Hvordan lykkes med den initiale fasen av en markedsutvidelsesbasert ekspansjonsstrategi med teknologikonseptet Cloud Computing?

Morten Berglind, Kandidatnummer: 108

Alexander Breive Havre, Kandidatnummer: 122

Masteroppgave i økonomi og administrasjon/siviløkonom

Strategi og kompetanseledelse

Høgskolen i Buskerud og Vestfold

Hønefoss, Juni 2014

Forord

Denne masteravhandlingen er gjennomført som et ledd i vår mastergradsutdannelse i økonomiske og administrative fag ved Høgskolen i Buskerud og Vestfold, avdeling Hønefoss. Vi er to medstudenter som har utarbeidet oppgaven, og vi har begge valgt siviløkonomretningen med spesialisering innenfor strategi og kompetanseledelse. Arbeidsprosessen har gitt oss innsikt i et spennende fagfelt og dette året har vært svært lærerikt. Vi mener de funnene vi har avdekket er viktige for akademia og for praktisk anvendelse senere.

Vi vil rette en stor takk til vår veileder Øystein Sørebø som har vært en solid støttespiller for oss. Tusen takk for all seriøsiteten du har vist og at døren din alltid har vært åpen. Vi kunne ikke fått en bedre veileder når det kommer til vårt tema, med din kunnskap og ekspertise innenfor IT & org/marketing. Likeså vil vi også takke Ole Morten Boldevin i CSC for konstruktive tilbakemeldinger, samt Kari-Anne Melby for innspill og glimrende bistand når det kom til trakting av kaffe. Videre vil vi takke våre nøkkelinformanter som har tatt seg tid til å bistå oss i en travel arbeidshverdag. Uten dere hadde ikke dette vært mulig å gjennomføre.

Arbeidsprosessen har til tider vært svært krevende, samtidig mener vi at vi har levert en avhandling vi kan være stolte av. Vi sitter igjen med mye kunnskap, og mener du som leser vil få ny innsikt i et spennende område. Til slutt vil vi takke hverandre for et godt samarbeid og et krevende år, der vi har lært mye om både samarbeid, teori og praksis.

Hønefoss, 10.juni 2014

_____ _____

Morten Berglind Alexander Breive Havre

Sammendrag

I denne avhandlingen fokuserer vi på hva som skal til for å lykkes med den initiale fasen av en markedsutvidelsesbasert ekspansjonsstrategi med teknologikonseptet Cloud Computing. Oppgaven tar for seg helsesektoren, der vi ser på hvilke faktorer som er kritiske for en vellykket markedsekspansjon av Cloud Computing i fasen før produktet skal tilbys markedet. Videre ser vi på hvilke implikasjoner som kan møte en leverandør med intensjon om ekspansjon av Cloud Computing i denne sektoren.

Cloud Computing konseptet utgjør en komplett IT løsning som ivaretar en organisasjons IT behov fra A til Å. Løsningen gir full frihet til å velge forretnings-applikasjon, arbeidssted og hvilke enheter som organisasjonen skal benytte for effektiv tilgang til data, tjenester og applikasjoner. Nesten alle Cloud Computing leverandører lover kundene en moderne IT løsning med garantert utviklingstakt, slik at de alltid vil få tilgang til de nyeste versjonene og tjenestene på en rask og effektiv måte. Basert på dette ser vi store muligheter for at det offentlige skal kunne bruke slike løsninger. Offentlig virksomheter har tidligere brukt egenutviklede og spesialtilpassede løsninger til eget bruk som har vært svært kompliserte og kostbare. Vi ser store muligheter for effektivisering og modernisering innenfor helsesektoren.

Avhandlingen er et videre arbeid basert på vårt forprosjekt som ble levert våren 2013 ved Høgskolen i Buskerud og Vestfold: *"Hvordan kan en leverandør av Cloud Computing ekspandere fra et næringslivsorientert Cloud Computing marked til et offentlig Cloud Computing marked?"*. For å besvare våre forskningsspørsmål har vi foretatt en utfyllende teorigjennomgang. Avhandlingen er løst med en kvalitativ forskningsstrategi, der vi har gjennomført et casestudie hvor vi har intervjuet syv personer tilknyttet ledelsen i helsesektoren.

I vår analyse har vi kodet empirien etter teoretiske variabler. Deretter har vi tatt for oss hver enkelt kategori for å finne sammenhenger og ulike synspunkter i informantenes svar. Våre svar viser hva som kreves fra helsesektoren sin side og hva som forventes av en Cloud Computing leverandør.

Innholdsfortegnelse

Figurliste

Tabelliste

1. Innledning

1.1 Bakgrunn

De fleste selskaper har et mål om å få virksomheten til å vokse og ekspandere, noe som ofte gjenspeiler seg i selskapenes visjoner og strategier. I dag ser vi dette innenfor både privat og offentlig sektor. IKEA er et eksempel hvor visjonen er å skape en bedre hverdag for alle mennesker. Deres forretningsidé er å ha lave priser slik at så mange som mulig har råd til å kjøpe deres produkter. Skal de nå sin visjon må de ekspandere til nye markeder og i eksisterende (IKEA, u.å.). Et viktig spørsmål knyttet til ekspansjon er hva som skal til for å realisere denne strategien og lykkes med den.

Penrose (1959) ser på to sider av bedrifters vekst. Den ene siden er å fase inn i nye produkter, mens den andre siden er å komme inn i nye markeder, innenfor rammen bedriftene har av tilgjengelige ressurser. Med andre ord etablerte Penrose (1959) et klart skille mellom produkt og markedsekspansjon. I skillet mellom marked- og produktekspansjon kommer Nelson & Winther (1982) inn med sitt rutinebaserte syn på vekst. De antyder at markedsekspansjon vil være enklere og vil føre til raskere organisatorisk vekst enn produktekspansjon. De mener at en vekst i markedet vil oppstå på bakgrunn av tidligere erfaringer og øke eksisterende salgskanaler som bedriften har i dagens marked. På den andre siden krever produktekspansjon utvikling av nye rutiner, eller en rekombinasjon av gamle rutiner og vil derfor innebære større grad av uforutsigbarhet etterhvert som ekspansjonsprosessen går fremover (Leonard-Barton, 1995; Winter & Szulanski, 2002). På bakgrunn av denne uforutsigbarheten krever ekspansjon av et nytt produkt mer tid til produktutvikling, testing og produksjon, sammenlignet med ekspansjon av et eksisterende produkt i et nytt marked (Mishina, Pollock & Porac, 2004).

En beslutning om å etablere en utviklingsstrategi mot et nytt marked vil i neste instans føre til en ekspansjon, og deretter vil dette betinge valg av inngangsstrategi. Slike valg bør derfor tas med, som basis i veloverveide og grundige strategiske analyser (Jakobsen & Lien, 2001). Valg av inngangsstrategi er en viktig del av en slik utviklingsstrategi mot et nytt marked. Det er ikke bare viktig å være opptatt av det nye

markedet man skal inn i, men også hvordan man velger å entre markedet eller markedene (Lee & Lieberman, 2010).

Vi har vært så heldige å få bruke CSC (Computer Sciences Corporation) som case-organisasjon, derfor vil vi i denne masteravhandlingen gjennomføre en undersøkelse i forbindelse med dette firmaet som er i starten av en ekspansjonsprosess. CSC ønsker å ekspandere fra det private til det offentlige markedet innenfor helsesektoren. Dette firmaet er en av de største aktørene innenfor informasjonsteknologisektoren, og satser stort på nye innovative IT-løsninger. CSC er med 90 000 ansatte en av verdens ledende tilbydere av IT-relaterte tjenester.

CSC som Cloud Computing leverandør tilbyr en tjeneste som gir muligheten til å skalere ressursene, noe som fører til at kunden ikke trenger å tenke så mye på de store variasjonene i ressursbruk, da dette blir håndtert av CSC. Vi kan se dette i perspektiv til bedrifter i det offentlige markedet, som f.eks. sykehus. I norske sykehus benytter de seg av løsninger som blant annet analyseverktøy, lagringssystemer, sikkerhetssystemer osv., som går igjennom store mengder data for så å komme frem til et resultat, en person eller en løsning. Ettersom hvor ofte en slik oppgave kjøres, kan det være besparende å benytte seg av Cloud Computing.

En annen fordel er at informasjonen er tilgjengelig på en plass. Dette er noe som ville spart sykehusene for både tid og penger. Tid på et sykehus er noe som kan redde liv. Dersom du ser på kostnadsaspektet, betaler bare kunden for den faktiske bruken. Ikke nok med det, men kunden trenger ikke selv å investere i servere (engangskostnader). Alle kostnader assosiert med drift av serverne blir inkludert inn i en fast pris (Sultan, 2010). Dette fører til at kunden kan fokusere på sin egen kjernekompetanse og ikke benytte store ressurser på servere som kanskje ikke blir optimalt utnyttet. Cloud Computing bygger på følgende grunnleggende egenskaper:

- En delt ressurs
- Tilgjengelig via internett
- Alltid tilgjengelig
- Skalerbar – umiddelbart
- Betal etter bruk
- Mulighet for selvbetjening

Kort fortalt er Cloud Computing et system for å lage en nettverkssammenslutning til en felles base av f.eks. nettverk, servere, lagringssystemer, applikasjoner og tjenester som raskt kan settes opp med minimale ressurser og kostnader.

1.2 Problemstilling og forskningsspørsmål

CSC er allerede etablert i det private markedet med sine Cloud Computing tjenester og vurderer nå en ekspansjon til det offentlige markedet. Denne masteroppgaven vil omhandle den initiale fasen i en ekspansjonsstrategi og fokuset vil være på kundesiden. Vi vil se på Cloud Computing før det eventuelt blir implementert for å få et innblikk på hvordan man kan lykkes med en markedsutvidelsesbasert ekspansjons-strategi. Økonomisk suksess kommer av kjennskap til kunden. En viktig suksessfaktor er derfor å vite hva kunden vil ha. Vi vil se på hva som skal til for at sykehusene vil ta i bruk dette konseptet og hva som eventuelt holder de tilbake. Er det sikkerhets-problemer, effektivitetsproblemer, sykehusenes holdning til Cloud Computing eller økonomien som eventuelt vil sette en stopper for en ekspansjon?

