornas utformning och ordningsföljd. I en intervju som är helt standardiserad ställs samma frågor till samtliga respondenter i samma ordning. Detta är användbart om svaren skall jämföras och analyseras skriver Patel och Davidson (1994). Vid en helt ostandardiserad intervju formuleras frågorna under intervjun och ställs i den ordning som frågorna verkar mest lämpligt för respektive respondent.

6.2.3 Besöksintervju

En intervju genomförs enklast om intervjuaren åker till respondenten och genomför intervjun på arbetsplatsen. Enligt Jacobsen (1993) finns det olika sätt att genomföra en intervju.

När en besöksintervju skall genomföras är det enligt Dahmström (1991) viktigt att information kring syftet med undersökningen ges till respondenten. Det är även viktigt att på ett tidigt stadium kontakta respondenten om tillåtelse till intervjun skriver Patel och Davidson (1994).

Fördelar och nackdelar

Denna typ av undersökning är väldigt tidskrävande men kan oftast ge mer givande svar då intervjuaren kan vägleda och förklara eventuella missförstånd av frågeställningarna skriver Patel och Davidson (1994). Det finns även möjlighet att ställa följdfrågor och längre frågor vid intervjutillfället. En besöksintervju ger en personlig kontakt mellan intervjuaren och respondenten vilket kan ge bättre och mer uttömmande svar.

Nackdelar med besöksintervjuer är bl.a. att det kan vara svårt att få tag i rätt personer och bestämma plats och tid för intervjun. Det kan vara svårt att bestämma tid för intervjun om respondenten har ett tidspressat schema. En annan nackdel kan vara att det är en relativt dyr metod och tar lång tid att genomföra, eftersom intervjuaren måste ta sig till den plats där intervjun skall genomföras.

6.2.4 Telefonintervju

En telefonintervju fungerar på liknande sätt som en besöksintervju. Skillnaden är att intervjun sker per telefon. En telefonintervju är ett alternativ till en besöksintervju om det inte finns tillfälle eller tillgång att genomföra en besöksintervju. Enligt Dahmström (1991) är det svårare att behålla respondentens intresse och motivation vid en telefonintervju. Denna typ av intervju får därför inte vara för lång och inte ha alltför svåra och komplicerade frågeställningar.

Fördelar och nackdelar

Fördelar med en telefonintervju är att det liksom vid en besöksintervju finns möjlighet att ställa följdfrågor. Om det skulle uppstå några missförstånd eller feltolkningar finns det möjlighet till förklaring och vägledning från intervjuaren. Detta är även en billig och snabb undersökningsmetod.

Nackdelar är att intervjun inte kan hållas lika lång som en besöksintervju, då respondenten lättare tappar intresset. En telefonintervju kan innebära att svaren inte blir lika uttömmande som svaren skulle vara i en vanlig intervju eftersom det inte finns någon personlig kontakt.

6.3 Val av metod

Tidigare har jag beskrivit de metoder som kan vara relevanta för detta arbete. I detta avsnitt ska jag diskutera vilka metoder jag tänkt använda mig utav i detta arbete, och varför jag valt just dessa metoder.

6.3.1 Intervjuundersökning

Besöksintervjuer och telefonintervjuer har jag valt för insamling av material. Dessa metoder tror jag kommer att ge mig det underlag som krävs för att komma fram till ett svar på min problembeskrivning. Detta eftersom en besöksintervju tillåter längre frågeställningar och ger möjlighet till följdfrågor och öppna frågor. En besöksintervju kan på så sätt ge mig ett kvalitativt material att analysera. Telefonintervjuer kommer att bli nödvändigt då det inte finns möjlighet att besöka en av de tänkta vårdcentralerna. En telefonintervju tillåter i stort sett samma möjligheter som en besöksintervju, varför detta inte kommer att påverka undersökningens resultat.

Metoderna, besöksintervju och telefonintervju, ger mig mindre kvantitet av underlaget då jag måste begränsa antalet intervjuer. Jag anser dock att denna typ av undersökning ger mig en större kvalitet av materialet, än t.ex. enkätundersökning skulle gett, då jag finns närvarande under intervjun och kan ge eventuella förklaringar på frågor som kan verka oklara. Detta skulle på så sätt ge mig ett bättre underlag att sedan arbeta vidare med.

Metoderna anser jag vara lämpliga då jag begränsat min undersökningsgrupp till vårdcentralerna inom Skövde kommun. Det finns därmed möjlighet för mig att åka runt till de olika vårdcentralerna och på så sätt skapa en mer personliga kontakt, vilket i sin tur kan motivera respondenterna och därmed ge mig mer uttömmande svar än jag skulle fått exempelvis vid en enkätundersökning.

6.4 Metoder som valts bort

Jag valde bort enkätundersökning eftersom det finns en stor risk för bortfall och inga följdfrågor är möjliga vid “intervjutillfället”. En enkätundersökning skulle ge mig ett större materialunderlag att arbeta med, men eventuellt en sämre kvalitet. Vid en enkätundersökning finns det nämligen begränsade möjligheter att ge förklaringar till respondenten om någon av frågorna verkar oklara, vilket jag ansåg vara av stor vikt för min undersökning.

Litteraturstudie föll bort då det inte finns någonting dokumenterat om medvetenheten kring säkerhetspolicys och riklinjer. Endast bakgrundsmaterial om säkerhetspolicys och ett BKS fanns tillgängligt i litteraturen. Detta innebar att metoden föll bort, eftersom det då inte var relevant att genomföra en litteraturstudie.

7 Genomförande och materialpresentation

I detta kapitel kommer jag att beskriva hur jag gått tillväga vid materialinsamlingen. Jag kommer att presentera hur jag gått tillväga för att skapa mitt frågeformulär, vilka erfarenheter jag fick av detta. Jag kommer även att presentera förberedelserna inför mina intervjuer och vilka erfarenheter jag fick av dessa. Slutligen kommer jag att värdera det insamlade materialet.

7.1 Förberedelser av frågeformulär

För att genomföra min undersökning skapade jag ett frågeformulär. Detta frågeformulär utformades med delvis helt öppna frågor och dels frågor med olika svarsalternativ, så att jag sedan lättare skulle kunna sammanställa och analysera de svar jag fått. Frågeformuläret är delvis helt strukturerat då vissa frågor har fasta svarsalternativ. Somliga frågor är öppna och graden av strukturering varierar därför beroende på hur frågan formulerats.

Det frågeformulär som jag tog fram använde jag till samtliga respondenter på vårdcentralerna. Jag ställde således samma frågor till samtliga respondenter och ställde frågorna i samma ordningsföljd till alla respondenter, detta för att få en struktur över intervjun. Detta innebär att intervjuerna som genomförts är helt standardiserade.

Frågeformuläret strukturerade jag i fyra olika kategorier, dels för att göra sammanställningen enklare och dels för att få en bra dialog med intervjupersonen. Frågeformuläret delades in i kategorierna, introduktion, personalens lösenordshantering, utbildning och åsikter kring behörighetskontrollsystemet med avseende på de säkerhetspolicys och riktlinjer som finns uppsatta och slutligen övriga frågor (se bilaga 2).

Jag valde att först börja intervjun med en introduktion för att få en mjuk start och lite grundläggande underlag om intervjupersonen. Frågorna var av allmän karaktär som berör yrke, ålder och kunskaper kring systemet. Frågan om respond entens yrke var relevant för att vid analysen kunna jämföra respondenternas svar. Detta för att se om svaren skiljer sig beroende på respondenternas arbetsuppgifter. Efter detta gick jag in på personalens lösenordshanteringen för att skapa mig en bild över personalens medvetenhet om vilka säkerhetsrutiner som gäller vid användningen av behörighetskontrollsystemet.

Därefter kunde jag ställa frågor om säkerhetspolicyn. Jag undersökte dels om personalen sett några dokument över säkerhetspolicyn och hur personalen i så fall tagit del utav denna. Frågorna som berörde utbildningen ställde jag för att få en förståelse kring hur ofta personalen får information om säkerhetspolicyn. Dessa frågor skulle även besvara om personalen var medveten om den säkerhetspolicy som finns för behörighetskontrollsystemet.

Erfarenheter

I efterhand tycker jag att det var relativt svårt att ta fram frågor som ger svar på det som är tänkt. Jag gjorde ingen ”testintervju” på frågorna, men upptäckte efter att ha bett en utomstående person att läsa igenom formuläret att det krävdes viss omarbetning av frågorna. Det krävdes en hel del arbete med skapandet av frågeformuläret innan jag var nöjd med resultatet av detta, och tyckte mig ha de frågor som jag trodde skulle ge mig svar på mitt problemområde. Efter första intervjun

redigerade jag lite i mitt frågeformulär, och flyttade om vissa frågor för att få intervjuerna att flyta på smidigare.

7.2 Urval av respondenter

Innan jag tog kontakt med föreståndarna på vårdcentralerna, bestämde jag mig för vilka respondenter jag ville genomföra min undersökning på. Jag bestämde mig för att försöka intervjua olika personalkategorier på vårdcentralerna. Detta gjorde jag för att då skulle kunna få en större spridning på svaren i min undersökning. Jag valde även att genomföra undersökningen på olika personalkategorier för att eventuellt se vart i organisationen det finns mer eller mindre medvetenhet kring säkerhetspolicyn.

Jag försökte att intervjua personer som var systemansvarig, distriktsläkare, distriktssköterska och undersköterska, på de vårdcentraler där det fanns möjlighet till att göra detta. Alla kategorier var dock inte tillgängliga på samtliga vårdcentraler och samma kategorier har därför inte intervjuats på alla vårdcentralerna.

Min undersökningsgrupp är relativt stor, 17 respondenter, då jag vill undersöka personalens medvetenhet. Jag ansåg att det var viktigt att få en stor undersökningsgrupp eftersom medvetenheten kanske skiljer sig beroende på vilka arbetsuppgifter personalen arbetar med. Det krävdes många intervjuer för att sedan kunna jämföra de svar jag fått fram.

7.3 Kontakt med vårdcentralerna

Jag hade bestämt mig för att genomföra min undersökning på några vårdcentraler inom Skövde kommun. Jag ansåg detta vara en intressant undersökningsgrupp då det florerar mycket integritetskänslig information inom vården, vilket kräver en säkerhetspolicy för behörighetskontrollsystemet.

Det första jag gjorde var att jag tog kontakt med föreståndaren på respektive vårdcentral då jag kortfattat beskrev syftet med min undersökning. Detta var det som var mest tidskrävdande av förberedelserna. Jag tillbringade en hel del tid vid telefonen innan jag fick tag på rätt person. När jag fick kontakt med föreståndaren bestämde vi tid för intervju, och samtidigt förklarade jag att jag ville intervjua olika personalkategorier för att på så sätt få en större spridning på svaren från respondenterna.

Jag fick mycket positiv respons från föreståndarna på vårdcentralerna, som var till stor hjälp med att ordna med vilka respondenter som skulle intervjuas på respektive vårdcentral. Det var alltså inga problem med att få tag i respondenterna eller att få dem att ställa upp på min undersökning.

7.4 Genomförande av intervjuer

Vid varje intervjutillfälle tog jag kontakt med föreståndaren på varje vårdcentral. Föreståndarna presenterade mig för de personer som jag skulle intervjua, för att intervjuerna skulle flyta på smidigt. Innan jag genomförde mina intervjuer började jag att kortfattat beskriva varför jag genomförde min undersökning (se bilaga 1), detta gjorde jag både i mina telefonintervjuer och i samtliga besöksintervjuer.

Intervjuerna genomförde jag genom att ställa samma frågor alla respondenter i en viss ordning. Genomförandet av intervjuerna gick bra och personalen hade inga större

problem med att besvara mina frågor. Jag fick förklara en del frågor, men annars upplevde jag inte att det var några problem.

7.4.1 Telefonintervjuer

Jag genomförde två telefonintervjuer, då det inte fanns någon möjlighet att träffa personalen på denna vårdcentral. Det resultat som jag fick från intervjuerna var något mindre uttömmande än de svar jag fick vid besöksintervjuerna, det material jag fick fram anser jag dock vara bra.

Erfarenheter

Telefonintervjuerna tyckte jag var något svårare att genomföra, det var stor skillnad jämfört med de besöksintervjuer jag gjorde. Vissa frågor som behövde förklaras och klargöras var svårare att förklara per telefon. Resultatet av telefonintervjuerna blev att respondenten gav mer kortfattade svar.

Det intryck jag fick av respondenterna var att det kändes som att personalen var mindre intresserade och motiverade av undersökningen. Det kändes som om respondenterna var stressande, och snabbt ville ha intervjun avklarad. Detta tror jag medförde att svaren från intervjuerna blev mindre uttömmande.

7.4.2 Besöksintervjuer

Besöksintervjuerna fungerade som jag tidigare beskrivit att jag blev presenterad för respondenterna av föreståndaren på respektive vårdcentral. Jag genomförde sedan tre eller fyra intervjuer vid ett och samma tillfälle på vårdcentralen. Intervjuerna genomfördes dock med en person i taget.

Erfarenheter

Jag tycker att jag har fått ett positivt bemötande vid besöksintervjuerna. Jag fick intrycket att respondenterna var intresserade av undersökningen och ställde utan några problem upp på intervjun. Besöksintervjuerna anser jag var mer givande än de telefonintervjuer som jag genomförde. Besöksintervjuerna tyckte jag gav mig ett mycket bra underlag att arbeta med, då jag anser mig ha fått de svar jag behöver.

Jag upplevde att det var enklare att ställa eventuella följdfrågor och motivationen och intresset för undersökningen verkade större. Ibland kunde jag dock känna att vissa respondenter kände sig stressade och ville genomföra intervjun på så kort tid som möjligt. Detta ledde till att vissa intervjuer inte blivit lika uttömmande som andra.