Problemstillingen vi har utarbeidet lyder som følger:

Hvordan lykkes med den initiale fasen av markedsutvidelsesbasert ekspansjons-strategi med teknologikonseptet Cloud Computing?

Med bakgrunn i dette fremmer vi følgende tre forskningsspørsmål:

1. Hvilken forkunnskap og hvilke initiale holdninger eksisterer blant potensielle kunder av teknologikonseptet Cloud Computing i markedet det skal ekspanderes til?

2. Hvilke atferdsintensjoner (dvs. intensjon om å adoptere teknologikonseptet) kan vi slutte at eksisterer i markedet ut fra informasjon om kunnskap og holdninger blant potensielle kunder?

3. Hvilke implikasjoner har eksisterende forkunnskap, holdninger og atferdsintensjon for en leverandør med intensjon om å etablere et nytt marked innen denne sektoren?

1.3 Avgrensning av oppgaven

I dette delkapittelet presenterer vi avgrensninger i studien vår, bl.a. å synliggjøre gyldighetsområdet av det vi studerer.

Slik det fremgår av problemstillingen og forskningsspørsmålene så fokuserer vi på Cloud Computing, ekspansjon og holdninger. Et annet tema vi har valgt å ta med er informasjonssikkerhet, fordi vi mener at dette må være ivaretatt før en eventuell ekspansjon av det teknologiske konseptet. Dette er en kvalitativ studie. Formålet er å gjennomføre en idiografisk undersøkelse, fordi vi ønsker å gå i dybden for å se på det "individuelle, spesielle og unike". Hvis vi hadde vært ute etter å få oversikt over det generelle med det mål å generalisere funnene våre, ville vi valgt en nomotetisk tilnærming.

Cloud Computing har møtt kritikk for mangelfulle informasjon om teknologiens reelle sikkerhet, samt kundenes begrensede kunnskap til produktet. Informasjons-sikkerhet og potensielle kunders holdning til teknologien er sentralt i forhold til det foreliggende forskningsarbeidet, derfor vil vi ha et spesielt fokus på disse to elementene i studien vår. Vårt forskningsarbeid vil ikke bare fokusere på sikkerhetsaspekter ved Cloud Computing, men også om holdninger hos helsesektoren når det kommer til Cloud Computing. Dette er den primære avgrensningen i denne studien. Samtidig vil vi fokusere på andre fordeler og ulemper, som til slutt vil være med å skissere en fremtidig prediksjon av Cloud Computing. Selv om det finnes ulike organisasjoner rundt om i verden som for tiden bruker Cloud Computing, så har denne forskningen begrenset sin studie mot helseforetak i Norge. Dette er oppgavens sekundære avgrensning.

Cloud Computing er fortsatt i den innledende bruksfasen. Det er bare noen få store IT-organisasjoner som for øyeblikket tilbyr og bruker Cloud Computing i dagens tekniske marked, derfor har det vært vanskelig for oss å finne informasjon på området. Imidlertid har vi funnet noen kilder som er blitt identifisert som relevant data og er samlet inn for å opprettholde forskningens troverdighet.

1.4 Struktur for avhandlingen

I avhandlingens første kapittel presenteres bakgrunnen for valg av tema, oppgavens problemstilling, forskningsspørsmål og oppgavens struktur. I kapittel to som omhandler det teoretiske rammeverket, tar vi for oss de ulike begrepene som går igjen i oppgaven og teorien rundt disse. Det tredje kapittelet fokuserer på metodikken i forskningen som brukes i denne oppgaven. Metodekapittelet leverer det teoretiske rammeverket, forskningsstudie og design brukt i denne studien. I tillegg skisserer de forskjellige metodene og verktøyene som brukes for datainnsamling, analyse og markerer troverdigheten til forskningen. Kapittel fire viser vår analyse av data-materialet. I kapittel fem tar vi for oss de ulike funnene i analysen som vi har fått gjennom intervjuer. Videre i kapittel seks vil vi presentere implikasjoner og videre forskning. Til slutt kommer vi med styrker og svakheter ved vår studie i kapittel syv.

2. Teoretisk referanseramme

Temaet er ”Markedsutvidelsesbasert ekspansjonsstrategi av teknologikonseptet Cloud Computing.” Med basis i dette temaet lanserte vi en problemstilling i innledningen. Avslutningsvis lanserte vi tre spesifikke forskningsspørsmål. Sentralt i forskningsspørsmålene står begrepene ekspansjon, Cloud Computing og holdninger. I dette kapittelet vil vi starte med å ta for oss begrepet ekspansjon. Deretter vil vi ta for oss Cloud Computing og sikkerhet, før vi går over til begrepet holdning. Til slutt vil vi ta for oss begrepskombinasjonen som består av sikkerhet og holdninger.

Valget om å inkludere dette er gjort av hensyn til relevansen vi finner at det har for markedsutvidelsesbasert ekspansjon i helsesektoren.

2.1. Ekspansjonsteori

Formålet med dette delkapittelet er å komme frem til en grundig og gyldig forståelse av begrepet ekspansjon. Dette fordi temaet for masteroppgaven dreier seg om hva som skal til for at helsesektoren skal ta i bruk Cloud Computing, samt hvordan leverandøren skal klare å realisere dette. Det er med andre ord snakk om en ekspansjon fra det private Cloud Computing-markedet til det offentlige markedet. Vi vil derfor i avsnitt 2.1.1 ta for oss selve begrepet ekspansjon og vise hvordan begrepet defineres i litteraturen, mens vi i avsnitt i 2.1.2 vil ta for oss skillet mellom ekspansjon og vekst.

2.1.1 Definisjon av ekspansjon

Jakobsen og Lien (2001) definerer ekspansjon som ”*det å øke antallet produkt-markeder en bedrift konkurrerer i”*. Som vi ser er denne definisjonen konkret og handlingsorientert. Det kan beskrives så enkelt som Jakobsen og Lien (2001) sin definisjon, for ekspansjon handler kun om å nå ut til nye markeder. Bang & Joshi (2008) definerer ekspansjon som ”*en strategi for å øke primærbehovet for en produkt-kategori ved å konvertere ikke-kunder til kunder i en industri og/eller ved å øke brukerfrekvensen av bransjens eksisterende kunder”*. Denne definisjonen er litt mer detaljert enn Jakobsen og Lien sin, ved at de definerer ekspansjon som en strategi og sier hvordan man kan ekspandere. Videre har North America`s Business Center definert ekspansjon som ”*et steg når et selskap identifiserer nye uutnyttede markeder og søker muligheter for vekst via disse nye markedsmulighetene”* (Missouri

Development, u.å.). Videre sier de at en markedsekspansjon vil føre til at en eventuelt kan levere nye funksjoner til et eksisterende marked, og levere eksisterende produkter til nye potensielle markeder. North America`s Business Center avslutter med at en markedsekspansjon også vil identifisere alternativ teknologi, andre bruksområder for produkter samt måle relative kostnader for å diversifisere seg inn på nye markeder (Missouri Development, u.å.). Vi ser at deres definisjon er i tråd med definisjonene vi har nevnt tidligere og mener at dette også er en god og konkret definisjon på begrepet ekspansjon.

2.1.2 Skillet mellom ekspansjon og vekst

Det er viktig å skille mellom ekspansjon og vekst. Hvis man øker markedsandelene sine i eksisterende markeder så er ikke dette ekspansjon, selv om det er en form for vekst. Vekst forekommer uten at en trenger å etablere seg i nye produktmarkeder. Vi kan skille mellom tre typer ekspansjon: vertikal integrasjon, internasjonalisering og diversifisering (Jakobsen, 2012; Jakobsen og Lien, 2001). En vertikal ekspansjon vil være opp- eller nedstrøms i kjeden. Internasjonal ekspansjon går ut på å etablere seg i nye geografiske områder med eksisterende produkter. Diversifisering vil være når man etablerer seg i nye produktmarkeder i et eksisterende geografisk område (Jakobsen, 2012; Jakobsen & Lien, 2001). Hill og Jones (2004) skiller mellom to typer diversifisering, som er relatert og urelatert diversifisering. Med relatert diversifisering mener de ekspansjon inn i en ny forretningsaktivitet som relaterer seg til selskapets eksisterende virksomhet. Urelatert diversifisering er ekspansjon i bransjer som ikke har en åpenlys sammenheng med selskapets eksisterende drift.

Ekspansjon vil være viktig for videre verdiskapning for bedrifter, og vil forsterke et foretaks konkurransedyktighet. Ekspansjon går under ressurs-basert strategi, og Penrose (1959) var en av de første som tok opp viktigheten av ressurser for foretakets konkurransedyktighet (Newbert, 2007). Ressursbasert teori (RBT) er opprinnelig bygget på teori fra forskning innen strategi, og reflekterer i stor grad viktigheten av selskapsspesifikke muligheter (Hendersen & Mitchell, 1997; Raymond, Rivard & Verreault, 2006). Spanos og Lioukas (2001) påpeker at strategien til selskapet bør være bygget på de unike ressursene selskapet har. Hvordan foretaket klarer seg eksternt og internt avhenger av hvordan disse ressursene blir fordelt. Ressursbaserte teoretikere har hevdet at en bedrifts unike portefølje av materielle og immaterielle

ressurser påvirker hastighet og retning av en bedrifts ekspansjon (Barney, 1991; Mahoney & Pandian, 1992; Penrose, 1959; Peteraf, 1993).

2.2 Fenomenet Cloud Computing

I denne delen av oppgaven ønsker vi å komme med definisjoner på begrepet Cloud Computing og sikkerhet, samt komme med en del konkret informasjon om Cloud Computing konseptet til CSC. Deretter vil vi ta for oss konseptets styrker og svakheter i lys av ulike forskningsartikler. Dette for å se på hvordan Cloud Computing passer for ulike bedrifter/organisasjoner som jobber i det offentlige markedet. Vi er av den oppfatning at det er flere og ulike måter å tilnærme seg markedet på. Selv de som innehar samme spesialområde, har ulikheter i form av strategi, drift og bemanning. Det vil si at selv om det er en teknologisk nyvinning på området som passer bra for noen, så passer det nødvendigvis ikke like bra for alle.

2.2.1 Hva er Cloud Computing

Ettersom begrepet Cloud Computing er relativt nytt og ikke helt utbredt i markedet, så er det heller ingen felles definisjon på begrepet (Sultan, 2011). Dette ble klart etter at vi hadde gått igjennom de ulike artiklene vi hadde på området. Ut i fra artiklene kommer det klart frem at de fleste lager egne definisjoner, samt at de velger å skrive om punkter de selv anser som mest sentrale. Videre ser vi at det er noen begreper som forekommer hyppigere enn andre. Noen av disse begrepene er skalerbarhet, elastisitet, virtualisering og global tilgjengelighet. Vi har valgt å basere vår oppgave på de mest sentrale definisjonene på området, som er beskrevet nedenfor.

Marston et al. (2011:177) definerer Cloud Computing som: "*It is an information technology service model where Computing services (both hardware and software) are delivered on demand to customers over a network in a self-service fashion, independent of device and location. The resource required to provide the requisite quality-of-service levels are shared, dynamically scalable, rapidly provisioned, virtualized and released with minimal service provider interaction. Users pay for the service as an operating expense without incurring any significant initial capital expenditure, with the Cloud Computing services employing a metering system that divides the Computing resource in appropriate blocks.*"

Zissis og Lekkas (2010) definerer Cloud Computing som: "*Cloud Computing is a model for enabling convenient, on-demand network access, to a shared pool of configurable Computing resources, (E.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

Buyya et al. (2009) definerer Cloud Computing som: "*A Cloud Computing is a type of parallel and distributed system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified Computing resource(s) based on service-level agreements established through negotiation between the service provider and consumers."*

Wang et al. (2010) definerer Cloud Computing som: *"A Computing Cloud Computing is a set of network enabled services, providing scalable, QoS guaranteed, normally personalized, inexpensive Computing platforms on demand, which could be accessed in a simple and pervasive way."*

De overnevnte definisjonene omkring Cloud Computing beskriver konseptet som en tjeneste som byr på en løsning i form av både maskinvare og programvare, via et nettverk. Cloud Computing er en skalerbar tjeneste som har mulighet for virtualisering av maskinvare, ofte med lite arbeid i forkant fra leverandørens side. Ressursene i Cloud Computing blir tildelt etter avtale med leverandøren, dette i form av at kunden ofte bare betaler for den faktiske bruken og slipper de store oppstarts investeringene, som f.eks. kjøp av maskinvare.

2.2.2 Ulike typer av Cloud Computing

Ettersom det finnes ulike typer av Cloud Computing for ulike aktører, har vi valgt å ta for oss disse. Dette er gjort for å bidra til en bredere forståelse av Cloud Computing, fordi konseptet er relativt vidt.

Private Cloud Computing

Skyens infrastruktur drives utelukkende for en organisasjon. Den kan bli administrert av organisasjonen eller en innledende tredjepart. Det gir mer sikkerhet (Mell & Grance, 2011).

Public Cloud Computing

Skyens infrastruktur er gjort tilgjengelig for allmennheten eller et stort industri-konsern, og eies av organisasjonen som selger Cloud Computing-tjenester. Skyens brukere kan få tilgang til tjenester fra hvor som helst i verden (Mell & Grance, 2011).

Hybrid Cloud Computing

Skyens infrastruktur er en sammensetning av to eller flere skyer som forblir unike enheter. Disse er bundet sammen av standardiserte eller proprietære teknologier som gjør at data-og applikasjoner er mobile (Mell & Grance, 2011).

Vi har tatt for oss de ulike typene av Cloud Computing, for å finne hvilke type som kan passe best innenfor helsesektoren. Dette har vi gjort fordi vi mener det er enkelte løsninger som passer bedre innenfor helsesektoren enn andre.

2.2.3 Ulike teknologiske begreper

I dette delkapittelet vil vi ta for oss ulike teknologiske begreper og tjenester, dette bidrar til en bedre forståelse av det teknologiske konseptet. Cloud Computing er kjerneproduktet i den markedsutvidelsesbaserte ekspansjonsstrategien.

Infrastructure as a Service (IaaS)

Infrastruktur som en tjeneste innebærer outsourcing av utstyr som brukes til å støtte operasjoner, inkludert lagring, maskinvare, servere og nettverkskomponenter (Techtarget, 2011).

Software as a Service (SaaS)

Software som en tjeneste er en distribusjonsmodell, der programmene er arrangert av en leverandør eller tjenesteleverandør og gjort tilgjengelig for kunder via et nettverk. (Techtarget, 2011).

Platform as a Service (PaaS)

Plattform som en tjeneste er et paradigme for å levere operativsystemer og tilhørende tjenester over internett uten nedlastning eller installasjon (Techtarget, 2011).

Vi har valgt å ta for oss de tre tjenestene som vi anser som mest relevante for helsesektoren. Vi vil likevel nevne at det finnes andre tjenester som for eksempel ”Clusters” og ”Grid Computing” som kan være relevante, men som vi har valgt å se bort ifra med tanke på avgrensning til oppgaven.

2.2.4 CSC og Cloud Computing

CSC’s Cloud Computing tilbyr en portal som gir deg en operasjonell åpenhet inn i tjenester, pre-konfigurerte tjenestekataloger, samt gir deg muligheten til å bygge og administrere flere programmiljøer. Dette blir gjort for å organisere Cloud Computing til å utvikle og administrere operasjonelle prosesser. Fra Cloud Computing portalen kan du få tilgang til en bedrifts tjenestekatalog. Dette fungerer fra et hvilket som helst program, plattform eller operativsystem som kundene bruker. Med portalen får du også innsikt i egen bruk og serviceytelse for løpende drift, dette for å bidra til sikkerhet og budsjettstyring.

Cloud Computing organiserer og automatiserer livssykluser i programmet, samtidig som tjenesten sørger for at arbeidsflyten rundt arbeidsoppgavene er bra. Dette bidrar til rask konfigurering, klargjøring og fjerning av ressurser. CSC’s Cloud Computing løsning tilbyr sikkerhet, sikkerhetskopiering, gjenoppretting og høy tilgjengelighet av alternativer for å støtte kontorproduktivitet og bedriftsapplikasjoner. Du kan velge å administrere Cloud Computing selv, eller du kan velge å få CSC til å håndtere det for deg. Med ”CSC ledelse” får du støtte til å bygge ut det virtuelle miljøet. Dette bidrar til at CSC kan kjøre og vedlikeholde Cloud Computing for deg, samt gi oppdateringsstyring, distribusjon av programvare, VM (Virtual Monitoring), overvåking og vern mot trusler (CSC IaaS, 2013).

I dagens marked er ikke teknologi alene nok for å sikre motstandsdyktige Cloud Computing miljøer. Det kombineres derfor ledende og utprøvde teknologier i regi av CSC’s prosesser. Disse er basert på ”best praksis”, utviklet og finjustert på grunnlag av mer enn 50 års globalstyrt tjenesteerfaring. ”Cloud Computing kontroll” er et sikkerhetsprogram som dekker områder med datastyring, anleggssikkerhet, risikostyring og informasjonssikkerhet.
Med Cloud Computing-infrastrukturen til CSC har hver komponent i denne infra-strukturen et potensial til å påvirke tjenestens ytelse. Hver av disse komponentene har

en feiltoleransemekanisme på plass, dersom feil skulle oppstå. For eksempel: produktet har to redundante strømforsyningsenheter i Cloud Computing for å sikre at et enkeltindivids strømbrudd ikke vil påvirke anleggets tilgjengelighet. Mange infrastrukturkomponenter bærer flere strømkilder for å aktivere feiltoleransen til en sekundær effektstøtte uten å påvirke systemets tilgjengelighet eller ytelse (CSC IaaS, 2013).

Cloud Computing er beskyttet i dybden av et forsvar i sikkerhetsrammeverket, noe som betyr at det leverer en fysisk og logisk sikkerhet med både adgangskontroll og alternativer til dataintegritet. Dette er for å støtte driftskritiske prosesser og back-office applikasjoner (CSC IaaS, 2013).
Videre er det også personell til å kontrollere hendelsens respons, virtuelle brannmurer og nettverksinntrengende beskyttelsessystemer, som overvåker standardfunksjoner 24 timer i døgnet, 7 dager i uken. Valgfrie sikkerhetstjenester inkluderer antivirus og sårbarhetsskanning. Det tjenesten til CSC sikrer er at alle de viktige nettverkene og systemloggene er sentralt lagret, korrelert og analysert av deres team av sikkerhetseksperter.

Med åpenhet i Cloud Computing er CSC i stand til å dempe bekymringer over tapet av synlighet, noe som vanligvis oppstår når programmer og data blir flyttet fra en kundes lokalbaserte løsning til Cloud Computing. Eksempler på informasjon som deles ved å bruke Cloud Computing-protokollen er gjeldende konfigurasjon, data-beliggenhet, tilgangsrettigheter, historie og eventuelt journallogger.

2.2.5 Styrker og svakheter ved Cloud Computing

I dette underkapittelet vil vi ta for oss empirien rundt ulike typer av styrker og svakheter i forhold til produktet Cloud Computing. Dette gjør vi for å belyse styrker og svakheter ved konseptet. Svakhetene er spesielt viktig ettersom det er disse som kan bidra til å hemme muligheten for ekspansjon, mens styrkene igjen kan bidra til å fremme muligheten for ekspansjon.

Styrker:

Lave driftskostnader og oppstarts investeringer

Et av forretningsgrunnlagene til Cloud Computing baserer seg på at man slipper de store oppstarts investeringene (Marston et al, 2011). Dette kommer av at bedriftene leier en aktør som allerede er etablert på området, istedenfor å investere store summer i serverinfrastruktur. Deretter trenger de kun å betale de faktiske kostnadene ved bruken av systemet. Hvis man benytter seg av andre leverandører til å utføre arbeidet, så blir det deres jobb å sørge for at de har tilstrekkelig kapasitet. Det er leverandørens oppgave å sørge for at de har kapasitet til å kjøre eventuelle variasjoner i ressursbruk, dersom det skulle bli nødvendig (Zissis og Lekkas, 2010).