7.4.3 Värdering av insamlat material

Efter genomförd undersökning har jag fått in en stor kvantitet material, trots att jag gjorde besöksintervjuer. Detta tycker jag är mycket positivt och gör att jag kan komprimera det material jag fått in i form utav tabeller, för att få en övergripande bild och en helhet av samtliga vårdcentralers medvetenhet av säkerhetspolicyn.

Många av frågorna jag ställde gav korta svar, vilket gör att materialet var lättare att sammanställa och analysera, än det skulle varit vid t.ex. diskussionsfrågor. Materialet som jag tagit fram visar att många av respondenterna svarat mycket lika på många av frågorna, detta gör att trovärdigheten av materialet blir starkare.

Beroende på respondentens arbetsuppgifter och kunskaper inom området så varierar dock svaren på frågorna. Respondenter med större kunskaper inom området hade således mer information att tillföra undersökningsmaterialet. Jag anser att respondenterna kunde svara på mina frågor, och att jag fått de svar som krävs för att besvara min problemställning.

7.5 Kontakt med IT-enheten

Efter jag genomfört mina intervjuer, fick jag en del tips om att jag kunde ta kontakt med IT-enheten för vårdcentralerna inom Västra Götalandslän. Detta gjorde jag för att eventuellt få lite bakgrundsmaterial till den säkerhetspolicy och den information som går ut till vårdcentralerna. IT-enheten är de som underhåller vårdcentralernas system inom Västra Götalandslän. Samtalet gav mig lite information om säkerhetspolicyn, men inget som direkt kunde användas i mitt arbete.

7.6 Materialpresentation

I detta avsnitt kommer jag att presentera det material jag fått fram i min undersökning på de olika vårdcentralerna. Jag har sammanställt samtliga respondenters svar till en helhet för att på så sätt göra materialet tydligare och lättare att ta del av. Varje intervju är alltså inte representerad, utan finns presenterad i bilagor. Jag kunde ha presenterat varje vårdcentral för sig, men jag ansåg att många respondenter svarat likvärdigt och att det därför skulle bli mycket upprepningar i presentationerna av materialet.

7.6.1 Introduktion

Intervjuerna genomfördes på fem vårdcentraler i Skövde kommun, varav 17 personer intervjuades. Två av respondenterna var män och 15 stycken var kvinnor. Av samtliga respondenter var en under och resten över 35 år. På varje vårdcentral intervjuades en systemansvarig, övriga arbetade antingen som distriktsläkare, distriktssköterska, undersköterska, biomedicinsk analytiker eller läkarsekreterare.

Respondenterna använder behörighetskontrollsystemet en eller flera gånger dagligen beroende på vilken vårdcentral de arbetar på. De flesta respondenter anser att de vet vad syftet med behörighetskontrollsystemet innebär. I bild 1 åskådliggörs respondenternas svar på frågan om de vet vad syftet med behörighetskontrollsystemet är.

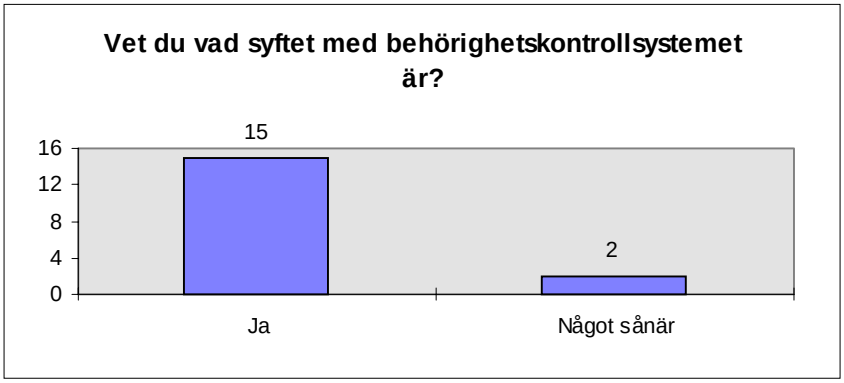

Bild 1. *Personalens vetskap om syftet med behörighetskontrollsystemet.*

De säkerhetsrutiner som finns för inloggningen av behörighetskontrollsystemet, anser sig större delen av personalen att de endast ibland tänker på vad det är som gäller. De

som svarat att de ibland tänker på säkerhetsrutinerna säger att de tänker på det bl.a. när man blir påmind om att byta lösenord.

Andra säger att det endast händer ibland eftersom inloggningen blivit en rutin. En av respondenterna som aldrig tänker på säkerhetsrutinerna säger att man alltid varit medveten om sekretessen och tystnadsplikten inom vården och att det nu inte är någon skillnad p.g.a. att allt blivit datoriserat (se bilaga 6).

Av de respondenter som säger att de alltid tänker på vilka säkerhetsrutiner som gäller svarar någon att det beror på att man är medveten om vilka rutiner som gäller och att man därför alltid tänker på det. I bild 2 presenteras respondenternas svar på hur ofta de tänker på säkerhetsrutinerna.

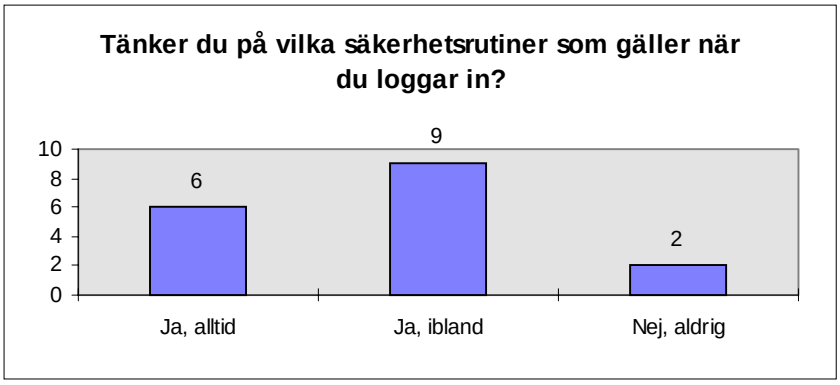

Bild 2. *Hur ofta personalen anser sig tänka på de säkerhetsrutiner som gäller vid inloggningen.*

Behörighetskontrollsystemet används för att skydda all information som vårdcentralerna hanterar, svarar större delen av respondenterna. Respondenterna säger att behörighetskontrollsystemet används till att skydda patientuppgifter, post och tidbokning. De flesta anser dock att det är patientjournalerna som är viktigast att skydda med behörighetskontrollsystemet.

Personalen på vårdcentralerna säger att de har tillgång till olika typer av information och program beroende på vilka arbetsuppgifter de har. Fyra av de systemansvariga hade tillgång till all information som hanteras inom vårdcentralens system. En av respondenterna som var dataadministratör för vårdcentral fyra, hade tillgång till den mesta informationen. Respondenten kunde dock inte skriva i allt p.g.a. att hon var distriktssköterska (se bilaga 6). Distriktsläkaren på vårdcentral ett som tidigare varit systemansvarig, säger att även han har tillgång till all information (se bilaga 3).

På vårdcentral tre säger två av respondenterna att det är beroende av personalens arbetsuppgifter som de har tillgång till viss information som finns på vårdcentralen, trots det har tre av de fyra respondenterna tillgång till all information. En av respondenterna på vårdcentral tre säger att alla har tillgång till all information. Detta beror på att vårdcentralen är så liten och skulle vara mycket sårbar om inte alla hade tillgång till all information (se bilaga 5). En svarade dock att hon endast hade tillgång till journalerna (se bilaga 5).

Undersköterskorna har inte tillgång till att skriva i journalerna, utan har endast tillgång till det som krävs för dennes arbetsuppgifter, bl.a. att läsa i patientjournalerna. De flesta av respondenterna säger att de har tillgång till patientjournalerna.

Den information som vissa respondenter inte har tillgång till framkommer även under intervjuerna. Det är t.ex. någon av respondenterna som inte har tillgång till psykiatrisköterskans journaler och att man inte har tillgång till medicinjournaler eller att signera recept (se bilaga 5).

Behörighetskontrollsystemet som personalen använder sig utav dagligen tycker de sig ha olika mycket kunskap om. I bild 3 presenteras respondenternas svar på hur stor kunskap de anser sig ha om systemet.

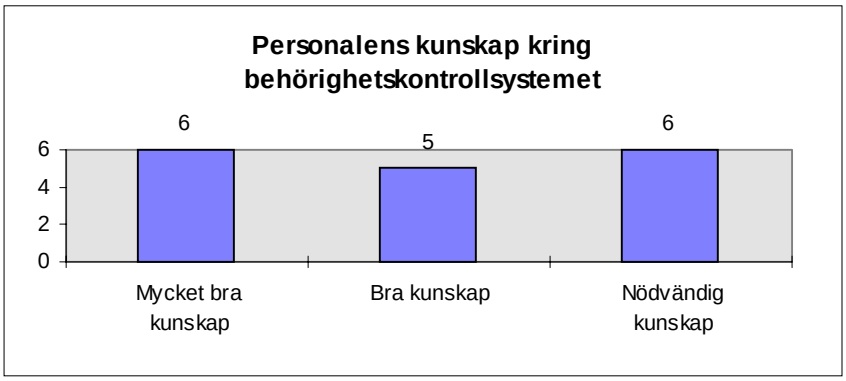

Bild 3. *Personalens kunskap kring behörighetskontrollsystemet*

7.6.2 Personalens lösenordshanteringen

Behörighetskontrollsystemet fungerar så att personalen blir tilldelad vissa rättigheter. De rättigheter de får visar vilken information och applikationer de får ha tillgång till i sitt arbete. Personalen på de olika vårdcentralerna anser att behörighetstilldelningen har fungerat bra eller mycket bra.

För att få tillgång till behörighetskontrollsystemet krävs det ett inloggningsnamn och lösenord (se bilaga 7). Personalen på vårdcentralerna anser att lösenordshanteringen fungerar bra eller mycket bra. Det är vissa problem vid nyanställning säger en respondent på vårdcentral två, detta brukar dock inte vara några problem då vårdcentralen är relativt liten (se bilaga 4). På vårdcentral fem säger systemansvarig att det endast är problem med lösenordshanteringen om någon anställd lagt in ett å,ä eller ett ö i sitt lösenord, då kan systemansvariga på vårdcentralen inte själva fixa detta utan måste ta kontakt med IT-enheten (se bilaga 7).

Lösenordshanteringen fungerar likadant i hela Västra Götalandslän säger distriktsläkaren på vårdcentral fem (se bilaga 7). Alla användare är unika i Västra Götaland och det är samma regler som gäller för samtliga vårdcentraler inom länet.

För att komma in i journalsystemet som personalen arbetar med krävs det två olika lösenord säger en respondent på vårdcentral två (se bilaga 4). Dessa lösenord måste bytas efter en viss tidsperiod, datorn meddelar då användaren automatiskt att det är dags att byta lösenord. Personalen kan även bli tvungen att byta lösenord utan att datorn säger ifrån, t.ex. om något problem uppstår och det inte går att logga in.

- 12 personer säger att lösenordsbyte sker var tredje månad.
- Två personer säger att lösenordsbyte sker var annan månad.
- Två personer säger att lösenordsbyte sker var sjätte månad.
- En person säger att man byter lösenord när datorn säger ifrån.

De lösenord som respondenterna använder, säger samtliga respondenter att de håller hemligt. Det är alltså ingen förutom respondenten själv som känner till vilket lösenord denne har.

Den lösenordshantering som administreras har respondenterna olika uppfattningar om vem det är som ansvarar för. De flesta anser att det är systemansvarig på vårdcentralen som ansvarar för detta eller IT-enheten. I bild 4 presenteras respondenternas svar på vem som de anser bär ansvaret för lösenordshanteringen. Två personer säger att det är både systemansvarig på vårdcentralen och IT-enhetens uppgift, därför är dessa placerade i båda staplarna.

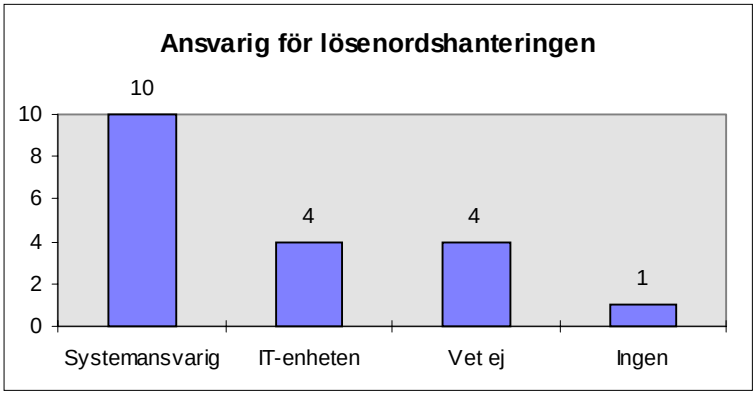

Bild 4. *Personalens uppfattning om vem som ansvarar för lösenordshanteringen.*

Respondenterna på vårdcentralerna anser att deras ansvar för att skydda känslig information så att den inte hamnar i orätta händer är följande:

- Använda skärmsläckare med lösenord, för att skydda informationen så att patienter inte kan ta del av informationen.
- Hålla lösenordet hemligt. På vårdcentralerna säger samtliga respondenter att det endast är de själva som känner till deras lösenord.
- Logga ur när de lämnar datorn utan uppsikt under en längre period.
- Låsa dörren om de lämnar datorn under en längre period.
- Byta skärmbild där det inte visas några känsliga uppgifter.
- Stänga ner datorn.
- Inte ha framme papper på skrivbordet som berör någon patient.

På vårdcentralerna har det enligt respondenterna inte förekommit att känslig information hamnat i orätta händer. Endast en av respondenterna säger sig ha hört att någon eventuellt fått tag i sådan information som kanske inte varit avsedd för denna person (se bilaga 5), men inte om det förekommit på dennes vårdcentral.

Distriktsläkaren på vårdcentral ett nämnde att det var lättare att information hamnade i orätta händer tidigare då allt inte var datoriserat. Då sköttes allt manuellt och vem som helst kunde ta del av information som låg framme på skrivbordet (se bilaga 3).

7.6.3 Utbildning och åsikter om behörighetskontrollsystemet

Personalen tycker att det är lätt att använda behörighetskontrollsystemet, det är endast en på vårdcentral ett (se bilaga 3) som tycker att behörighetskontrollsystemet kan vara lite besvärligt eftersom det är många olika lösenord som man måste hålla reda på. Denna respondent anser att det tar lite tid varje gång man loggar in och tycker att det skulle kunna finnas enklare sätt att använda ett inloggningssystem. Det är för övrigt tre andra respondenter som även de tycker att inloggningen tar lång tid.

Respondenterna säger att de brukar lämna sina datorer utan uppsikt om de är inloggade. Det är endast två stycken som inte gör det, en distriktssköterska och personen som var biomedicinsk analytiker. Om respondenterna lämnar datorn utan uppsikt har de olika sätt att försöka skydda informationen. Olika sätt att skydda informationen är att logga ur, låsa dörren eller så skyddas informationen med hjälp av att skärmsläckaren sätts igång. Det är många av respondenterna som nämner att skärmsläckaren går igång och att det då krävs lösenord för att komma åt informationen igen. Det är dock inte alla respondenter som har lösenord på sina skärmsläckare.

På vårdcentralerna finns datorerna placerade inne i personalens expeditioner, på vissa vårdcentraler finns det även datorer i labbrummen. Respondenterna säger att det brukar finnas patienter i många av de rum där datorerna är placerade. På vårdcentral fem finns det inga datorer inne i undersökningsrummen (se bilaga 7). Sex av respondenterna svarar att det inte brukar finnas patienter i deras arbetsrum.

Om det finns patienter närvarande i rummen där det finns datorer, säger några respondenter att man brukar skydda informationen genom att ha en bild på skärmen som inte visar någon känslig information som patienten inte bör ta del av. På vårdcentral tre säger en av respondenterna att patienterna aldrig lämnas ensamma med datorn (se bilaga 5). Enligt en respondent på vårdcentral ett (se bilaga 3) används även skärmsläckackaren som skydd av informationen.

Den säkerhetspolicy som finns dokumenterad för användningen av behörighetskontrollsystemet är det endast fem stycken som tagit del utav. I bild 5 nedan åskådliggörs respondenternas svar på frågan om de sett någon säkerhetspolicy.

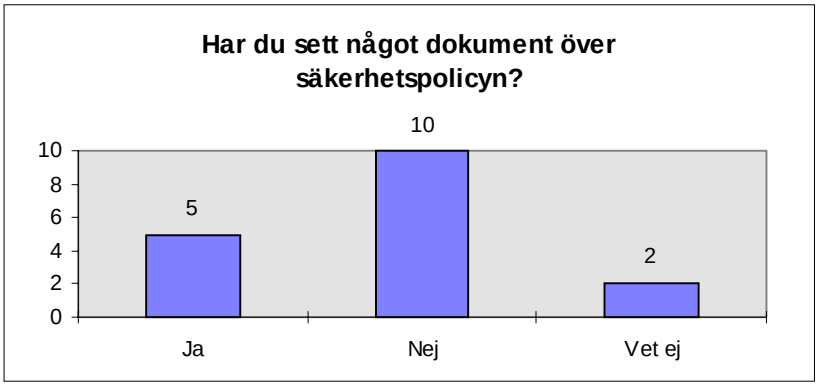

Bild 5. *Om personalen sett dokument över säkerhetspolicyn.*

De fem personer som tagit del utav säkerhetspolicyn är de personer som är systemansvariga på respektive vårdcentral. Övriga respondenter vet inte om de sett något dokument eller så vet de med säkerhet att de inte sett något. En av de systemansvariga ansåg att detta dokument var svårt att förstå och ta del av medan övriga som sett dokumentet ansåg att det var lätt att förstå och ta del av.

Om personalen fått någon utbildning eller information om säkerhetspolicyn är det inte många repondenter som kan besvara. Det är endast de systemansvariga som säger att de fått någon sorts utbildning eller information vad gäller säkerhetspolicyn.

Det finns även respondenter som fått annan utbildning och information, men detta gällde då inte säkerhetspolicyn utan endast de säkerhetsrutiner som finns för att på bästa sätt skydda informationen som finns datoriserad. De systemansvariga har tagit del av säkerhetspolicyn genom:

- Skriftlig information i form utav t.ex. informationsblad.
- Muntlig information.
- Utbildning.
- Informationshäfte.

Flera av respondenterna ansåg att personalen inte fick särskilt mycket information och utbildning överhuvudtaget. En respondent på vårdcentral tre (se bilaga 5) säger att personalen inte ens får utbildning en gång om året. Några säger att det sker vid förändring, t.ex. har personalen fått utbildning av det nya system som installerats på flera av vårdcentralerna.

I utbildningen av det nya systemet på vårdcentralerna ingick även säkerhetsutbildning säger några respondenter, men inte någonting om säkerhetspolicys. Om det är något som personalen undrar över säger en av respondenterna på vårdcentral två (se bilaga 4) att det går att ringa till supportavdelningen, IT-enheten, för att få svar på sina frågor.

På vårdcentralerna i Skövde kommun anser personalen att det är viktigt med utbildning kring säkerhetspolicyn. Detta tycker personalen eftersom:

- det är viktigt att veta syftet med behörighetskontrollsystemet, och vilka konsekvenser det kan innebära om något görs felaktigt i systemet.
- det är viktigt att hålla sig ajour med det som händer, det händer ju hela tiden nya saker.
- det är viktigt att lära sig och veta vad man ska hålla reda på.
- det är viktigt att bli påmind om säkerheten och säkerhetspolicyn eftersom det har blivit en vardag för personalen.
- det är viktigt att sjukvårdspersonal är medveten om sekretessen.
- det är roligt att lära sig nytt.
- det är alltid viktigt, men speciellt viktigt är det vid nyanställning.
- man blir effektivare som användare.
- det gör att personalen känner sig tryggare i sitt arbete.

Vem det är som ansvarar för att sprida information om säkerhetspolicyn är respondenterna inte helt överrens om. Respondenterna säger att det är IT-enheten, systemansvarig på vårdcentralen eller så vet de inte. I bild 6 nedan presenteras respondenternas svar på vem de anser ansvarar för att sprida information kring säkerhetspolicyn.

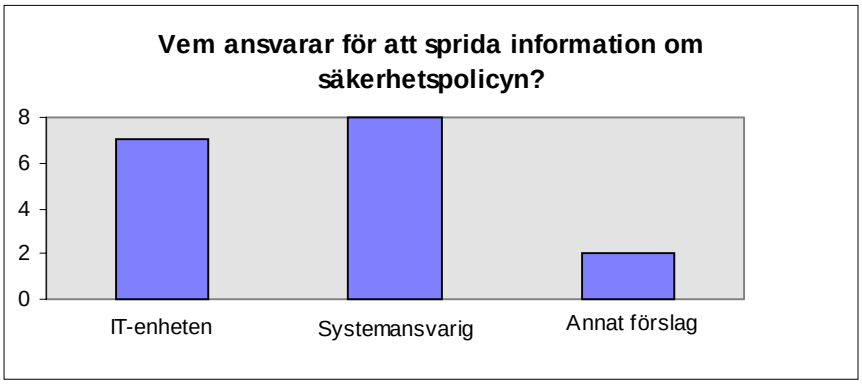

Bild 6. *Personalens uppfattning om vem som ansvarar för information och utbildning kring säkerhetspolicyn.*

På frågan om personalen vet om det finns något uppföljningssystem som kontrollerar att personalen efterlever de säkerhetspolicys och riktlinjer som finns, är det fyra stycken som säger att det finns. I bild 7 åskådliggörs personalens svar på detta.

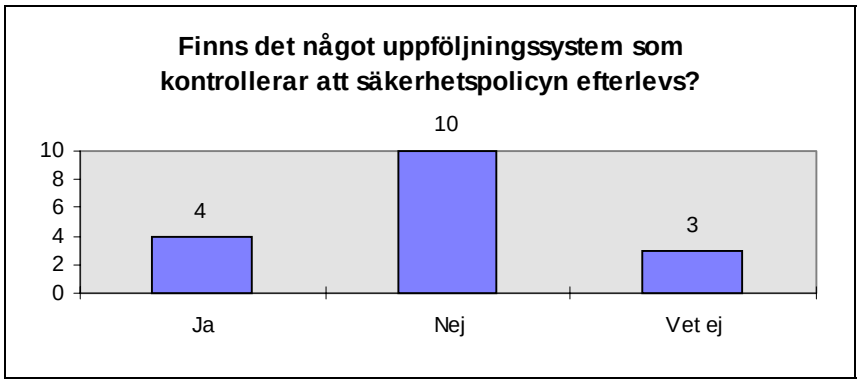

Bild 7. *Personalens uppfattning om det finns något uppföljningssystem av säkerhetspolicyn.*

Två respondenter på vårdcentral ett (se bilaga 3) säger att det inte behövs då det inte går att komma förbi systemet eftersom det krävs dubbla lösenord för att komma in i systemet. En respondent på vårdcentral fem (se bilaga 7) säger att det inte finns något uppföljningssystem eftersom det är svårt att kontrollera sådana saker som att någon anställd lämnar sitt rum i flera timmar med olåst dörr.

Systemansvarig på vårdcentral fem säger att det tidigare gick att kontrollera vem som varit inne i vilka journaler, vid en viss tidpunkt men trodde inte att det gick att göra längre (se bilaga 7). Distriktsläkaren på vårdcentral ett säger dock att detta går att kontrollera, och att säkerheten att skydda informationen därför är bättre än den varit tidigare då allt sköttes manuellt (se bilaga 3). En av respondenterna som säger att det finns, säger att det inte sker kontinuerligt utan att det är deras dataansvarige som kontrollerar att personalen gör som de ska.

7.6.4 Övrigt

Medvetenheten hos personalen vad gäller säkerhetspolicys anser personalen skulle kunna förbättras genom:

- mer utbildning och information.
- att prata mer inom personalen.

- ta upp detta på arbetsplatsgruppmötena.
- ta upp det som en mer naturlig del i arbetet.

Ett par av respondenterna tror att medvetenheten vad gäller säkerhetsarbetet är bättre i en mindre organisation. En av respondenterna på vårdcentral två säger att det finns större brister i en större organisation exempelvis på sjukhus (se bilaga 4).

Säkerheten är inbyggd inom vården, vilket är viktigt eftersom personliga uppgifter inte får hamna i orätta händer säger en respondent på vårdcentral ett (se bilaga 3). I andra verksamheter kan däremot ett behörighetskontrollsystem antagligen uppfattas som svårt och onödigt säger respondenten (se bilaga 3).

På vårdcentral tre (se bilaga 3) säger en respondent att det finns mycket att förbättra inom detta område. De flesta respondenter är eniga om att det krävs mer utbildning och information för att öka medvetenheten.

7.7 Information från IT-enheten

Jag genomförde ingen intervju med personalen på IT-enheten, utan hade endast ett samtal med en person som var ansvarig för vårdcentralernas säkerhetspolicy. Jag ansåg att detta var tillräckligt då jag endast ville ha bekräftat information om säkerhetspolicyn.

Respondenten jag pratade med gav mig uppgifter om vilken information som går ut till vårdcentralerna. Respondenten berättade att den information som vidarebefordrades till vårdcentralerna, gick via ansvarig på IT-enheten till systemansvarig på respektive vårdcentral.

Den information som förmedlades till vårdcentralerna var bl.a. information om inloggningen och lösenordshanteringen. Jag fick bekräftelse på att byte av lösenord sker var tredje månad. Lösenorden som personalen på vårdcentralerna använder sig utav kan inte återanvändas. Vid varje lösenordsbyte måste personalen hitta på nya lösenord till båda systemen som kräver lösenord.

Respondenten klargjorde att det inte fanns något dokument över någon säkerhetspolicy som var relevant i nuläget. En ny säkerhetspolicy höll på att utvecklas, som skall komma att gälla för samtliga vårdcentraler inom Västra Götalandslän. Samtliga vårdcentraler håller på att bli en enhet och skall ha samma regler för behörighetskontrollsystemet, säger respondenten.

8 Analys

I detta avsnitt kommer jag att analysera det material som jag presenterat i föregående avsnitt, materialpresentation kap 7.6. Jag kommer att behandla detta material med avseende på problemställningen.

8.1 Personalens grundläggande kunskaper

De neutrala frågorna som jag klassificererat som inledande frågor i mina intervjuer, ställde jag för att sedan kunna analysera mitt material och eventuellt kunna göra jämförelser av svaren beroende på vilka arbetsuppgifter, ålder och kön som respondenterna hade.

-Ålder, kön och yrke.

Utifrån min undersökning tyder svaren på att större delen av personalen på vårdcentralerna är över 35 år och att de flesta är kvinnor, då endast två av de tillfrågade var män. Detta verkar dock inte ha någon avgörande roll för resultatet av undersökningen och därför kommer materialet inte att analyseras utifrån respondenternas ålder. Undersökningen visar att svaren varierar en del beroende på respondentens arbetsuppgifter. Det tyder på att systemansvariga på respektive vårdcentral och de två män som intervjuats har störst kunskap om behörighetskontrollsystemet.