Det kommer også frem at det er mest hensiktsmessig å overlate innkjøp, drift og vedlikehold til en tredjepart som har kjernekompetanse på området. Ved hjelp av en tredjepart får du også muligheten til å benytte deg av bulkinnkjøp, det vil si at dersom du kjøper store mengder så oppnår du bedre priser ved kvantumsrabatt (Zissis og Lekkas, 2010). Dette medfører lavere komponentpriser, som igjen vil gjenspeile seg i totalprisen. Leverandørene på området har også mulighet til å finne en gunstig geografisk plassering for serverparkene. Dette kan bidra til at strøm og annen infrastruktur er billigere og mer pålitelige, dersom det skulle oppstå brudd på nett- og strømlinjer (Zissis og Lekkas, 2010).

Cloud Computing påvirker IT innovasjon i den forstand at den fjerner barrierer (Marston et al, 2011). Dersom man bare tar betalt for den faktiske bruken og skalerbarheten, så er det enklere for ulike bedrifter å komme seg inn på nye markeder uten å investere alt for store summer i form av maskinvarer o.l.

Fra en annen side er det ulike applikasjoner som bruker mer av en ressurs enn andre (Armbrust et al, 2009). Hvis du for eksempel ser på sikkerhetskopiering, så kommer det frem at det kan kreve mye lagring, analysering av datasett og utnyttelse av prosessorkraften. Noe bruker mye nettverk, mens annet kjører relativt lave ressurskrav. Dersom man skulle velge å benytte seg av Cloud Computing kan man individuelt betale for hver ressurs (Armbrust et al, 2009).

Skalerbarhet

Skalerbarhet gjør det mulig å skalere ressursene etter behov og dette er en av de store fordelene ved å benytte seg av Cloud Computing. Marston et al. (2011:178) sier at:

"Cloud Computing makes it easier for enterprises to scale their services- which are increasingly reliant on accurate information – according to client demand. Since the Computing resources are managed through software, they can be deployed very fast as new requirement arise." Dette er ifølge Marston et al. (2011) hovedfunksjonen til Cloud Computing.

Ressursbruken til bedrifter varierer blant annet fra tid på døgnet til kvartaler i året. Ettersom det forekommer mest aktivitet i arbeidstiden, så vil det på dette tidspunktet være at systemet bruker mest ressurser.

Global tilgjengelighet

Cloud Computing løsninger er nesten uten unntak knyttet opp mot internett. Det vil si at brukere har tilgang til tjenesten uansett hvor de befinner seg. Vi kan skille mellom to typer tilganger til Cloud Computing-løsninger:

1) Tjenester som kun er knyttet opp mot et begrenset antall brukere f.eks. ansatte i en bedrift eller organisasjon.
2) Tjenester som er åpne for alle, eksempler på slike løsninger er Hotmail, Yahoo og Google. Disse tjenestene er tilgjengelige uansett hvor man befinner seg, så lenge en internettilkobling er tilgjengelig (CSC, 2013).

Sikkerhet

Mange hevder at ved å benytte seg av Cloud Computing så vil man få høyere sikkerhet (Marston et al, 2011; Zissis og Lekkas, 2010). Dette er fordi løsningene til Cloud Computing gir større innsikt i hvem som bruker tjenesten og hva de bruker den til. Med andre ord har man muligheten til å kontrollere når, hvor og hvordan ansatte har tilgang til bedriften sitt system via et simpelt webgrensesnitt (Marston et al, 2011). Sikkerhet må bli sett i sammenheng med bruken av tjenesten. Basert på hvilke type tjeneste man leier, så finnes det ulike sikkerhetsnivåer. Blant annet ved bruk av leide virtuelle servere, finnes det muligheter for å ta sikkerhetskopier av den aktuelle databasen/tjenesten. Dette hadde vært en aktuell funksjon som f.eks. politiet kunne hatt brukt ifm. etterforskning i straffesaker etc. Lovverk og internasjonale regler er da nødvendig ifm. bruk/misbruk av denne type tjenester.

Videre har Cloud Computing også avansert teknologi som beskytter mot virus, spion-programmer og andre skadelige angrep, samtidig som den beskytter brukeren mot identitetstyveri. Selv nye og framvoksende trusler avverges umiddelbart. Skadelige

nettsteder blokkeres automatisk slik at du kan bruke nettet trygt. Det finnes programmer som sørger for pålitelig identifikasjon av nettsteder som er sikre, og nettsteder som ikke er det. Skadelige nettsteder som sprer skadeprogrammer eller stjeler den elektroniske identiteten din, identifiseres automatisk i bakgrunnen og du får en advarsel for å hindre at du utilsiktet åpner dem. Den generelle nettleserbeskyttelsen lar deg utforske internett fredelig og trygt.

Integrering i eget system

Ved å bruke VPN (Virtual Private Network) kan kunder koble sin eksisterende infrastruktur opp mot den leide infrastrukturen. Cloud Computing kan brukes som en del av et eget nettverk. En svakhet med systemet er at man er sårbar for driftsbrudd på f.eks. kommunikasjonslinjer og hardware feil. Avhengig av hvordan man har knyttet seg opp mot Cloud Computing, hva slags software og hardware-løsninger man bruker, er det ikke garantert at alle løsninger gir samme funksjonalitet til Cloud Computing.

Marston et al. (2011) hevder at bedrifter kan redusere sitt karbonutslipp, dersom de benytter seg av Cloud Computing løsninger. Zhu, Sun og Hu (2011) hevder at ved hjelp av automatisk provisjonering av virtuelle enheter, vil dette medføre redusert energiforbruk og dermed spare miljøet. Ettersom Cloud Computing er et innovativt produkt med innovative løsninger, med et fokus på miljøbesparelse så vil dette medføre at Cloud Computing bidrar til å redusere energibehovet samt skalerer ressurser etter behov. Zheng og Cai (2011) kommer frem til at ca. 30% av all strømforbruk er fra kjøling av maskinvare. Ettersom Cloud Computing produktet har fokus på å redusere karbonutslipp, har de en mulighet til å investere i gode og innovative kjøleteknikker. Dette er for å redusere eget strømforbruk og dermed redusere CO2 utslipp. En annen strategisk løsning på dette problemet er å plassere seg på en strategisk lokasjon, hvor tilbudet på stabil, miljøvennlig og billig strøm er tilgjengelig.

Nye applikasjoner

Cloud Computing muliggjør nye applikasjonsløsninger som tidligere ikke var mulig. Blant annet kan Cloud Computing benyttes til å tilby tjenester til mobile enheter der prosesseringskapasiteten er begrenset (Marston et al. 2011; Armbrust et al. 2009). Armbrust et al. (2009) nevner blant annet eksempler på mobile applikasjoner som

opererer med store datamengder i nåtid, noe som fører til at det blir vanskelig å kjøre slike applikasjoner alene på mobile enheter. Et eksempel på dette kan være nummeropplysningen 1881, hvor du får tilgang til alt fra telefonnummer, adresser og navn til bedriftsopplysninger. Både Marston et al. (2011) og Armbrust et al. (2009) legger frem forslag om tjenestekombinering som en stor mulighet. Her benyttes Cloud Computing til å samle data fra forskjellige tjenester og kombinerer de sammen for å få en ny tjeneste.

Svakheter:

Forhold til leverandør

Vanlig praksis er at det ikke lages kontrakt med bindingstid for Cloud Computing, men bare for den faktiske bruken. Filosofien er at kunden står fritt til å avslutte tjenesten, uten at dette medfører merkostnad. Utfordringen til kunden ligger i at mange funksjoner er knyttet opp til Cloud Computing leverandørens Application Programming Interface (API). API er koblingen mellom de ulike programvarene. Sultan (2010) henviser til at noen Cloud Computing leverandører tilbyr slike API'er til sine kunder, slik at de kan få benyttet seg av den fulle funksjonaliteten til Cloud Computing. Noen API'er er produsent-eid programvarer, og kan dermed bare benyttes dersom brukeren har betalt for lisensen. I motsetning til frie programvarer, har man ikke lov til å undersøke eller endre programvaren, samtidig som kildekoden er hemmelig. I tillegg kan lisensen ha begrensninger som er ment å sikre produsentens salgsinntekter, som forbud mot videreformidling. I noen tilfeller har brukeren ingen andre rettigheter enn å kjøre programmet på en bestemt datamaskin, og er låst til et bestemt produkt (Sultan, 2010). De leverandørene som ikke bruker standardløsninger låser fast kundene. Hvis kunden av ulike årsaker ønsker å bytte Cloud Computing leverandør så kan dette både bli tidskrevende og kostbart.

Ved å låse seg til en leverandør kan det ende med flere problemer som kan ha store påvirkninger for kunden. Dette blir illustrert i punktene under:

- Ved bytte av leverandør, vil den gamle leverandøren hjelpe til?
- Vil all data som har blitt lagret på Cloud Computing bli slettet?
- Hva med sikkerhetskopier?

Slike spørsmål vil være kritiske når kunder skal gå over til bruk av Cloud Computing. Armbrust et al. (2009) kommer frem med flere scenarioer der båndet til Cloud

Computing leverandører kan være en negativ affære. Blant annet ved at kunder er sårbare for eventuelle prisstigninger, noe som kan endre i hvilke grad Cloud Computing løsninger er lønnsomt. Et annet scenario er hva som skjer hvis leverandøren går konkurs. Vil den lagrede dataene bli slettet? Vil man få muligheten til å flytte dataene ut før de avslutter tjenesten, samt tid til å forflytte seg til en ny leverandør? Dette blir ekstra vanskelig dersom løsninger utviklet ved bruk av produsent-eid programvare (API 'er) er benyttet. Dette fører til at kunden må utvikle programvare eller løsninger som passer med en ny Cloud Computing leverandør. Slike spørsmål er spesielt viktige dersom bedriften bruker driftskritiske applikasjoner i den daglige driften.

Det kan få store konsekvenser for kunder som benytter slike leverandører, man er til en viss grad "låst" til nåværende leverandør. Man er avhengig av at leverandører vedlikeholder systemene og hele tiden er à jour med markedsutviklingen og at de har plattformer som ivaretar kundens behov.

Avtaler

Avtaler mellom en Cloud Computing leverandør og en kunde blir ofte omtalt som Service Level Agreement (SLA). Noen viktige punkter som en Cloud Computing avtale bør inneholde er:

- Formålet bør være angitt
- Beskrive hvordan personopplysningene skal behandles
- Konkrete rutiner for bruk av personopplysningene
- Regler for utlevering av personopplysninger
- Bruk av underleverandør skal reguleres i avtalen
- Ivareta den registrertes rettigheter
- Avtalen må pålegge databehandleren å ha tilfredsstillende informasjonssikkerhet
- Avtalens varighet
- Overføring til utlandet

En viktig og kritisk faktor er blant annet informasjon som "oppe tid" i prosent. Amazon Web Services skal ha en "oppe tid" på 99.95% (Marston et al, 2011). Det er kun et fåtall av bedrifter som har behov for større "oppe tid". Det er kun bedrifter/organisasjoner med bedriftskritiske applikasjoner som har behov for mer

"oppe tid". Eksempler kan være sykehus, flyselskaper, banker, forsvaret og andre store selskaper med 24 timers drift 365 dager i året.
Et annet problem som Armbrust et al. (2009) tar opp er misbruk. Dette dreier seg blant annet om hvordan kunder og ansatte misbruker systemet, i form av å sende ut søppelpost, virus, useriøse programmer eller sender linker til markedsføring av pornografi o.l. Dette føre til at IP adresser kan bli plassert i svartelister som igjen kan gjøre det vanskelig for noen bedrifter å fungere. Armbrust et al. (2009) tar også opp et problem med fordeling av ansvar når man flytter over til Cloud Computing. Cloud Computing leverandøren vil at ansvaret skal være hos kunden og ikke seg selv.

En annen utfordring er at når man overfører data vil det i grunn si at man også overfører eierrettighetene til dataene. Dette henger ofte sammen med at leverandører kan ha selskaper i mange land. Ikke alle lavkostland er like seriøse og har en mer liberal holdning til lover, regler, etikk og moral. Marston et al. (2011:183) sier: "*Consumers and businesses today not only own their data, but they also control how the data is physically housed. The distributive nature of Cloud Computing alters many notions about residency and ownership of data and information*".

Sentralisert plassering/tilgjengelighet

Marston et al. (2011) kommer frem med problemer som blant annet store politiske omveltninger, kriger og lignende. Datasentrene kan være plassert på steder hvor slike hendelser kan oppstå, dette kan være en stor trussel for bedrifter når de skal velge leverandør. Men merk at slike hendelser også kan skje dersom bedriften selv velger å ha systemet internt. Cloud Computing leverandører kan plassere datasentrene i geografiske områder som er relativt sikre, i motsetning til vanlige bedrifter som ofte plasserer datasystemet der de selv er lokalisert. Armbrust et al. (2009) hevder at dersom du vil ha en stor grad av sikkerhet, burde man benytte seg av flere forskjellige Cloud Computing leverandører samtidig. Dette er for å spre sikkerheten og få flere ben å stå på. Hvordan dette fungerer med virtuelle enheter er noe uvisst, men med aspekter som sikkerhetskopier kan dette være en sikker løsning. Grunnen til at Armbrust et al. (2009) foreslår bruk av forskjellige leverandører er at Cloud Computing ofte benytter seg av samme struktur eller programmer innad i selskapet.

Armbrust et al. (2009) tar frem et problem som også kan være sentralt. Cloud Computing leverandører har en kundedatabase som i seg selv skal være relativt isolert fra hverandre (i den form av at de er virtualisert og skilt fysisk mellom servere o.l.), men dette betyr ikke at man slipper unna andre problemer som blant annet DDOS (distributed denial-of-service attacks). Det som kan skje er at en av kundene til Cloud Computing leverandøren terger på seg eventuelle kriminelle organisasjoner med tilgang til store mengder datamaskiner, som ved et organisert angrep kan bombardere serverne med spam og/eller virus. Noe som igjen kan resultere i at de får problemer med å takle den mengden med data. Armbrust et al. (2009) sier at slike angrep blir enklere å håndtere for en Cloud Computing leverandør, da de som regel har de beste overvåkningssystemene og verktøyene til å håndtere slike angrep (Paquette, Jaeger & Willson, 2010). Dette er spesielt viktig for kunder som ønsker å holde på personlig informasjon og skal ha denne i Cloud Computing. Et eksempel på dette er kredittkortselskap og banker der flere uavhengige juridiske selskaper har behov for å utveksle sensitiv informasjon på tvers av landegrensene. Som Paquette et al. (2010:249) sier: "*If the vendor's servers span multiple countries, data access and distribution may very well be subject to the privacy laws and precepts of the host country that do not synch well with American regulations*". Selv om dette er sett i sammenheng med Amerika kan det oppstå eventuelle problemer for oss i Norge grunnet personvern, lover, etikk og moral. Svantesson og Clarke (2010) henviser også til at det ikke bare er problemer med å overføre mellom land, men at det også kan bli problematisk å overføre informasjon mellom forskjellige bedrifter.
Marston, Bandyopadhyay, Zhang og Ghalsasi et al. (2011:184) sier:
"*Cloud Computing raises new privacy issues that require clear standards for custodians of this information who received government request for access to that information*".

Båndbredde/flaskehalser ved overføring av data/responstid

Ulike bruksområder av Cloud Computing fører til forskjellig krav av ressurser. Noen benytter Cloud Computing for dens prosesseringskraft, andre for lagring. Slike forskjeller mellom bruksområdene kan utgjøre store utslag på både pris og opplevd nytte. Vi ser at bedrifter som kun benytter seg av Cloud Computing ifm. interne servere, ikke nødvendigvis har så store krav til høy hastighet på internett. Bedrifter

som f.eks. banker benytter seg av store mengder datautveksling og har et ekstremt stort behov for hastighet og 100% "oppe tid".

Man må merke seg at noen Cloud Computing leverandører tar betalt avhengig av hvor mye data som blir overført mellom deres tjenester, og dette kan fort bli en stor kostnadspost. Amazon er blant en av Cloud Computing leverandørene som benytter seg av "pris-matrise per gigabyte overført". Armbrust et al. (2009) kom frem til at det var rimeligere å sende fysiske harddisker enn å overføre alt over internett, samt at det var tidsbesparende. Men ettersom dette var i 2009 er ikke dette nødvendigvis like sentralt nå, og en kost/nytte analyse vil gi svar på hva som er mest lønnsomt for bedriften. Armbrust et al. (2009) gjorde beregningene basert på en overføringsmengde på 10 terabyte (1 terabyte = 1024 gigabyte) med en gjennomsnittlig hastighet på 20 megabit (mbit). Dette ville ta 45 dager å fullføre, og det sier seg selv at dette ikke hadde vært en lønnsom affære. Eksemplet viser at hvis en bedrift skal velge en Cloud Computing løsning, så er det viktig med grunnleggende analyse og behov/datamengde sett opp mot kost/nytte. Hvis det viser seg at Cloud Computing ikke er lønnsomt, må bedriften vurdere andre løsninger som tilfredsstiller behovet og er mer kostnads-effektivt.

Sultan (2010) nevner at responstid kan være en fare for Cloud Computing. Det er mange forhold som påvirker responstiden:

- Lokalisering av datasentrene
- Infrastrukturen (hos Cloud Computing leverandøren)
- Cloud Computing brukeren
- Internettleverandøren

Tap av fysisk kontroll

Kunder som benytter seg av Cloud Computing løsninger mister den fysiske kontrollen over dataene. Ifølge Marston et al. (2011) er det mange som er skeptiske ved tap av den fysiske kontrollen og infrastrukturen. Zissis og Lekkas (2010) forklarer at det tradisjonelt er mange som tror at dersom man kobler til noe utenom sin egen organisasjon eller sitt eget system, så blir dette et åpent vindu for uautoriserte brukere. Det er stor variasjon på de ulike pakkeløsningene som blir tilbudt fra Cloud

Computing leverandører når det gjelder sikkerhetsnivåer. Dette er både innenfor virtuelle enheter, data og kommunikasjonsløsninger.

Kjøper seg inn i eksisterende data struktur

Otey (2010) ser det som et problem at bedrifter kjøper seg inn i eksisterende infrastrukturer som er delt mellom flere brukere. Otey (2010) mener at dette kan føre til dårligere ytelse, spesielt i tider da systemet er mest brukt. Videre foreslår han at bedrifter som tenker på å benytte seg av Cloud Computing, prøver å finne leverandører med en Service Level Agreement (SLA) som kan garantere den ytelsen som kreves. I følge Paquette et al. (2010) oppstår det problemer hvis Cloud Computing kommer opp i 80 % av maks kapasitet. Dette er ifølge dem grunnet at serverne vil få for mye jobb med å flytte data mellom disker og minne, noe som fører til at maskinene kan få problemer med å svare. Dermed kan maskinene få ytelsesproblemer som igjen kan redusere kundens brukertilfredshet. Det er viktig at Cloud Computing leverandøren gjør gode estimater på behov og kalkyler. Leverandøren lager kalkyler på hva kostnadene blir ved maksimal bruk og det tas hensyn til fremtidig langsiktig vekst. Det er viktig for bedrifter som ønsker å benytte seg av Cloud Computing løsninger å finne frem til hvilke krav de har, om leverandøren har muligheten til å tilfredsstille disse kravene.

2.2.6 Sikkerhet

I de siste tiårene har det skjedd et radikalt teknologisk skifte i samfunnet. Tidligere var det de ansatte som overvåket og betjente de ulike arbeidsområdene. I dag blir anleggene fjernstyrt av komplekse IKT-systemer. Denne utviklingen har imidlertid utvidet trusselbildet, ved at eventuelle ”angrep kan gjennomføres når som helst, mot hvem som helst og fra hvor som helst”. Faktumet er at norske virksomheter og samfunnskritiske funksjoner blir oftere utsatt for kriminelle handlinger via de logiske kanalene. Samtidig rapporteres det fra flere hold at informasjonssikkerheten er sviktende i mange bedrifter (Røyksund, 2011).

Ut i fra ulike artikler vi har funnet på området ser vi at begrepet sikkerhet kan defineres på ulike måter. Whitman og Mattord (2011) definerer bl.a. sikkerhet slik:

”Beskyttelse av informasjon, kritiske komponenter og systemer som bruker, lagrer eller videreformidler informasjon.”