Det pekar mot att svaren och kunskaperna inte skiljer sig nämnvärt beroende på om respondenten är undersköterska eller distriktssköterska. Jag anser inte heller att svaren skiljer sig beroende på vilken vårdcentral som respondenterna arbetar på.

-Vet du vad syftet med ett behörighetskontrollsystemet är?

-Hur ofta använder du behörighetskontrollsystemet?

Jag anser att personalen som intervjuades verkar veta vad syftet med ett behörighetskontrollsystem är, eftersom endast två stycken sade sig ha något sånär mycket vetskap om det. Jag ställde denna fråga för att kunna förklara syftet med behörighetskontrollsystemet för respondenten, om denne inte hade någon vetskap om detta.

På frågan om hur ofta personalen använder behörighetskontrollsystemet tyder respondenternas svar på att systemet används dagligen eller flera gånger dagligen, beroende på vilken vårdcentral de arbetar på. Svaren pekar mot att personalen inte använder systemet olika ofta beroende på vilka arbetsuppgifter de har.

-Tänker du på vilka säkerhetsrutiner som gäller när du sköter din inloggning?

Jag ansåg det vara relevant att undersöka personalens medvetenhet kring de vardagliga säkerhetsrutinerna, vid användning av behörighetskontrollsystemet. Detta ansåg jag skulle kunna visa att personalen kanske har medvetenhet kring den vardagliga säkerheten, trots att de kanske inte tagit del av säkerhetspolicyn.

Det verkar som om personalen inte alltid tänker på vilka säkerhetsrutiner som gäller vid inloggningen, större delen tänker endast på detta ibland. Beroende på om respondenterna är systemansvariga eller ej, tyder svaren på att detta inte gör någon skillnad. Tre av respondenterna som alltid tänker på vilka säkerhetsrutiner som gäller

är systemansvariga, en systemansvarig säger sig aldrig tänka på vilka rutiner som gäller.

-Vilken information kräver skydd, vilken information har du tillgång till, har personalen olika behörigheter?

Jag ansåg att det var av stor vikt att undersöka vilken kunskap och medvetenhet personalen hade angående vilken information som kräver skydd och vilken information de olika respondenterna hade tillgång till. Detta skulle då ge mig en bild av personalens medvetenhet kring behörighetstilldelningen.

Svaren på dessa frågor pekar mot att personalen på vårdcentralerna anser att i stort sett all information på vårdcentralernas datorer kräver skydd och olika behörigheter. Utifrån de svar jag fått pekar det främst mot att det är patientbunden information som kräver mest skydd, men även uppgifter som tidbokning och labblistor, som används i deras arbetsuppgifter kräver skydd och olika behörigheter. Det tyder på att respondentens arbetsuppgifter inte har någon avgörande roll i dessa svar.

Materialet visar att det tyder på att olika personal har olika rättigheter till olika program och applikationer beroende på deras arbetsuppgifter. Alla respondenter anser att varje anställd har olika rättigheter som finns uppsatta i systemet, vilket tyder på att personalen är medveten om att alla i personalen inte har tillgång till all information i systemet.

Svaren från systemansvariga tyder på att de har tillgång till all information inklusive viss lösenordshantering medan övriga respondenter endast har tillgång till t.ex. kassan eller patientuppgifter. Svaren pekar dessutom mot att undersköterskorna inte har några rättigheter att skriva i journalerna, utan endast har rättigheter att läsa dessa.

-Vad anser du dig ha för kunskap om hur behörighetskontrollsystemet fungerar?

Eftersom behörighetskontrollsystemet används av hela personalen i så stor utsträckning verkar det som om de flesta anser sig ha bra eller mycket bra kunskap kring systemet. Det insamlade materialet tyder på att männen tycker sig ha mycket bra kunskap om systemet. Undersökningen pekar mot att undersköterskorna endast anser sig ha nödvändig kunskap om behörighetskontrollsystemet, medan det är en större spridning på svaren från distriktssköterskorna. Distriktssköterskornas svar varierar mellan mycket bra kunskap och nödvändig kunskap. Det pekar mot att de systemansvariga på vårdcentralerna tycker sig ha bra kunskap, då det endast är två systemansvariga som anser sig ha mycket bra kunskap.

8.2 Behörighetstilldelning och lösenordshantering

Frågorna kring lösenordshanteringen och behörighetstilldelningen ställde jag för att skapa mig en bild av personalens uppfattning om systemet och hur de ansåg att tilldelningen fungerat.

-Hur tycker du att behörighetstilldelningen fungerade?

-Hur tycker du att lösenordshanteringen fungerar?

Då respondenterna blev tilldelade den behörighet de har, tyder de svar jag fått på att de tyckte att detta fungerat bra eller mycket bra. Detta tyder på att det inte finns någon som uppfattat att detta varit några problem.

Den lösenordshantering som krävs för att använda behörighetskontrollsystemet ansåg samtliga respondenter fungerar bra eller mycket bra. Problem och krångel med lösenordshanteringen kan dock förekomma, det tyder de svar som framkom under vissa intervjuer med de systemansvariga på vårdcentralerna. Övriga respondenter som undersköterskorna och distriktssköterskorna verkar inte se några problem med lösenordshanteringen.

8.3 Personalens medvetenhet kring lösenordshanteringen

Jag tog med frågorna kring lösenordshanteringen i mina intervjuer för att få material kring personalens medvetenhet om detta. Lösenordshanteringen är en stor del av inloggningssystemet och måste fungera tillfredsställande för att kunna skydda känslig information. Frågorna ger mig inte svar på om personalen är medveten om säkerhetspolicyn, utan mer om medvetenheten kring det vardagliga säkerhetsarbetet.

-Är det någon mer än du som känner till ditt lösenord?

-Hur ofta byter du ditt lösenord?

-Finns det någon som ansvarar för lösenordshanteringen, i så fall vem?

Lösenordshanteringen verkar fungera likvärdigt på samtliga vårdcentraler, det finns dock olika svar på hur ofta personalen byter ut sina lösenord. Det verkar inte vara någon skillnad på svaren beroende på vilken vårdcentral som respondenterna arbetar på. Materialet tyder på att byte av lösenord sker var tredje månad, då datorn automatiskt säger ifrån att det är dags att byta. Detta eftersom majoriteten av respondenterna anser det. Materialet pekar mot att personalen har medvetenhet kring hur ofta lösenorden skall bytas, då uppgifter från IT-enheten bekräftar detta.

Personalen på vårdcentralerna verkar alla vara överrens om att det inte finns någon mer än de själva som känner till deras lösenord. Detta pekar mot att det finns stor medvetenhet om att lösenorden inte skall komma i orätta händer, vilket skulle kunna innebära att information kommer till skada eller att information hamnar i orätta händer och skadar någon patients integritet.

De som ansvarar för och hanterar lösenorden, exempelvis byte av lösenord vid eventuella inloggnings problem är det enligt samtliga systemansvariga och tre andra respondenter på vårdcentralerna, IT-enheten som sköter. Vilket tyder på att de systemansvariga anser detta var IT-enhetens uppgift, medan majoriteten av respondenterna anser detta vara systemansvariges uppgift. Det pekar mot att detta är riktigt, eftersom IT-enheten bekräftar att de endast ger information kring lösenordshanteringen till de systemansvariga på vårdcentralerna.

De flesta respondenter ansåg att det var systemansvarig på vårdcentralen som ansvarar för detta, vilket jag tycker pekar mot att information om lösenordshanteringen kommer personalen tillhanda på olika sätt, dels från IT-enheten och dels från systemansvarig på respektive vårdcentral. Av de som ansåg att det var systemansvariga som ansvarar för lösenordshanteringen var det stor spridning bland respondenterna, det var bl.a. systemansvariga, distriktsläkare och undersköterskor som ansåg detta.

-Vad tycker du är ditt ansvar för att obehöriga inte skall få tillgång till känslig information?

-Har det förekommit på denna vårdcentralen att information hamnat i orätta händer, i så fall vilken typ av information var det?

För att kontrollera om personalen på vårdcentralerna är medvetna om att skydda känslig information ställde jag frågan om vad personalen anser vara deras ansvar för att skydda känslig information. Jag ansåg det även vara intressant att ta reda på om personalen känner till om det förekommit att information på vårdcentralen kommit i orätta händer.

Personalen hade en rad olika förslag på vad deras ansvar var när det gällde att skydda känslig information, t.ex. patientuppgifter. Svaren jag fick tyder på att personalen känner ett ansvar att skydda den information som de hanterar.

- Materialet tyder på att personalen tycker det är viktigt att ingen annan har kännedom om dennes lösenord, vilket är ett sätt att skydda information så att ingen utomstående kan ta del av den.
- Materialet tyder på att många använder sig utav skärmsläckare för att skydda informationen. Det tyder även på att många i personalen hade en skärmsläckare som krävde lösenord.

Utifrån de svar jag fick tyder det på att de flesta i personalen försöker så gott det går att skydda informationen genom skärmsläckare, eller genom att helt enkelt försöka undvika att det finns några patientuppgifter på skärmen.

På vårdcentralerna inom Skövde kommun, tyder de svar jag fått på att det inte förekommit att information hamnat i orätta händer, eftersom ingen av de tillfrågade hade någon vetskap om det förekommit på deras vårdcentral.

-Brukar du lämna din dator utan uppsikt om du är inloggad?

-Hur är datorerna placerade på vårdcentralerna, finns det patienter i rummen med datorer?

Ovanstående frågor ställde jag för att se hur säkerhetsmedveten personalen är. Jag ansåg det vara intressant att kontrollera ifall personalen kan genomföra säkerhetsarbetet som det är tänkt teoretiskt sätt, i praktiken.

Om personalen tänker på vilken säkerhetspolicy som gäller är det befogat att personalen inte lämnar datorn utan uppsikt om de är inloggade. Hur datorerna är placerade på vårdcentralerna kan vara av stor vikt för att se hur medvetna personalen är att patienter inte bör ta del utav information som inte berör dem.

Personalen ansåg att deras ansvar för att skydda känslig information dels var att använda lösenord och skärmsläckare då de lämnar datorn. Trots det så brukar de flesta respondenter lämna sin dator utan uppsikt. Detta anser jag tyder på att det inte alltid går att genomföra säkerhetsarbetet såsom det är tänkt rent teoretiskt, i praktiken.

Materialet tyder på att det brukar finnas patienter i de flesta av respondenternas rum där datorerna är placerade. Om det finns patienter i rummet säger några respondenter att informationen skyddas genom att visa en bild på skärmen som inte visar någon känslig information eller att ha igång skärmsläckaren. Detta tyder på att personalen är medveten om att försöka skydda informationen i den mån som detta går.

8.4 Personalens åsikter om utbildning kring säkerhetspolicyn

Användningen av behörighetskontrollsystemet och utbildning av detta med avseende på de säkerhetspolicys som finns var en viktig del av min undersökning. Jag tänkte att personalen kunde ge mig materialunderlag om hur ofta de får utbildning och information kring säkerhetspolicys och om de tagit del utav något dokument över säkerhetspolicyn. Detta skulle ge mig svar på om det finns någon medvetenhet hos personalen kring säkerhetspolicys vid användning av behörighetskontrollsystemet.

-Hur uppfattar du att användningen av behörighetskontrollsystemet fungerar?

Denna fråga ställde jag för att se om personalen uppfattade behörighetskontrollsystemet som positivt eller krångligt och svårt. Om personalen anser att det är svårt och krångligt att använda systemet skulle detta eventuellt kunna medföra att personalen försöker kringgå systemet. Detta skulle eventuellt minska säkerhetsarbetet att skydda känslig information.

Tidigare presenterade jag att materialet tyder på att personalen använder sig utav behörighetskontrollsystemet dagligen, vilket medför att det är viktigt att personalen är medveten om hur viktigt det är att använda systemet på det sätt som är tänkt.

Samtliga tillfrågade ansåg att behörighetskontrollsystemet var lätt att använda, vilket tyder på att det inte brukar uppstå några problem vid inloggningen och att personalen därför inte heller försöker kringgå systemet.

Svaren från ett par respondenter tyder dock på att inloggningen tar tid och kan vara lite besvärligt eftersom det är många lösenord att hålla reda på. Detta anser jag tyder på att systemet skulle kunna förbättras, vilket även en respondent på vårdcentral ett anser.

-Har du sett något dokument över hur säkerhetspolicyn ser ut för behörighetskontrollsystemet?

-Tyckte du att säkerhetspolicyn var lätt att förstå eller svår att förstå och ta del av?

Om personalen sett något dokument över säkerhetspolicyn är viktigt för min undersökning, då detta till viss del besvarar om personalen är medveten om denna och vet vad den innehåller.

Av de tillfrågade är det endast systemansvarig på respektive vårdcentral som tagit del av dokumenterade säkerhetspolicys, vilket tyder på att övrig personal inte fått någon skriftlig information vad gäller säkerhetspolicyn för behörighetskontrollsystemet.

De systemansvariga som tagit del av och sett säkerhetspolicyn, tyder materialet på att denna var enkel att förstå. Endast en av de systemansvariga ansåg att säkerhetspolicyn var svår att förstå och ta del av. Många av respondenterna hade tagit del av utbildning och information kring säkerhetsrutiner, men inte någonting om säkerhetspolicyn. Materialet som tagits fram tyder på att den utbildning och information som personalen får, behandlar endast de vardagliga säkerhetsrutinerna och inte någonting som rör säkerhetspolicyn för behörighetskontrollsystemet.

-Har du fått någon information kring säkerhetspolicys och riktlinjer kring behörighetskontrollsystemet och hur tog du del av informationen?