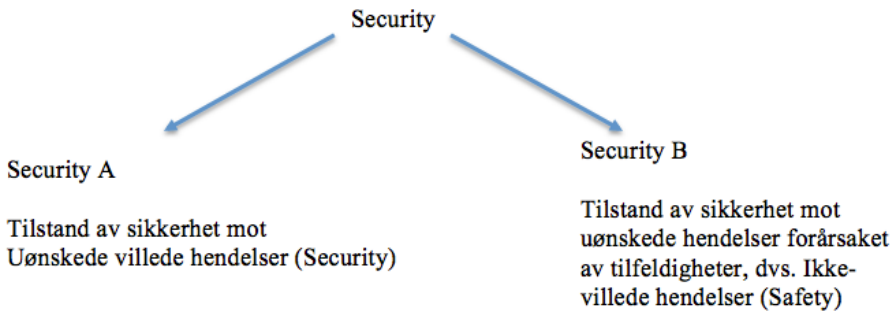
Det Whitman og Mattord (2011) mener er at når fysisk lukkede systemer blir sammenkoblet og går over til å bli åpne systemer, er det viktig å igangsette tiltak for å sikre informasjonen. Det er derfor viktig med robusthet i systemet. Robuste systemer er designet for å ikke la seg affektere av feil og unormal drift som det ikke har blitt tatt høyde for under design. Dette gjør systemene mer motstandsdyktige mot et større sett av angrep (Eriksen, 2013). Robusthet er definert slik:

"Et systems iboende egenskap til å endre sin virkemåte avhengig av ytre endringer eller forstyrrelser, slik at systemet kan fortsette sine operasjoner selv etter store uhell eller kontinuerlig høy last på systemet" (Eriksen, 2013).

Videre fant vi en annen god definisjon på Reference som går dypere inn i begrepet sikkerhet, det blir definert som:

"Security is the condition of being protected against danger or loss. In the general sense, security is a concept similar to safety. The nuance between the two is an added emphasis on being protected from dangers that originate form outside. Individuals or actions that encroach upon the condition of protection are responsible for the breach of security" (Reference, 2008)

Definisjonen som vi fant på Reference viser til forskjellen mellom begrepene sikkerhet og trygghet. Ut i fra definisjonen tolker vi sikkerhet som et teknisk begrep, mens f.eks. trygghet blir sett på som kundens trygghet til leverandøren, i form av kompetanse, økonomisk stabilitet etc.



Figur 1: Nyansen i begrepet sikkerhet ifølge NOU-2006-6

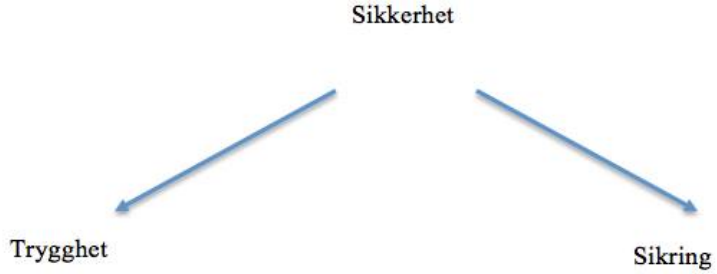
Da man på norsk har samlet de to engelske begrepene ”security” og ”safety” i et ord, kan det lett oppstå feiltolkninger dersom det ikke kommer klart frem fra konteksten hvilket av disse to det er snakk om. Forskjellen mellom sikkerhet og trygghet i definisjon av begrepet er diskutert i NOU (2006:6), se figur 1. NOU 2000 ”Et sårbart samfunn” har definert begrepet sikkerhet som noe mer overordnet. Trygghet blir her definert som:

” Sikkerhet mot uønskede hendelser som opptrer som følge av en eller flere tilfeldigheter.”

Mens sikkerhet blir definert som:

” Sikkerhet mot uønskede hendelser som et resultat av overlegg og planlegging.”

NOU (2006:6) tar her for seg forskjellen mellom hensiktsmessig skade og skade ved uhell. Videre i tråd med NOU (2006:6) foreslås det å dele det overordnede begrepet sikkerhet til trygghet og sikring:



Figur 2: Forslag til nyansering av sikkerhet ifølge NOU 2006:6

Ideen om å ta med sikring som en del av sikkerhetsbegrepet begrunnes i NOU(2006:6) med at det også kan brukes som et adjektivabstrakt, fordi sikring innebærer en tilstand eller en egenskap, og er sikkerhetsmessig forstått som en adjektivs avledning. Det kommer også frem av innledningen at man ikke finner støtte for dette i litteraturen om emnet, og at man ved bruk av denne må redegjøre for hvilken betydning man legger til grunn (NOU, 2006:6).

Ettersom de tidligere definisjonene vi fant på området var mer generelle, så har vi funnet en definisjon som dreier seg mer om informasjonssikkerhet. Innenfor norsk lovgivning (Personopplysningsloven, 2000) så er det tre aspekter og disse er:

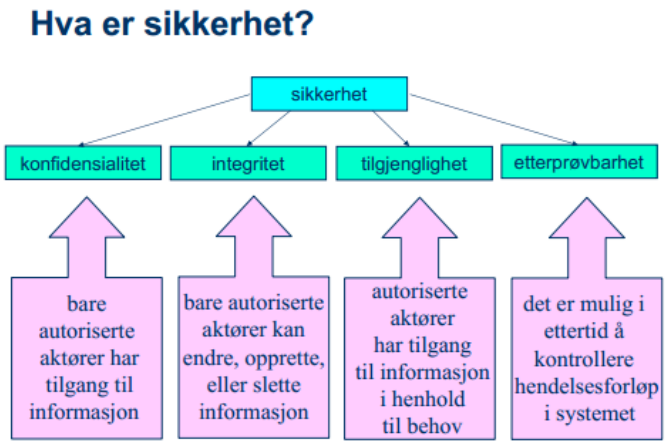
integritet (korrekte, oppdaterte og fullstendige data), konfidensialitet (data skal bare være tilgjengelig for de som har begrunnet behov for informasjon) og tilgjengelighet (det skal gis korrekt informasjon til riktig tid, innenfor fastsatte rammer). Panko (2004) brukte også denne inndelingen når han definerte begrepet IT-sikkerhet. Definisjonen til Panko (2004) (I Sinclaire, 2005:202) lyder slik:

"Corporate IT security is defined by three general security goals: confidentiality, integrity and availability."

Videre valgte Soo Hoo (2002) å definere begrepet ved å konseptualisere det ved hjelp av fire dimensjoner:

"Availability, integrity, authenticity and confidentiality."

Sjefsforsker Kjetil Stølen (2006) fra SINTEF snakker rundt sikkerhet, her kommer det også frem klare likhetstrekk med Panko (2004) sin definisjon. Eneste forskjellen er at Stølen (2006) tar med seg etterprøvbarhet. Med etterprøvbarhet skal det være mulig å kontrollere hendelsesforløpet i systemet i ettertid (Stølen, 2006). Stølen (2006) illustrerer ulike aspekter av sikkerhet i modellen under.



Figur 3 : Ulike sikkerhetsaspekter (Stølen, 2006)

Ettersom vi nå har vært gjennom en rekke ulike definisjoner på området, ser vi at det er hensiktsmessig for oss å avgrense oppgaven til sikkerhet (security) og ikke trygghet (safety). Dette er fordi det hovedsakelig dreier seg om frykten for at sensitiv

pasientinformasjon skal komme på avveie. Derfor vil vi etterhvert se på informasjons-sikkerhet.

2.3 Holdningsteori

Nå har vi definert begrepene ekspansjon, Cloud Computing og sikkerhet. Videre vil vi se på begrepet holdning med basis i avhandlingens problemstilling. Sikkerhet er et av de mest kritiske forholdene i forbindelse med etablering og bruk av Cloud Computing. Potensielle kunders holdninger til Cloud Computing og sikkerhets-aspektet ved dette teknologiske konseptet blir avgjørende for viljen til å ta det i bruk. Vi har funnet flere modeller gjennom vår litteraturgjennomgang hvor begrepet holdning blir brukt, senere i dette kapittelet vil de ulike modellene bli definert. Videre vil vi se på ulike definisjoner til holdning, samt hvordan holdningen er til informasjonssikkerhet innenfor Cloud Computing.

2.3.1 Begrepet holdninger

Holdningene vi mennesker har er ikke tilfeldige, disse har ulike funksjoner for vår personlighet. Denne "funksjonelle" problemstillingen har blitt presentert i flere ulike forskningsprosjekter (Katz, 1960; Mann, 1972; Kahle, 1984; Eagly & Chaiken, 1993). Det ser likevel ut til å være enighet om hvilke funksjoner som er sentrale.

Hva er egentlig holdninger? Ajzen (1988:4) definerer dette som *"An attitude is a disposition to respond favorabel and unfavorable to an object, person, institution, or event"*. Så teoretisk sett er holdninger sammensatt av flere underliggende komponenter som kan knyttes opp mot en persons oppfatning av og følelser overfor et objekt, samt personens atferd i forhold til objektet (Ajzen & Fishbein, 1980; Sørum, 2012).

Bohner & Wanke (2002) har også sett på personers holdninger, de antar at en persons holdning kan forutsi atferd. Ajzen (1988) nevner objekt i sin definisjon på holdning, innenfor holdningsteori kan begrepet objekt være en ting, et menneske, en vare, et livssyn, en tjeneste, et dyr, et land eller bestemte handlinger som personer kan knytte opp mot positive eller negative følelser. Blindheim og Sætrang (1991) er inne på dette og stiller spørsmål om hvordan disse følelsene fører til en bestemt handling, hvordan disse følelsene påvirkes og om en holdning er et resultat av en handling. Ås (1992)

forklarer at holdninger er et begrep som brukes av sosialpsykologer for å beskrive og forklare menneskelig atferd.

Ifølge Ås (1992) består holdninger av tre hoveddeler. Den første delen er en kunnskapsdel, her ligger troen på at når mennesker blir fortalt hva som er farlig og skadelig for dem, så vil de endre seg og gjøre det rette. Den andre delen er følelser, disse er en like viktig del av holdningene som kunnskapen er. Videre sier Ås (1992) at følelseskomponenten av holdningene ofte holder den gamle atferden fast i et system av tilstøtende meninger og handlinger. Den siste og tredje komponenten i holdninger er handling. Når man utfører meningsundersøkelser er dette for å få et grunnlag for å kunne forutsi hva folk vil gjøre (Christensen, Kristensen og Sætre, 2000).