Om personalen tagit del utav säkerhetspolicyn tyckte jag det kunde vara intressant att ta reda på varifrån denna information kommit. Jag tyckte även att det var viktigt att ta reda på hur ofta personalen tog del av information eller utbildning av säkerhetspolicyn, därför ansåg jag det relevant att ställa ovanstående fråga.

Materialet tyder på att det går ut för lite information och utbildning till personalen kring säkerhetspolicyn. Detta anser jag eftersom det endast är de systemansvariga på respektive vårdcentral som tagit del av utbildning och information kring säkerhetspolicyn. Eftersom övriga personalkategorier inte har tagit del av någon information om säkerhetspolicyn, tyder detta på att det inte finns någon medvetenhet av säkerhetspolicyn hos dessa personalkategorier på vårdcentralerna.

-Hur ofta ges utbildning eller information kring säkerhetspolicys och riktlinjer vad gäller behörighetskontrollsystemet?

Enligt respondenterna svar på om hur ofta de får utbildning om säkerhetspolicys tyder det på att det inte ges någon information om detta. Det pekar dessutom mot att det inte ges särskilt mycket information och utbildning överhuvudtaget på de olika vårdcentralerna inom Skövde kommun. Det är några av respondenterna som anser att de får utbildning om det sker någon förändring på vårdcentralen, dessa svar tyder på att det inte görs några större förändringar inom vårdcentralerna och därmed får de heller ingen utbildning.

Många av respondenterna säger att de nyligen fått utbildning eftersom de installerat ett nytt system, profdoc. Några respondenter trodde att det där ingick utbildning även kring hur säkerheten skall skötas. Det verkar som om personalen endast fått information om de säkerhetsrutiner som gäller för lösenordshanteringen och vardagliga säkerhetsrutiner och ingenting om säkerhetspolicyn.

-Tycker du att det är viktigt med utbildning kring behörigheten, om ja varför?

Dessa frågor var relevanta för min undersökning för att ta reda på om personalen är intresserade av utbildning kring säkerhetspolicys av behörighetskontrollsystemet.

Det tyder på att personalen på vårdcentralerna anser att det är viktigt med utbildning. De svar jag fått säger att utbildning är viktigt bl.a. eftersom det gör att personalen blir effektivare som användare, gör att personalen känner sig tryggare i sitt arbete om man vet vad man gör, det är viktigt att hålla sig ajour med säkerhetsarbetet och att det är roligt att lära sig nya saker. Detta anser jag pekar mot att personalen på vårdcentralerna tycker att det är viktigt med utbildning. Materialet tyder på att personalen vill ha mer utbildning, och att det finns ett intresse hos personalen att utbilda sig kring säkerhetspolicys vad gäller behörighetskontrollsystemet.

-Vem ansvarar för att sprida information kring säkerhetspolicys och riktlinjer?

Det kunde även vara intressant att se om personalen vet vem det är som ansvarar för att sprida informationen kring säkerhetspolicys för behörighetskontrollsystemet.

Sju av respondenterna tror att det är IT-enheten som ansvarar för att sprida information som behandlar säkerhetspolicyn. Det tyder på att personalen har en aning om vem det är som ansvarar för att sprida informationen, trots att de säger att de inte fått någon information om detta. Enligt de svar jag fått fram, anser 8 stycken att detta är systemansvariges uppgift och två stycken har gett andra förslag. Av de sju som säger att det är IT-enhetens ansvar, är fem av dem systemansvariga.

Detta tyder på att personalen har olika uppfattning om vems ansvar det är att sprida informationen kring säkerhetspolicys och riktlinjer. Svaren tyder på att personalen anser ansvaret ligga hos olika personer, beroende på vilka arbetsuppgifter respondenten har. Det verkar som att svaren varierar beroende på om man är systemansvarig eller befinner sig inom någon av de övriga personalkategorierna, distriktsköterska, undersköterska etc.

-Finns det något uppföljningssystem som kontrollerar att personalen efterlever den säkerhetspolicy som finns?

Det pekar mot att det inte finns något uppföljningssystem, eftersom majoriteten av respondenterna säger att det inte finns. Någon säger dock att det finns en kontrollfunktion i vårdcentralens system, där det går att kontrollera vem som varit inne i vilken journal och vid vilken tidpunkt detta var. Detta anser jag tyder på att det finns någon sorts uppföljningssystem inbyggt i vårdcentralernas system.

8.5 Förbättring av medvetenheten kring säkerhetspolicyn

-Hur anser du att medvetenheten om säkerhetspolicys kan bli bättre hos personalen?

Svaren tyder på att personalen anser att medvetenheten kring säkerhetspolicys, vad gäller behörighetskontrollsystemet, skulle kunna ökas genom att de får mer information och utbildning. Respondenterna säger även att de skulle prata mer på arbetsplatsgruppmötena.

9 Resultat och slutsatser

I detta avsnitt kommer jag att presentera det resultat och de slutsatser jag kommit fram till i mitt examensarbete, map den problemformulering som presenterades i kap 5. Jag kommer att ge en helhetsbild av det område som jag undersökt.

9.1 Personalens kunskaper om behörighetskontrollsystemet

Kunskaper om behörighetskontrollsystemet är nödvändigt för att personalen skall ha möjlighet att skydda känslig information på ett tillfredsställande sätt. Utifrån det material som presenterats drar jag slutsatserna att personalen på vårdcentralerna har tillräcklig kunskap om behörighetskontrollsystemet (BKS) och skyddar informationen i den mån det går. Materialet visar också att personalen på vårdcentralerna är medvetna om vilket syfte behörighetskontrollsystemet har, vilket är viktigt för att det ska finnas någon medvetenhet kring säkerhetspolicyn och riktlinjerna för systemet.

Personalens kunskaper om behörighetskontrollsystemet varierar beroende på vilka arbetsuppgifter de har. De systemansvariga har därmed mer kunskap och mer information att ge om behörighetskontrollsystemet, medan distriktssköterskor och undersköterskor endast tagit till sig den kunskap som krävs för att behärska sina arbetsuppgifter. Distriktssköterskorna och undersköterskorna har således endast nödvändig kunskap om behörighetskontrollsystemet.

9.2 Medvetenheten kring lösenordshanteringen

Behörighetskontrollsystemet (BKS) används dagligen på vårdcentralerna. Lösenordshanteringen är därför en central del av BKS, varför det är viktigt att personalen kan hantera sina lösenord. För att sköta arbetsuppgifterna som finns på vårdcentralerna krävs det att personalen behärskar lösenordshanteringen för BKS. Detta eftersom lösenordshanteringen är en del av personalens vardagliga arbetsuppgifter. Kunskapen om lösenordshanteringen är central inom verksamheten eftersom detta medför att det är viktigt att personalen är medvetna om vilka konsekvenser systemet kan medföra om säkerhetsarbetet inte efterlevs. Enligt uppgifter från det insamlade materialet kan jag dra slutsatsen att personalen har god kunskap om lösenordshanteringen och behärskar denna på ett tillräckligt sätt för att sköta sina arbetsuppgifter. Detta trots att personalen inte tagit del av säkerhetspolicyn.

9.3 Medvetenheten kring säkerhetspolicys och riktlinjer

Resultatet av undersökningen visar att det inte finns någon medvetenhet kring säkerhetspolicys och riktlinjer, hos större delen av personalen på vårdcentralerna. Det är endast de systemansvariga på respektive vårdcentral som är medvetna om att det finns en säkerhetspolicy, och har tagit del av denna. Personalen på vårdcentralerna har dock god kunskap och medvetenhet kring det vardagliga säkerhetsarbetet, då detta ingår i deras vardagliga arbetsuppgifter.

Information från systemansvariga om säkerhetspolicys och riktlinjer har inte förmedlats till övrig personal. Mer utbildning och information till personalen skulle kunna öka medvetenheten kring säkerhetspolicys och riktlinjer, och därmed även öka engagemanget i personalens säkerhetsarbete.

10 Diskussion

Efter att ha genomfört detta examensarbete har jag erhållit en del värdefulla erfarenheter. De erfarenheter jag fått kommer jag att presentera i detta avsnitt.

10.1 Erfarenheter

Genom att göra en intervjuundersökning för insamling av material har jag erhållit en del erfarenheter. De erfarenheter jag erhållit genom denna arbetsprocess kommer jag därför att presentera i nedanstående avsnitt.

Intervjuer

Intervjuundersökningen var en central del av mitt arbete, som också var nödvändig för att besvara min problemställning. Jag anser att undersökningen gav mig det underlag som krävdes, för att besvara min problemställning.

Undersökningen som genomfördes var relativt omfattande, d.v.s. det var många intervjuer trots att jag gjorde besöksintervjuer som är en ganska tidskrävande undersökningsmetod. Detta medför att slutsatserna jag dragit är mer trovärdiga och säkrare, eftersom många av respondenterna gav likvärdiga svar. Vid en mindre undersökningsgrupp skulle det nog vara svårare att generalisera svaren vad gäller medvetenheten.

Jag anser fortfarande att intervjuer var den bästa metoden för att besvara min problemställning, då det inte finns någonting dokumenterat om personalens medvetenhet kring säkerhetspolicys och riktlinjer.

Frågeställningarna jag hade tycker jag gav mig svar på mitt problem, men jag tror att även diskussionsfrågor kunde varit till stor hjälp för att vidareutveckla respondenternas svar. Jag anser dock att jag fick fram mycket nyttig och intressant information från respondenterna utifrån de frågor jag ställde.

För att eventuellt få ett bättre materialunderlag genom intervjuerna, kunde jag ha tagit kontakt med IT-enheten för vårdcentralerna inom Västra Götalandslän på ett tidigare stadium. Utifrån den säkerhetspolicy och de riktlinjer som finns för vårdcentralernas BKS kunde jag sedan ha gjort jämförelser med personalens svar.

Arbetsprocessen

Jag anser att denna form av arbetssätt har varit mycket utvecklande och roligt. Arbetssättet har varit en stor skillnad jämfört med tidigare kurser jag läst.

Erfarenheter jag fått är att det är viktigt med en tidsplanering för att strukturera sitt arbete. De tidsramar som varit uppsatta tycker jag har gjort att arbetstakten flutit på bra.

10.2 Resultatet

Jag anser mig ha fått svar på min problemställning. Jag fick en uppfattning om att personalen anser att säkerhetsarbetet är mycket viktigt inom deras verksamhet. Resultatet om personalens medvetenhet kring säkerhetspolicys och riktlinjer var förvånande. Inom vårdcentraler florerar en mängd integritetskänslig information, varför resultatet jag fick fram inte överensstämmer med det resultat jag trodde mig få fram när jag började med detta arbete.

Jag trodde att medvetenheten om säkerhetspolicys och riktlinjer för behörighetskontrollsystemet skulle vara större hos personalen på vårdcentralerna, då det är viktigt att skydda integritetskänslig information inom verksamheten. Medvetenhet kring säkerhetspolicys och riktlinjer fanns det inte på vårdcentralerna, men trots det anser jag att personalen försöker skydda sin information på ett bra sätt.

Den information jag fick om personalens utbildningen och information kring säkerhetspolicyn och riktlinjerna var inte vad jag förväntat mig. Jag trodde att säkerhetspolicyn för deras BKS var en central och viktig del inom vården eftersom det finns mycket känsliga uppgifter som t.ex. patientjournaler.

Samtliga vårdcentraler inom Västra Götalandslän har, enligt uppgift från IT-enheten för vårdcentralerna inom Västra Götalandslän, samma inloggningssystem och versamhetssystem. Information kring säkerhetspolicys och riktlinjer förmedlas till samtliga systemansvariga på respektive vårdcentral från IT-enheten, därefter är det de systemansvarigas uppgift att förmedla information angående säkerhetspolicys och riktlinjer till övriga personalkategorier.

Medvetenheten kring säkerhetspolicys och riktlinjer kan inte generaliseras för samtliga vårdcentraler inom Sverige, eftersom detta skulle kräva en mer omfattande undersökning. Information och utbildning kring säkerhetspolicys och riktlinjer inom Västra Götalandslän verkar dock ske på liknande sätt på samtliga vårdcentraler varför medvetenheten och kunskapen kring säkerhetspolicys och riktlinjer för behörighetskontrollsystmet kan vara relativt likvärdig hos personalen på vårdcentralerna inom länet.

10.3 Förslag till fortsatt arbete

Denna undersökning visar endast personalens medvetenhet på vårdcentralerna inom Skövde kommun. Verksamheten som undersökts är relativt liten, varför skillnader kan finnas inom större verksamheter som t.ex. sjukhusen.

Utifrån denna undersökning anser jag att det kan vara intressant att även undersöka personalens medvetenhet inom andra verksamheter, kring säkerhetspolicys och riktlinjer vid användning av ett behörighetskontrollsystem. Det kan exempelvis finnas skillnader beroende på verksamhetens behov av att skydda information.

Referenser

Litteratur

Aronsson, R. (1995), *ADB-säkerhet : Grundbok för säker ADB-hantering*, Ängelholm: Bokförlaget kommunlitteratur

Beckman, A. (1990), *PC-säkerhet för användare av persondatorer eller PC-nät*, Stockholm: Affärsinformation AB

Bell, J. (1993), *Introduktion till forskningsmetodik*, Lund: Studentlitteratur

Dataföreningen i Sverige (1997), *Steg för steg mot bättre IT-säkerhet*, Stockholm: Tryckeribolaget

Dahmström, K (1991), *Från datainsamling till rapport*, Lund: Studentlitteratur

Drätselkontoret (1998), *Informationssäkerhet : Mål, Policy och Riktlinjer för Lunds kommun 1998-1999*

Edlund, L., Hedqvist, J. och Holmberg, S. (1989), *Affärssäkerhet – Att förebygga svindleri inom bank, finans, företag och förvaltning*, Stockholm: Affärsinformation AB

Elgemyr, A. och Mattson, L. (1992), *Stora säkerhetsboken – För företag, myndigheter och andra organisationer*, Stockholm: Publica

Freese, J. och Holmberg, S. (1993), *Dataosäkerhet – Praktisk handbok för beslutsfattare*, Stockholm: Affärsinformation AB

Gratte, I. (1989), *ADB-datasäkerhet*, Stockholm: Liber AB

Jacobsen, J.K. (1993), *Konsten att lyssna och fråga*, Lund: Studentlitteratur

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

Repstad, P. (1999), *Närhet och distans - kvalitativa metoder i samhällsvetenskap*, Lund: Studentlitteratur

Statskontoret (1989:11), *Policy, ansvar och organisation*

Statskontoret (1991:14), *Behörighetskontrollsystem*

Thavenius (1997), *Allmän IT-kunskap*, Lund: Lundahls förlag

Trost, J. (1994), *Enkätboken*, Lund: Studentlitteratur

Internet

Datainspektionen (1998) http://www.din.se (As is : 10 Mars)

Information till personalen angående syftet med undersökningen

Denna undersökning är till för att se vilken medvetenheten det finns hos personalen på vårdcentralerna i Skövde kommun, vad gäller de säkerhetspolicys och riktlinjer som finns för användning av ett sk behörighetskontrollsystem (inloggningsystem).

Vissa av mina frågor är ganska känsliga, därför är undersökningen helt konfidentiell, vilket innebär att inga namn eller andra uppgifter som lämnas kommer att kunna härledas till en viss person. Svaren är väldigt viktiga för mitt arbete, men eftersom intervjun är helt frivillig får du själv bestämma om du vill svara på frågan eller inte.

Inledande frågor

1. Kön Man / Kvinna
2. Ålder över eller under 35
3. Vad arbetar du med?
4. Vet du vad syftet med ett BKS är(inloggningssystemet)? Ja / Något sånär / Nej, vet ej
5. a) Hur ofta använder du inloggningssystemet?

   b) Tänker du på vilka säkerhetsrutiner som gäller när du sköter din inloggning?

   Ja, alltid/ Ja, ibland / Nej, aldrig
6. Vilken typ av information krävs det behörighet och skydd av i er verksamhet?
7. a) Vilken information har du tillgång till?

   b) Har olika personer olika rättigheter till informationen?

Frågor kring behörighet och lösenordshantering

8. Hur tycker du att behörighetstilldelningen fungerat då du blev tilldelad dig de rättigheter du har? Mycket bra / Bra / Mindre bra
9. Hur tycker du att lösenordshanteringen fungerar? Mycket Bra / Bra /Svårt och krånglig
10. Är det fler än du som känner till ditt lösenord?
11. Hur ofta byter du lösenord, görs det enligt den säkerhetspolicy som finns?
12. Finns det några ansvariga för hur lösenordshanteringen skall skötas? I så fall vem?
13. Vad tycker du är ditt ansvar för att obehöriga inte skall få tillgång till känslig information?
14. Har det förekommit på denna vårdcentralen att information hamnat i orätta händer, i så fall vilken typ av information var det?
15. Brukar du lämna din dator utan uppsikt om du är inloggad?
16. a) Hur är datorerna placerade på vårdcentralen?

    b) Brukar det finnas patienter där datorerna är placerade?

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Har du sett några dokument över hur säkerhetspolicyn för behörighetskontrollsystemet ser ut?
18. Är den säkerhetspolicyn tydlig och enkel att förstå eller svår att förstå och ta del av?
19. Hur uppfattar du att användningen av inloggningssystemet fungerar? Lätt att använda / Svårt att använda

20. a) Har du fått någon information kring säkerhetspolicys och riktlinjer?

    b) Hur har du i så fall tagit del av säkerhetspolicyn?

21. Hur ofta ges utbildning/information kring säkerhetspolicys och riktlinjer vad gäller inloggningssystemet?
22. Tycker du att det är viktigt med utbildning kring säkerhetspolicyn? Om ja, varför?
23. Vet du vem det är som ansvarar för att sprida informationen kring säkerhetspolicys och riktlinjer?
24. Vad anser du att du har för kunskap om hur behörighetskontrollsystemet fungerar? Mycket bra kunskap / Bra kunskap / Nödvändig kunskap
25. Vet du om det finns något uppföljningssystem som kontrollerar att personalen efterlever den säkerhetspolicy som finns för behörighetskontrollsystemet?

Övrigt

26. Hur anser du att man eventuellt kan öka medvetenheten om säkerhetspolicys hos personalen?
27. Har du något att tillägga utöver dessa frågor?

Vårdcentral ett

Intervju 1

Inledande frågor

1. Man
2. Över 35.
3. Distriktsläkare.
4. Ja.
5. a) Flera gånger dagligen.

   b) Ja, ibland.
6. Patientuppgifter, Internet, Post (alla har olika lösenord).
7. a) Jag har tillgång till all information eftersom jag har högst behörighet.

   b) Ja, det är beroende av vilka arbetsuppgifter man har.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Relativt bra.
10. Nej.
11. Ja, alltid (det finns inlagt i systemet, som säger ifrån ca var tredje månad att man ska byta lösenord)
12. Ingen, man måste logga in på två ställen för att komma in i systemet. Det behövs därför ingen som ansvarar för detta. Varje dag måste två lösenord användas för att kunna använda journalsystemet. Man måste först in i Windows och sedan in i journalen.
13. Genom att använda lösenordet, och att ingen mer än jag känner till det.
14. Nej, tidigare då allt sköttes manuellt var det lättare att information kom i orätta händer. Då kunde vem som helst läsa t.ex. patientjournaler som låg framme på skrivbordet. Idag är detta svårare eftersom det finns möjligheter att se vem som varit inne i systemet, vilken tidpunkt och i vilka journaler. Därför har detta blivit svårare och jag tycker att säkerheten är bra på så sätt.
15. Varje gång jag lämnar datorn loggar jag ur eller så låser jag dörren. Det finns dock fler i personalen som har tillgång till nyckeln till mitt rum, då helt säkert är det inte. Jag har en skärmsläckare som går på efter en stund, denna har jag däremot inget lösenord till. Många andra i personalen har det, vet jag.
16. a) Datorerna finns placerade i varje personals rum.

    b) Ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Vet inte, det kanske jag har. (Jag har inte med det att göra eftersom jag mer har lite allmän datakunskaper.
18. -
19. Systemet är lätt att använda, lite besvärligt eftersom det är många olika lösenord som man måste känna till, det kan vara lite krångligt tycker jag. Det kan finnas enklare sätt att använda ett inloggningssystem, det tar ju lite tid varje gång man ska logga in. Det skulle kunna finnas t.ex. igenkänningsloggning, att t.ex. känna igen handen.
20. a) Ja

    b) Jag har fått information muntligt, skriftlig information har vi fått om säkerhetsrutinerna.
21. Ja, det sker väl inte särskilt ofta men vid förändringar så får vi ny information om vad som gäller.
22. Ja, för att veta syftet med systemet och vilka konsekvenser det kan innebära om något görs felaktigt.
23. Systemansvarig.
24. Mycket bra kunskap.
25. Det behövs inte eftersom ingen kan komma förbi systemet då det krävs dubbla lösenord för att komma in i systemet.

Övrigt

26. Genom att själv komma ihåg lösenordet.
27. Inom vår verksamhet är det inbyggt med säkerhet och det är väldigt viktigt eftersom personliga uppgifter inte får komma i orätta händer. Det är nog svårare i andra verksamheter där det nog kan uppfattas som svårt och onödigt med behörighet till viss information. I vår verksamhet är nog de flesta trots allt medvetna om att det är viktigt med säkerheten.

Intervju 2

Inledande frågor

1. Kvinna.
2. Över 35.
3. Sekreterare, dataansvarig.
4. Ja.
5. a) Dagligen.

   b) Ja, alltid eftersom jag vet om dem.
6. Det finns behörighet till alla uppgifter, den information som du ska åt måste du ha behörighet till. Det är t.ex. patientuppgifter.

7. a) Ja, jag har högst behörighet och har därför tillgång till all information. Jag kan kontrollera och ändra lösenorden.

   b) Ja, alla har olika behörighet beroende på arbetsuppgifter.

Frågor kring behörighet och lösenordshantering.

8. Mycket bra.
9. Mycket bra.
10. Nej, ingen mer än jag själv.
11. Datorn talar automatiskt om när du ska byta lösenord, ca var tredje månad.
12. Dataansvarig.
13. Alla i personalen ansvarar var för sig att informationen skyddas.
14. Nej.
15. Ja, om jag springer i korridoren, men inte om jag ska fika eller på lunch då lämnar jag aldrig datorn inloggad.
16. a) Var dator är placerade i personalens rum. Var och en måste tänka på att inte lämna sin dator, så att andra inte kan ta del av t.ex. personuppgifter.

    b) Ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Ja.
18. Ja, de var enkla att förstå och ta del av.
19. Systemet är lätt att använda.
20. a) Ja.

    b) Man lär sig allt eftersom man använder systemet, annars har jag tagit del utav säkerhetspolicyn både skriftligt och muntligt.
21. Om det är något som man undrar över så kan man alltid ringa till supportavdelningen. Utbildning får vi väl annars när det sker någon förändring.
22. Jag tycker att det är mycket viktigt med utbildning, det är ju viktigt att man håller sig ajour med det som händer. När det gäller datorer händer det ju ständigt nya saker och därför är detta extra viktigt. Utbildning är också viktigt eftersom man måste lära sig och veta vad man ska hålla reda på. Särskilt viktigt inom vårt arbete är att känna till de lagar och förordningar som gäller.
23. Dataansvarig.
24. Mycket bra kunskap.
25. Nej, men om man inte följer lösenordsystemet så kommer man inte in i systemet. Det går inte att kringgå de rutiner som finns. Därför tror jag inte att det behövs något uppföljningssystem.

Övrigt

26. Mer information och utbildning är ju aldrig fel. Det är viktigt att vi pratar mer inom personalen, det finns nog många som går omkring med frågor utan att ha fått något svar.
27. Nej.

Intervju 3

Inledande frågor

1. Kvinna.
2. Över 35.
3. Undersköterska.
4. Ja.
5. a) Dagligen.

   b) Ja.
6. Patientjournaler.
7. a) Jag har bland annat tillgång till patientuppgifter.

   b) Ja, alla har olika behörighet till olika sorters applikationer. Alla har inte tillgång till alla journaler och alla kan inte skriva i journalerna.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Bra.
10. Nej.
11. En gång var tredje månad eller oftare om det t.ex. uppstår problem och man inte kan komma in i systemet.
12. -
13. Genom att ha skärmen släckt om jag lämnar datorn.
14. Nej.
15. Ja, datorn släcker sig efter en stund och sedan behövs det ju lösenord för att komma in. Det finns nämligen lösenord för att komma förbi skärmsläckaren.
16. a) Alla i personalen har varsin dator.

    b) -

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej, jag har inte sett något dokument.

18. Eftersom jag inte sett något dokument kan jag inte svara på detta, men jag har fått information om säkerhetsrutinerna och dessa var lätta att förstå.
19. Lätt att använda.
20. a) Nej.

    b) -
21. Inte särskilt ofta i alla fall, det är väl som nu när vi fått vårt nya system som vi dels fått lite information om säkerheten, men inte om säkerhetspolicys.
22. Ja, det är väl en självklarhet. Det är ju viktigt att veta vad man håller på med.
23. Dataansvarig här på vårdcentralen.
24. Nödvändig kunskap.
25. Ja, men inte kontinuerligt, det är vår dataansvarige som håller koll på oss.

Övrigt

26. Man skulle kunna be om mer utbildning och information när det gäller detta.
27. Nej.

Intervju 4

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska.
4. Ja.
5. a) Dagligen.

   b) Ja, ibland, men bara då när man blir påmind om att byta lösenord, annars tänker jag

   inte på det.
6. Alla uppgifter som vi hanterar kräver behörighet och skydd. Patientuppgifter osv.
7. a) Jag har tillgång till de uppgifter som krävs för mina arbetsuppgifter. Bland annat patientjournaler.

   b) Ja, alla har inte tillgång till all information som finns, därför är det också nödvändigt med de här rättigheterna som vi har fått.

Frågor kring behörighet och lösenordshantering

8. Mycket bra.
9. Bra men svårt, man måste byta lösenord ofta och det är svårt att komma ihåg lösenord och komma på nya lösenord. Det skulle vara bra om man kunde komma

på ett system för hur det ska vara lättast att hålla reda på ett nytt lösenord. Jag tycker att vi byter lösenord jämt och ständigt.

10. Nej.
11. Byter när datorn säger att det är dags att byta.
12. -
13. Genom att det endast är jag som känner till mitt lösenord och att jag inte har det uppskrivet någonstans.
14. Nej, eventuellt skulle det kunna vara när vi faxat iväg något men det är inget som jag vet har förekommit.
15. Ja.
16. a) Datorerna finns placerade inne på personalens rum.

    b) Det brukar finnas patienter närvarande, men då brukar jag ställa datorn på en bild där det inte visas några patientuppgifter, eller så är skärmsläckaren igång.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej.
18. -
19. Systemet är lätt att använda förutom att det tar lång tid att logga in varje gång.
20. a) Nej.

    b) -
21. -
22. Ja, patientuppgifter är vardag för oss. Det är därför viktigt med utbildning. Uppgifterna är viktigare för patienten och detta kan vara lätt att glömma, därför skulle det vara bra att bli påmind om säkerheten och säkerhetspolicyn.
23. IT-enheten.
24. Nödvändig kunskap.
25. Nej.

Övrigt

26. Man skulle prata mer om detta och ta upp det t.ex. på arbetsplatsgruppmötena. Vi skulle få mer information och utbildning kring säkerheten.
27. Nej.