2.3.2 Forbindelsen mellom holdninger og atferd

Et tema forskere innenfor sosialpsykologien lenge har vært opptatt av, er å finne ut hvordan holdninger og atferd henger sammen. Tidligere forskning på holdning har blitt kritisert for den tilsynelatende mangelen på sammenheng mellom målte holdninger og den faktiske atferden. Det har vært foretatt flere undersøkelser som bekrefter at det er lite samsvar mellom holdninger og atferd. Et kjent eksempel er LaPieres undersøkelse fra 1934. Her ble et kinesisk par nektet servering i bare en av 251 restauranter i USA. Seks måneder senere fikk de samme restaurantene tilsendt et brev som avslørte at hele 92 % av disse sa at de ville nekte et kinesisk par adgang. Her samsvarte ikke den faktisk atferden med de uttrykte holdningene (Mann, 1972).
Forklaringen på denne manglende forbindelsen mellom atferd og holdning kan forklares med at atferd ikke bestemmes av holdninger alene, men også av mange andre faktorer (Mann, 1972).

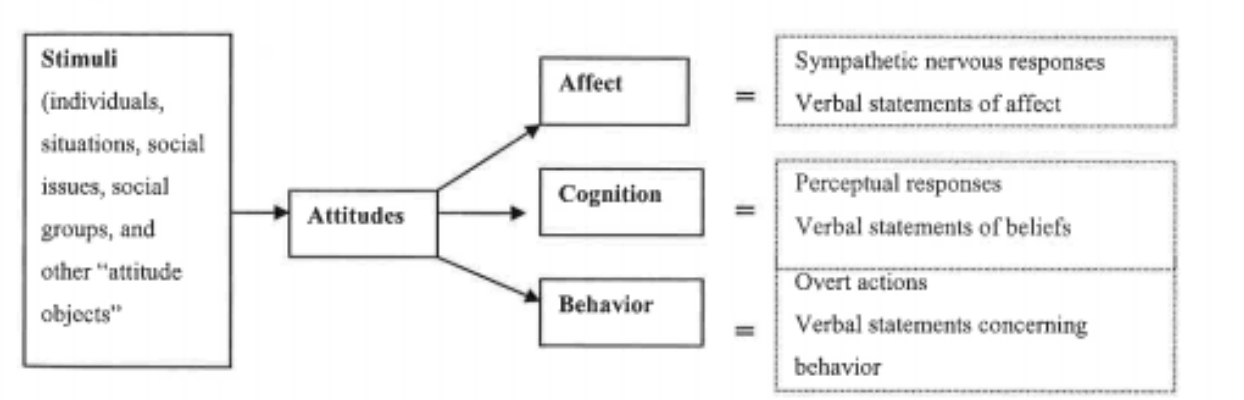
2.3.3 Holdningsteori og modeller

Som vi har nevnt tidligere sier Ås (1992) at holdninger består av tre deler. I 1960 utarbeidet Rosenberg og Hovland en modell som tar for seg tre måter å tolke en holdning på, denne blir kalt trekomponentmodellen (se figur 4). Ifølge Rosenberg og Hovland (1960:3) går denne holdningsteorien så langt tilbake som til år 1908, da var det McDougall som så på disse tre sidene rundt begrepet holdning. Ajzen og Fishbein (1980:13) mener at det var Thomas og Znaniecki (1918) som brukte holdnings-

begrepet for første gang for å forklare sosial handling. De så på holdninger som en mental prosess som bestemte en persons atferds respons.

2.3.4 Trekomponentmodellen

Rosenberg og Hovland (1960:1) definerer holdning som ”*predispositions to respond in a particular way toward a specified class of objects”.* Ser man på begrepet holdning så kommer det frem ulike typer stimuli på den ene siden og flere respons-typer på den andre siden. I følge Ajzen og Fishbein (1980:19) så blir all respons på et stimuli formidlet av personens holdninger til objektet



Figur 4: Rosenberg og Hovlands ”Trekomponentmodell”

I modellen til Rosenberg og Hovland (1960:1) sier de at ettersom holdninger (attitudes) er predisponerte så vil ikke disse være direkte observerbare eller målbare. De vil altså bli påvirket av hvordan vi reagerer på det spesielle stimuliet. Andre som deler dette synet på at holdninger ikke kan observeres direkte er Bohner og Wänke (2002:19), men de mener at den beste måten å måle begrepet på er å spørre direkte. Modellen til Rosenberg og Hovland (1960) skiller de forskjellige responsene på et holdningsobjekt i tre kategorier, disse er kognitive, affektive og atferdsmessige responser. Disse tre komponentene blir tolket slik:

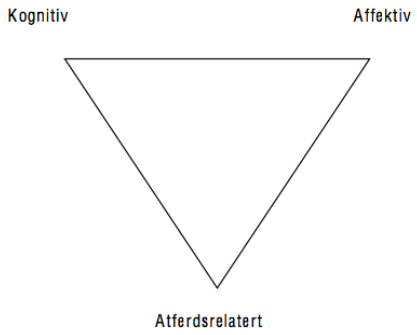
Affektive *(affect)* er emosjon som innebærer følelser og drifter. De affektive responsene blir ofte beskrevet som oppfatninger knyttet opp mot de følelsesmessige uttrykkene som kan oppstå mellom holdningsobjektet og dets egenskaper. Disse egenskapene som blir forbundet med holdningsobjektet kan resultere i en negativ, positiv eller nøytral oppfatning av holdningsobjektet (Ajzen og Fishbein, 1980; Blindheim og Sætrang, 1991; Sørum, 2012).

Kognisjon *(cognition)* handler om meninger, tro og tanker. En litt mer utdypende beskrivelse er at de kognitive responsene bygger på personens oppfatning av et holdningsobjekt og hva denne personen uttrykker om sine tanker rundt holdningsobjektet. Disse responsene blir beskrevet som oppfatninger knyttet til forbindelser, tanker og assosiasjoner som vil oppstå mellom holdningsobjektet og dets egenskaper (attributter). I likhet med de affektive responsene, vil også egenskaper som er forbundet med holdningsobjektet resultere i en negativ, positiv eller nøytral oppfatning av holdningsobjektet (Ajzen og Fishbein, 1980; Blindheim og Sætrang, 1991; Sørum, 2012).

De atferdsmessige responsene (*behavior)* handler om intensjon, atferdstendens og sannsynlighet for handling. Disse responsene er bygget på hvordan en person oppfører seg i forhold til holdningsobjektet og hva personen sier om holdningsobjektet. Responsene som oppstår kan resultere i en observerbar atferd ved at personen enten jobber aktivt imot eller for holdningsobjektet. Som tidligere nevnt omkring de kognitive og affektive responsene, så vil også de atferdsmessige responsene kunne vise en negativ, positiv eller nøytral oppfatning av holdnings-objektet (Ajzen og Fishbein, 1980; Blindheim og Sætrang, 1991; Sørum, 2012).
Det er uenigheter blant teoretikere om hvilke av de tre komponentene som er viktigst i trekomponentmodellen. Noen teoretikere mener at det er den kognitive komponenten som er viktigst, mens andre mener at det er den emosjonelle komponenten som er avgjørende. Ifølge Blindheim og Sætrang (1991) er det fullt mulig å argumentere for at den kognitive delen av holdningen er overflaten av den og at den sanne holdningen først blir synlig gjennom handling (konasjon).

Et problem som kan dukke opp er at handlingsdelen og tankedelen kan komme i konflikt med hverandre (Blindheim og Sætrang, 1991:125). Blindheim og Sætrang (1991) kommer med et eksempel på denne konflikten: man kan i utgangspunktet ha positive holdninger til en annen rase uten at man har noe nært forhold til et bestemt menneske fra denne rasen. Blir man f.eks. presentert for en fremtidig svigerdatter fra en annen kultur, så behøver ikke de tidligere positive følelsene for andre raser å bety så mye.

De tre responsene i trekomponentmodellen bør sees i en sammenheng, fordi en holdning kan f.eks. dannes på grunnlag av en respons og deretter bli integrert med de andre responsene (Ajzen og Fishbein, 1980; Sørum 2012).



Figur 5: Ajzen og Fishbein (1980) "Trekomponentmodell"

2.3.5 Studier i forhold til de ulike komponentene i trekomponentmodellen

I Rosenberg og Hovland (1960) sin bok er det nevnt at det er gjort mye forskning rundt de tre komponentene i trekomponentmodellen. Vi vil nå ta for oss de ulike komponentene.

Kognisjonskomponenten

Katz og Braly (1933) gjorde en studie av kognisjonskomponentmodellen der funnene deres viste at fordomsfulle informanter hadde merkbar lik måte å behandle medlemmer i ikke-velansette etniske grupper på. Videre gjorde Harding, Kutner, Proshansky og Chein (1954) en litteraturstudie basert på flere studier der Katz og Braly`s (1933) prosedyrer ble brukt for å studere de kognitive "normene" som er assosiert med fordommer (Rosenberg og Hovland, 1960). Kramer (1949) og Hartley (1946) utførte studier hvor det ble presentert funn som
viste at grupper som har ulik grad av tydelighet kan ha like fiendtlige holdninger.

Affektkomponenten

Ifølge Rosenberg og Hovland (1960) så er evaluering av affektkomponenten den mest sentrale for flertallet av forskerne. De fleste av forskerne har brukt en eller annen form av affektkomponenten i undersøkelsene, noen studier som bekrefter dette er

gjort av Harding et al. (1954), Green (1954) og Hovland (1954) (i Rosenberg og-Hovland, 1960). Noen forskere har vektlagt viktigheten av følelsen om å være for eller imot noe, altså en positiv eller negative affekt (Krech og Crutchfield, 1948)

Atferdskomponenten

Rosenberg og Hovland (1960) mener at det er gjort færrest studier når det kommer til denne komponenten og atferd er den minst brukte komponenten som hovedindeks for holdning. Studier gjort av Schanck (1932), LaPiere (1934) og Cartwright (1949) (i Rosenberg og Hovland, 1960) viser at forskere har konkludert med at "overt action" sett i forhold til et objekt, ikke bare reflekterer holdninger frembragt av objektet, men den er også influert av andre variabler.