Vårdcentral två

Intervju 1

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska, systemansvarig.
4. Något sånär.
5. a) Dagligen.

   b) Ja, man är ju medveten om det.
6. Tidbokning, journaler och labblistor.
7. a) Jag har tillgång till allt som är datoriserat, eftersom jag är systemansvarig hanterar jag även lösenordshanteringen.

   b)Ja, undersköterskor kan inte skriva något i journalerna utan endast läsa. De har bara behörighet till labblista och tidbokningen.

Frågor kring behörighet och lösenordshantering.

8. Bra.
9. Bra, det kan vara problem med ny personal, men eftersom vi har en liten arbetsplats är det oftast inga problem.
10. Nej.
11. Det måste man byta var 60:onde dag, då säger datorn automatiskt ifrån.
12. Systemansvarig.
13. Det finns ju skärmsläckare som används för att patienter inte ska kunna ta del av informationen. Skärmsläckarna är kodade, så varje går man ska in i måste man logga in igen.
14. Nej, det tror jag inte i alla fall.
15. Ja, men då går skärmsläckaren igång, denna är kodad så jag måste knappa in mitt lösenord för att komma in igen.
16. a) Datorerna är placerade i personalens kontorsutrymme. Det finns även en dator i labbrummet som alla har tillgång till. Där måste alla logga in, även där finns skärmsläckare.

    b) Jag brukar ha patienter där , ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Ja, de finns väl i någon pärm någonstans.
18. De var lätta att förstå.

19. Lätt att använda.
20. a) Ja.

    b) Vi fick information om detta när vi utbildade oss, för länge sedan.
21. Det händer som sagt inte så ofta.
22. Ja, det är viktigt eftersom det är viktigt att sjukvårdspersonal är medvetna om sekretessen och tystnadsplikten.
23. Ja, det är en man på IT-enheten i Mariestad.
24. Bra kunskap.
25. Det har jag aldrig varit med om, det vet jag faktiskt inte.

Övrigt

26. Genom att ha mycket mer utbildning.
27. Nej.

Intervju 2

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska.
4. Ja.
5. a) Dagligen.

   b) Ja, alltid.
6. Journaldelen, det har systemansvarig hand om.
7. a) Journaldelen och till viss del även administrativa uppgifter.

   b) Ja, alla har t.ex. inte tillgång till att skriva i journalen.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Bra.
10. Nej.
11. Det måste man byta var tredje månad, då säger datorn automatiskt ifrån att det är dags att byta. Vi har två inloggningssystem, som man måste logga in på för att komma in i systemet.
12. Ansvaret ligger upp till var och en. Man måste ju arbeta efter sekretesslagen inom vårt yrke. Allt är skyddat, om man vill skicka journalkopior måste man ha tillstånd från en läkare.

13. Genom att använda mitt lösenord så kan ingen annan läsa den informationen.
14. Nej.
15. Inte utan uppsikt, kan jag inte säga.
16. a) Datorerna är placerade på våra rum, varje anställd har en egen dator.

    b) Nej.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Det har vi säkert fått, men det är inget som jag säkert vet.
18. -
19. Lätt att använda.
20. a) Ja, säkert.

    b) Vid någon datautbildning, har vi säkert fått information om detta.
21. Det kommer direktiv från socialstyrelsen, men det pratas inte så mycket om detta.
22. Ja, det är viktigt att det finns medvetenhet kring sekretessen hos personalen.
23. Det är väl arbetsledaren i vårt fall, annars socialstyrelsen.
24. Bra kunskap.
25. Nej, det vet jag inte.

Övrigt

26. Man skulle prata mer om det och ta upp det som en naturlig del i arbetet. Det är lättare att vara medveten i en mindre organisation. Det finns nog större behov i en större verksamhet t.ex. på sjukhusen, där tror jag att det finns brist vad gäller medvetenheten kring säkerheten.
27. -

Vårdcentral tre

Intervju 1

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska, föreståndare och systemansvarig.
4. Ja, det tror jag väl.
5. a) Dagligen.

   b) Ja, ibland.
6. All information som vi hanterar.
7. a) Jag har tillgång till all information eftersom jag är systemansvarig.

   b) Ja, beroende på vilka arbetsuppgifter man har så varierar ens rättigheter.

Frågor kring behörighet och lösenordshantering

8. Mycket bra.
9. Bra, men det kan vara trassel ibland, eftersom alla kanske inte alltid lyckas logga in.
10. Nej.
11. Ja, vi byter var annan månad, då säger systemet automatiskt ifrån och vi måste byta lösenord.
12. Systemansvarig.
13. Genom att använda lösenordet och genom att hålla det hemligt så att ingen annan kan få tillgång till min information.
14. Nej.
15. Ja, det händer. Om jag lämnar rummet brukar jag trycka ett snabbkommando och skärmsläckaren går igång, sen måste jag logga in igen för att komma åt informationen.
16. a) Det är lite olika, de är inte placerade ut mot korridoren utan placerade i läge så att inga patienter kan ta del utav informationen.

    b) Ja, men de är aldrig ensamma, om det finns patienter i mitt rum så brukar jag använda snabbkommandot som låser skärmen.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Ja, det har jag säkert gjort men jag kan inte säga när det var.
18. Ja, men de var svåra att förstå och ta del utav.
19. Lätt att använda.

20. a) Ja, under utbildning så fick vi säkert information om detta.

    b) När vi skulle lära oss vårt nya system som kom förra sommaren, fick vi utbildning.

21. Det borde finnas mer utbildning och information, det är inte ens en gång om året som det sker tror jag.

22. Ja, det är viktigt med utbildning, det skulle dessutom inte skada att prata mer om detta, med enklare typ av information som är lättare att förstå.

23. IT-ansvarig, på IT-enheten.

24. Bra kunskap.

25. Nej, inte vad jag vet så finns det inte.

Övrigt

26. Genom att få information oftare om vad det är som gäller.

27. Det finns mycket att förbättra inom detta område. Det kan finnas patienter som kan vara intresserade av att titta på informationen som finns på skärmen, om man lämnar den utan uppsikt. Det är dock endast patientens egna uppgifter som visas på skärmen. Det borde finnas något som förhindrar detta.

Intervju 2

Inledande frågor

1. Kvinna.
2. Över 35.
3. Läkarsekreterare.
4. Ja.
5. a) Dagligen, använder jag flera olika lösenord för att logga in i de system som jag vill komma åt. Jag måste logga in i varje system som jag vill komma in i.

   b) Ja, ibland. Det är ju ändå ingen annan som kommer in till den information som jag vill åt eftersom de inte vet mitt lösenord. Så visst tänker jag på det.

6. Vi behöver skydda all vår information.
7. a) Jag har tillgång till allt utom att signera kan jag väl säga. Det är olika journaler och kassauppgifter bland annat.

   b) Ja, det har vi beroende på vilka arbetsuppgifter som vi har.

Frågor kring behörighet och lösenordshantering.

8. Mycket bra.
9. Bra, jag har min egen identitet och eget lösenord. Det syns dessutom i vilka system man varit inne i och när det var.

10. Nej.
11. Var tredje månad säger datorn automatiskt ifrån och jag måste byta lösenord.
12. Systemansvarig.
13. Eftersom vi är så få på denna vårdcentral så står det öppet överallt och vi kan gå in i varandras rum hur som helst. Patienterna har ingen rättighet att se informationen. Eftersom vi är så små vet alla vad alla sysslar med och vi pratar mycket under rasterna om detta. Som läkarsekreterare vet jag nog därför mer än jag borde veta.
14. Nej, om det skulle vara något så pratar vi med läkarna om detta. Alla hjälps åt om det skulle vara några problem.
15. Ja, det skulle inte gå att logga ur varje gång jag lämnar datorn. Jag lämnar den på även när jag går på rast eller fikar, det skulle vara för jobbigt att hela tiden logga in.
16. a) Alla har sin egen dator.

    b) Nej, inte här men på sköterskornas rum finns det naturligtvis patienter.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej, jag har kanske sett något men inte vad jag vet.
18. -
19. Lätt att använda.
20. a) Nej.

    b) -
21. Det händer inte alls särskilt ofta att vi får någon utbildning.
22. Ja, det är väldigt viktigt att hålla sig ajour och inte bara hålla sig till de gamla rutinerna.
23. Systemansvarig.
24. Mycket bra.
25. Systemansvarig.

Övrigt

26. Genom att prata om detta på arbetet, på en högre nivå, det är bättre om det är fler hjärnor som arbetar.
27. Nej.

Intervju 3

Inledande frågor

1. Kvinna.
2. Över 35.

3. Biomedicinsk analytiker.
4. Ja.
5. a) Dagligen.

   b) Det är väl inget som jag direkt tänker på, ibland kanske det händer men inte särskilt ofta.
6. Allt som finns i vår verksamhet.
7. a) Jag har tillgång till allt.

   b) Jag tror att alla har tillgång till all information på denna vårdcentralen.

Frågor kring behörighet och lösenordshantering.

8. Mycket bra.
9. Mycket bra.
10. Nej.
11. Byte av lösenord till journalsystemet tror jag är var sjätte månad som vi måste byta. Då säger datorn automatiskt ifrån.
12. Support och IT-enheten.
13. Genom att jag ser till att jag loggar ur när jag lämnar datorn utan uppsikt.
14. Nej.
15. Nej.
16. a) I alla rum där det sitter personal.

    b) Nej inte i detta rummet i varje fall.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej, jag är inte säker på att jag sett något dokument som rör säkerhetspolicyn. Jag har sett papper angående sekretessen, tystnadsplikten.
18. -
19. Lätt att använda.
20. a) Ja, det har jag antagligen.

    b) Vi får ju informationsblad, i början när allt datoriserades talade vi mycket om detta.
21. -
22. Ja, det är naturligtvis väldigt viktigt att hålla sig ajour och det är dessutom väldigt roligt att lära sig något nytt.
23. IT-enheten.
24. Nödvändig kunskap.
25. Nej.

Övrigt

26. De flesta är väldigt medvetna tror jag, men det finns nog alltid någon som inte följer säkerhetspolicyn. Men i och med att vår vårdcentral är ganska liten har vi nog en bra medvetenhet tror jag. Alla är ju väldigt insatta i sekretessen. Det är nog svårare på andra ställe och visst behövs det mer information för att påminna om hur viktigt det är med säkerheten. Ofta blir det en rutin och man tänker inge alltid på säkerheten.
27. -

Intervju 4

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska.
4. Ja.
5. a) Flera gånger dagligen.

   b) Det har blivit en rutin, men visst tänker jag på det ibland.
6. All information som vi hanterar.
7. a) Journaler.

   b) Ja, alla har all behörighet, det är så litet på denna vårdcentral och därför är det väldigt sårbart om inte alla skulle ha tillgång till all information. Om t.ex. en läkare är borta en dag och jag måste se hans filer så måste jag kunna göra det.

Frågor kring behörighet och lösenordshantering.

8. Bra.
9. Bra.
10. Nej.
11. Var tredje månad blir man uppmanad att byta lösenord, då säger datorn ifrån.
12. Ja, systemansvarig.
13. Genom att inte ha journaler eller väntelistor uppe på skärmen om någon patient finns här. Och genom att hålla mitt lösenord hemligt.
14. Nej, inte vad jag vet.
15. Ja, det händer. Om man är riktigt smart så kan man ta sig in i systemet. Helt säkert är det inte.
16. a) I varje rum.

b) Ja, det är bland annat därför som jag ställt stolen en bit ifrån datorn så att patienten inte ska kunna läsa det som står på skärmen. Annars så har jag skärmsläckaren på så att man inte kan se det som finns på skärmen.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej.
18. -
19. Lätt att använda.
20. a) Nej, vi har bara fått information om vilka säkerhetsrutiner som gäller.

    b) Genom informationsblad och sen ingick det i vår utbildning som vi gått.
21. Det sker ju förändringar succesivt och man måste få ny information hela tiden.
22. Ja, kunskap är inte fel att ha. Det är bra att ha en pärm med information som man kan gå tillbaka till om man vill kolla upp vad som gäller. Det finns även supportavdelningen som hjälper oss.
23. Systemansvarig.
24. Mycket bra kunskap.
25. Nej.

Övrigt

26. Genom att prata mycket om det. Man skulle prata mycket mer sinsemellan i personalen. Jag har ganska svårt att lära mig nya saker och vill helst kunna saker utantill. Därför skulle jag aldrig kunna vara dataansvarig.
27. -

Vårdcentral fyra

Intervju 1

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska och dataadministratör.
4. Ja, det vet jag.
5. a) Flera gånger dagligen.

   b) Nej, det kan jag väl inte säga att jag gör, vi har ju alltid varit medvetna om sekretessen och tystnadsplikten, nu är allt i datorn istället och kan inte hanteras hur som helst.
6. All information, utom bokningen.
7. a) Jag har tillgång till det mesta, jag kan inte skriva i allt men jag har bland annat tillgång till psykiatrisköterskans journaler.

   b) Ja, det har vi.

Frågor kring behörighet och lösenordshantering

8. Vi fick vårt system 1993, det fungerar bra tycker jag.
9. Det fungerar bra förutom att det kan vara krångligt ibland när systemet inte fungerar riktigt som det ska.
10. Nej.
11. Man måste byta när datorn säger ifrån, det sker väl var tredje månad. Vi måste byta lösenord till båda systemen som vi måste logga in till. Windows och vårt system Profdoc.
12. Det har vi support som hanterar, det är IT-enheten på Gesällgatan.
13. Genom att följa reglerna och ta fram en bild som inte visar några känsliga uppgifter. Det går även igång en skärmsläckare efter ett par minuter.
14. Nej.
15. Ja, det händer, men jag försöker att tänka på att logga ur.
16. a) Det finns datorer i alla våra rum.

    b) Ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Ja, det har jag. Det finns ju även datalagar och journallagar som vi måste kunna.
18. De är enkla att förstå och ta del av.
19. Lätt att använda, vid tidsnöd kan det vara jobbigt att vara tvungen att logga in.

20. a) Ja.

    b) Muntlig och skriftlig information

21. Vi har fått information en gång, det händer inte så ofta. Det är väl vid eventuella förändringar av systemet som vi får information.
22. Ja, det är alltid viktigt med utbildning. Vid nyanställning är det speciellt viktigt.
23. Nej, det är jag osäker på men jag tror att det kan vara IT-enheten som har hand om det.
24. Bra kunskap.
25. Nej, det vet jag inte.

Övrigt

26. Genom att ta upp det på möten och prata om det. På APG-mötena är bra tillfälle att göra det.
27. -

Intervju 2

Inledande frågor

1. Kvinna.
2. Över 35.
3. Undersköterska.
4. Ja.
5. a) Dagligen.

   b) Det vet jag inte direkt, ibland kanske jag tänker på det.

6. All information.
7. a) Jag har tillgång till journalerna, men jag får inte skriva något utan bara läsa. Jag har även tillgång till bokningslistorna.

   b) Ja.

Frågor kring behörighet och lösenordshantering

8. Mycket bra.
9. Bra.
10. Nej.
11. Var tredje månad måste jag byta lösenord. Det blir jag påmind om när det kommer upp en ruta på skärmen som säger att jag ska byta lösenord.
12. Det är dataansvarig här på vårdcentralen.

13. Genom att jag inte skrivit ner lösenordet och lagt det under skrivbordsunderlägget. Skärmsläckaren skyddar ju också informationen, den går igång efter ett tag. Jag har däremot inget lösenord till den.
14. Nej.
15. Ja, men inte utan att ha skärmsläckaren igång.
16. a) Datorerna är placerade ute i personalens kontor.

    b) Ja, det kan finnas patienter närvarande i rummen med datorer, men vi lämnar aldrig patienterna ensamma på rummet. Om jag lämnar datorn på lunchen brukar jag låsa rummet.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej.
18. -
19. Lätt att använda.
20. a) Nej.

    b) -
21. Det är inte särskilt ofta som vi får någon information överhuvudtaget tycker jag.
22. Ja, journalhanteringen är jätte viktigt att vara medveten om säkerheten, eftersom det är uppgifter som absolut inte får komma i orätta händer.
23. Dataansvarig här på vårdcentralen.
24. Nödvändig kunskap
25. Nej.

Övrigt

26. Genom att diskutera på APG-möten men även skriftlig information skulle vara bra.
27. -

Intervju 3

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktsläkare.
4. Ja, dels att veta vilket tillträde man har och att det även skall synas vart man varit inne, i vilket system.
5. a) En gång om dagen.

   b) Ja, ibland tänker jag på det, men oftast har man så mycket annat att tänka på så det händer inte så ofta.

6. Alla patientbundna uppgifter, ja allt i verksamheten är viktigt att skydda.
7. a) Jag har tillgång till samtliga journaler, psykjournaler och läkarjournaler, jag tror inte att jag har tillgång till kassan.

   b) Ja.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Bra, men än så länge har jag inte bytt lösenord någon gång.
10. Dataansvarig.
11. Var sjätte månad gissar jag på, men eftersom jag inte bytt någon gång så vet jag inte.
12. Dataansvarig här på vårdcentralen.
13. Genom att inte lämna datorn utan uppsikt. Låsa dörren om jag lämnar rummet så att inte någon obehörig kan gå in och dra ur kopior på något.
14. Nej, men jag har nog hört att personer fått tillgång till sådan information som de egentligen inte har rätt till. Men jag vet inte om det hänt på denna vårdcentralen.
15. Ja, jag kan lämna rummet för att gå in i undersökningsrummet mitt emot. Det finns alltid folk i korridoren, under lunchpauser så gör jag inte det utan då låser jag alltid dörren.
16. a) Placerade i rummen här på vårdcentralen.

    b) Ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej, ingen information om säkerhetspolicyn. Vi har däremot fått information om säkerheten och vilka rutiner det är som gäller.
18. Säkerhetsinformationen var enkel att förstå, det är det enda jag kan säga.
19. Lätt att använda.
20. a) Nej.

    b) -
21. Vi får inte särskilt mycket information måste jag säga.
22. Vid nyanställning är det framförallt extra viktigt med utbildning, annars vet jag inte om det är särskilt viktigt.
23. Nej, det vet jag inte men det finns ju datakunniga som man kan fråga om det är några problem.
24. Nödvändig kunskap, jag är ingen dataexpert utan klarar av att använda systemet utan några problem.
25. Ja, det tror jag att det finns. Det brukar alltid finnas.

Övrigt

26. Genom gruppmöten och föreläsningar främst på våra APG-möten skulle man kunna ta upp detta.
27. -

Intervju 4

Inledande frågor

1. Kvinna.
2. Över 35.
3. Sekreterare och dataansvarig.
4. Ja.
5. a) Dagligen.

   b) Ja, ibland.
6. Journaler.
7. a) All information eftersom jag är dataansvarig.

   b) Ja, det finns olika spärrar till journalerna om man får läsa, skriva eller kanske inte ens se uppgifterna.

Frågor kring behörighet och lösenordshantering.

8. Mycket bra.
9. Bra.
10. Nej.
11. Var tredje månad säger datorn automatiskt ifrån och vi måste byta lösenord.
12. Dataansvarig och IT-enheten.
13. Jag ser till att ha skärmsläckare som jag har lösenord till. Det är tänkt att alla i personalen ska ha det.
14. Nej.
15. Ja, men då har jag skärmsläckaren igång.
16. a) I rummen på vårdcentralen.

    b) Nej, det finns aldrig patienter i mitt rum.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Ja, jag har sett dokument över säkerhetspolicyn.
18. Jag tyckte att de var enkla att förstå.
19. Lätt att använda.

20. a) Ja.

    b) Vi har fått ett informationshäfte om säkerheten.

21. Inte särskilt ofta i alla fall.

22. Ja, det är så mycket förändringar hela tiden så det är mycket viktigt att man hela tiden blir informerad och får utbildning.

23. IT-enheten.

24. Mycket bra.

25. Ja, det finns.

Övrigt

26. Genom att få information, men det finns så klart de som inte följer detta i alla fall.

27. -

Vårdcentral fem

Intervju 1

Inledande frågor

1. Man.
2. Över 35.
3. Distriktsläkare, tidigare systemansvarig.
4. Ja, det vet jag. Vi måste först logga in på nätverket, Internet och in i journalsystemet.
5. a) En gång om dagen. Om jag lämnar datorn låser jag bara och då krävs det att man med lösenordet loggar in igen.

   b) Ja, det är ju ingen annan som känner till lösenordet. Detta fungerar bättre med det nya systemet, tidigare kände flera personer till varandras lösenord.
6. All information i journalen.
7. a) All information.

   b) Alla har rättigheter till all information, det finns dock de som även har tillgång till lösenordshanterinen, men det är supportavdelningen som hanterar detta. Själva underhållningen av systemet är också supports uppgift.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Ja, det fungerar bra. Det krävs minst sex positioner för lösenordet och detta ska man byta var tredje månad, i båda systemen när man loggar in. Vi har haft datorer i åtta år och det har fungerat bra tycker jag. Det har inte skett några större katastrofer, någon disk har kraschat ibland, men eftersom vi kör backup på allting så är det inga problem och ingen information har försvunnit utan att vi kunnat reparera den.
10. Nej.
11. Var tredje månad så byter vi båda lösenorden. Vi har alla egna hembibliotek som ingen annan kommer in i, detta är därför ett säkrare ställe att spara information på. Det finns nog ingen annan i personalen än jag som lagt in egna program. All lösenordshantering sköts likadant överallt i Västa Götalands län. Det är samma regler som gäller. Alla användare är dessutom unika i Västra Götalands län. Det skulle därför gå att logga in i ett system i Göteborg om man vill det.
12. Systemansvariga.
13. Genom att hålla lösenord hemliga och inloggningsnamnet hemligt. Genom att inge lämna datorn utan uppsikt utan att låsa skärmen, med en skärmsläckare.
14. Nej.
15. Ja, men andra kan ju inte gå in i journalprogrammen eftersom skärmen låser sig är det inga problem.

16. a) Datorerna är placerade inne i personalens expeditioner. Det finns inga datorer i undersökningsrummen. Flera personer använder samma datorer och alla kan alltså logga in på alla datorerna, en person kan endast vara inloggad på en dator i taget.

    b) Nej.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej, inte nyligen i alla fall. Jag har säkert sett någon men inte vad jag lagt på minnet.
18. -
19. Lätt att använda.
20. a) Nej, inte om säkerhetspolicyn.

    b) -
21. Det händer inte så ofta, vi har nyligen bytt system och fick utbildning vad gäller säkerheten men inte om någon säkerhetspolicy.
22. Ja, det gör ju att man blir effektivare som användare, jag tycker att det finns för lite utbildning och skulle gärna se lite mer utav det.
23. IT-enheten för primärvården i Skaraborg. I vårt tidigare system kunde vi gå in själva och lägga in nya användare. Nu är allt istället helt centraliserat och vi sköter ingenting utav det längre. Det enda som vi gör är att sköta backup av informationen, om något strular så får vi kontakta IT-enheten.
24. Mycket bra, eftersom jag tidigare skötte Novell själv.
25. Nej, eftersom det inte går att kontrollera om någon i personalen lämnar sitt rum i flera timmar med dörren olåst. Det finns inga rutiner för detta och det är svårt att kontrollera.

Övrigt

26. Genom att ha utbildning och då t.ex. ge exempel på vad som kan hända.
27. Nej, men ett tips är att ta kontakt och prata med dem på IT-enheten för att få lite bakgrundsinformation om säkerhetspolicyn.

Intervju 2

Inledande frågor

1. Kvinna.
2. Över 35.
3. Läkarsekreterare, systemansvarig.
4. Något sånär, det handlar väl om sekretessen och att det är viktigt att ingen annan känner till ens lösenord.
5. a) Dagligen.

b) Ja, alltid.

6. Mest patientuppgifter.
7. a) Patientjournaler, jag har inte tillgång till medicinjournalen, det är endast doktorn som kan skriva ut recept. Jag kan skriva i labblistorna.

   b) Ja, t.ex. har vi inte tillgång till psykssköterskans journaler.

Frågor kring behörighet och lösenordshantering

8. Bra, förutom att man kanske är ovan att byta lösenord.
9. Bra, om någon lagt in ett å,ä eller ö i sitt lösenord kan inte vi fixa det, det är nog det enda problemet. Det måste supportavdelningen fixa.
10. Nej, allt har blivit säkrare sedan vi fick det här nya systemet, 1998. Sedan dess är det nog ingen annan som känner till någon annan persons lösenord. Tidigare fanns det personer som gjorde det.
11. Var tredje månad.
12. Systemadministratören eller support som är extra utbildade inom profdoc.
13. Genom att använda skärmsläckaren med lösenord och undvika att det ligger patientuppgifter framme på skrivbordet om det kommer hit någon person.
14. Nej.
15. Det kan ju förekomma, men då brukar jag ha en skärmbild som inte visar några patientuppgifter på skärmen.
16. a) En dator i varje expedition, inte i något undersökningsrum.

    b) Nej.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej.
18. -
19. Lätt att använda.
20. a) Nej.

    b) -
21. Det händer sällan, men när det händer någonting som att vi nyligen bytt datasystem så har vi fått utbildning och information om bland annat säkerhetsrutinerna vid inloggningen.
22. Ja, det är viktigt det gör ju att man känner sig mer säker på det som man gör och tryggare i sitt arbete när man vet vad man håller på med.
23. Systemansvarig och support.
24. Bra.
25. Nej.

Övrigt

26. -

27. Det gamla systemet som vi använde hade ingen skärmsläckare, detta är ju mycket bra i detta nya systemet. Förut kunde vi dessutom gå in och kolla vem som varit inne i vilka journaler, detta kan vi inte göra längre - inte vad jag vet i alla fall.

Intervju 3

Inledande frågor

1. Kvinna.
2. Över 35.
3. Distriktssköterska.
4. Ja, det innebär att ingen annan ska kunna ta del utav den information som jag har tillgång till.
5. a) Dagligen (en gång på morgonen)

   b) Nej, allt går ju på rutin.
6. Patientuppgifter.
7. a) Patientjournaler, dessa uppgifter är ju skyddade av sekretesslagen och journallagen.

   b) Alla kan ju komma in i journalen, alla kan skriva och läsa. Alla har samma behörighet.

Frågor kring behörighet och lösenordshantering

8. Bra.
9. Bra.
10. Nej.
11. Var tredje månad, vad har de andra sagt för något.
12. Nej, jag tror inte att det finns någon som ansvarar för det.
13. Genom att stänga ner datorn om jag lämnar den.
14. Nej, det har jag ingen kännedom om.
15. Nej.
16. a) I de olika arbetsrummen som finns.

    b) Ja.

Frågor kring utbildning av BKS map säkerhetspolicyn

17. Nej.
18. -

19. Lätt att använda.
20. a) -

    b) -
21. -
22. Ja, det finns ju lagar som vi måste veta om.
23. Nej, det måste väl vara de som är systemansvariga.
24. Nödvändig kunskap.
25. Nej, jag vet inte om det finns något utarbetat system för detta.

Övrigt

26. Utbildning
27. Vi är ju alla styrda av de lagar som finns, detta har ju alltid funnits inom sjukvården.