Kritikk mot trekomponentmodellen

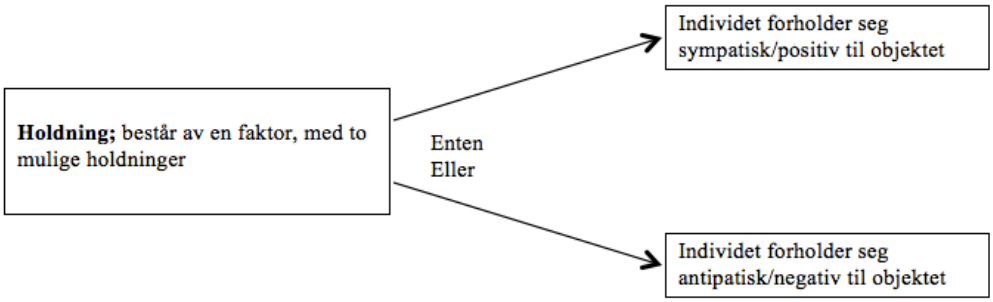
Blindheim og Sætrang (1991) skriver i sin bok at: *"Kritikerne av trekomponent-modellen hevder at dersom det skal være noe poeng å snakke om holdninger som er noe forskjellig fra tanker, følelser og handlinger, må det være en bestemt side av den emosjonelle delen vi prater om. Dvs. Hvorvidt et individ forholder seg sympatisk eller antipatisk i forhold til et objekt Det er mindre interessant om disse positive eller negative følelsene dreier seg om kjærlighet, hat, kvalme eller appetitt."*

Det vil alltid dukke opp kritikk til ulike modeller, denne modellen er ingen unntak. Det finnes flere innvendinger mot modellen og holdningsbegrepets inndeling i tre komponenter. Petty og Wegener (1998) kommer med dette utsagnet: *"That is, if one`s affect changes, one`s cognitive reponses and behavioral tendencies typically changes as well"*. Andre forskere mener at det ikke nødvendigvis er mulig å skille de tre komponentene fra hverandre, og de behøver nødvendigvis ikke å representere tre uavhengige faktorer (Katz og Stotland, 1959 i Bohner & Wänke, 2002).

2.3.6 Enkomponentmodellen

Trekomponentmodellen går ut i fra at holdning kan ha tre dimensjoner. Enkomponentmodellen ser på begrepet holdning i sin enkleste form, som er enten positive eller negative holdninger. Utgangspunktet til denne modellen er om man forholder seg positivt eller negativt til et objekt. Blindheim og Sætrang (1991) har

kommet frem til ulike svakheter ved denne modellen. Det konkluderes med at det er lite som blir fortalt om årsakene til hvorfor man er positiv eller negativ.



Figur 6: "Enkomponentmodellen", tegning hentet fra Kunnskapssenteret

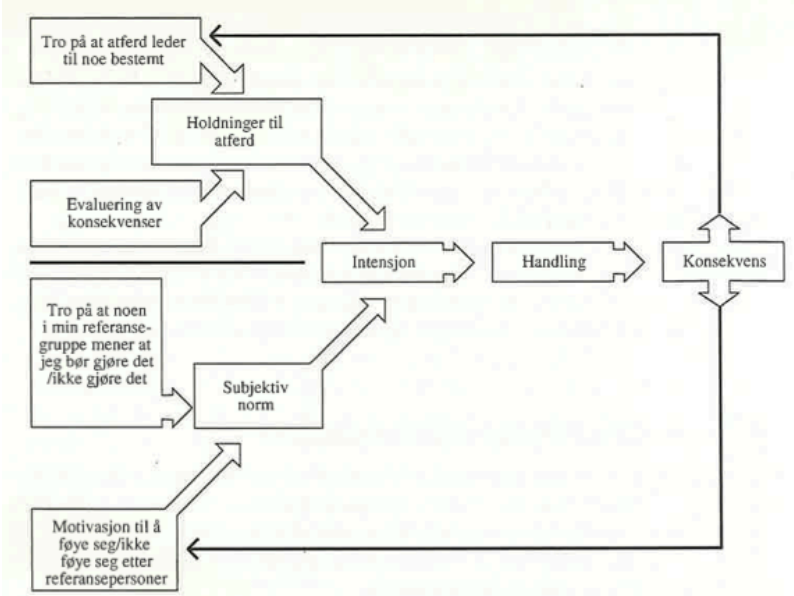
Blindheim og Sætrang (1991) bruker et eksempel der de tar utgangspunkt i individer fra jødiske trossamfunn. De gir leserne et eksempel på at man må trekke inn kulturelle, historiske og kognitive variabler for å få en full forståelse av bakgrunnen og konsekvensene av for eksempel et antipati. At mennesker er positive eller negative til et objekt betyr at man bruker en evalueringskomponent. Evaluering er det vi lagrer, gjerne uten affekt- og kognisjonsaspektet (Scholl, 2002). Evaluering blir gjerne sett på som en funksjon av de tre dimensjonene i trekomponentmodellen, kognisjon, affekt og atferd.

2.3.7 Multikomponent-modeller

Det kan være en tanke å bruke modeller med forskjellige antall komponenter for å kunne forstå holdninger til ulike objekter. Som tidligere nevnt har vi modeller som er evaluerende som enkomponentmodellen, der det er negativ vs. positiv, eller modeller som trekomponentmodellen som tar for seg affektive, kognitive og atferds-komponenter (Rosenberg og Hovland, 1960).

Vi vil fokusere på modeller som brukes innenfor IT, ettersom Cloud Computing er et IT produkt. Nå vil vi se på teorien "Theory of reasoned action" (TRA), denne teorien ble lagt frem av Fishbein i 1967 og har siden den gang blitt testet og endret opptil flere ganger. TRA teorien er brukt i ulike retninger for å kunne forstå forbrukerne og deres holdninger. Denne teorien kommer i utgangspunktet fra sosialpsykologiteorien. Det som skiller denne modellen fra andre modeller er at den beskriver holdning til

atferd, ikke holdning til objekt. Dette betyr i markedssammenheng holdning til kjøp og bruk av en vare, tjeneste eller idé (Sætrang og Blindheim, 1991).

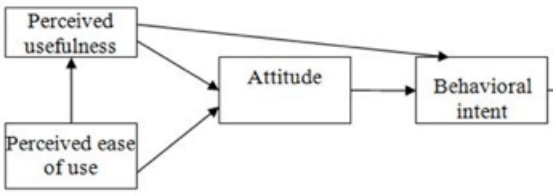


Figur 7: "Fishbein-modellen" (Theory of reasoned action- TRA)

Sætrang og Blindheim (1991) sier *at "Fishbeins modell er interessant, fordi den belyser hvordan trosmessige, evaluerende, sosiale, motivasjonelle, viljemessige og situasjonsbetingede variabler påvirker holdning til atferd og viljen til å utføre den (intensjon)*. Videre sier Sætrang og Blindheim (1991) at modellen måler intensjonen om f.eks. kjøp av noe, istedenfor holdningen til noe. De mener derfor at intensjonen forutsier atferden bedre enn holdningen.

2.3.8 Technology Acceptance model og holdning

TRA teorien bringer oss mot en annen modell som er mye brukt innenfor IT, denne blir kalt "Technology Acceptance Model", og forkortes til "TAM". Ser man på forskningen som har vært gjort innenfor informasjonssystemer, så har forskere brukt TRA som et utgangspunkt for TAM (Malhotra og Galetta, 1999)



Figur 8: "Technology Acceptance Model", av David 1985

I følge Davis (1989) sier TAM i sin enkleste form at nytten ved teknologien er den sterkeste påvirkningen på om teknologien tas i bruk, mens hvor lett teknologien er å bruke har mindre betydning. Videre sier professor ved UiO Jens Kaasbøll (2009) at ”*TAM kan brukes til å forutsi at et IT system som oppleves som nyttig av brukerne vil bli brukt, selv om de må slite med å lære det. Omvendt, et system som er lett å lære og lett å bruke, vil ikke bli brukt dersom folk ikke ser nytten av det”*. Modellen har vært mye brukt for blant annet å teste IS-suksess og brukeraksept. Det blir ofte brukt en positiv-nøytral-negativ likertskala i undersøkelser der holdning i forhold til bruken av informasjonssystemer blir målt.

Tidligere har vi nevnt det generelle rundt begrepet holdning, nå vil vi gå mer detaljert inn i begrepet i forhold til informasjonsteknologi. Begrepet holdning har vært mye brukt innenfor tradisjonell forskning av informasjonssystemer (Glassberg, Grover og Teng, 2006). Noen forskere har fokusert på atferd (Laaksonen, 1994, Laurent & Kapferer, 1985, i Glassberg et al, 2006) mens andre fokuserte mer på det kognitive aspektet (Davis, 1985, Davis et al, 1989; Mathieson, 1991; Taylor & Todd, 1995, i Glassberg et al, 2006.) Glassberg et al. (2006) tar opp spørsmålet ”Does measuring attitude help our ability to predict technology use?”
Bjerkheim (2008) har laget en tabell som gir en oversikt over ulike undersøkelser som er blitt gjort (tabell 1) der forskerne har tatt utgangspunkt i TAM, og bruker begrepet holdning som en av de uavhengige variablene.

Forsker	Tittel	Årstall	Tema
Pavlou & Fygenson	Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior	2006	Holdning som begrep i en undersøkelse som tok for seg aksept av elektronisk handel. Begrepet holdning blir her brukt i forhold til å hente inn informasjon og handle fra web-sider.
Wixiam & Todd	A Theoretical Integration of User Satisfaction and Technology Acceptance	2005	Her mener forskerne at holdninger basert på objektive vurderinger, er dårlige mål på reell handling. Det har vært brukt en kombinasjon av TAM og TRA, hvor holdning påvirker intensjon i forhold til tilfredshet og aksept.
Bhattacherjee & Premkumar	Understanding Changes in Belief and Attitude Toward Information Technology Usage: A Theoretical Model and Longitudinal Test	2004	Holdning som begrep i en studie hvor de forsker på endringer i holdninger i forhold til bruk av informasjonsteknologi.
Plouffe et al.	Richness versus parsimony in modeling technology adaption decisions – understanding merchant adoption of a smart card-based payment system	2001	Holdning som begrep i forhold til aksept av et smartkort-betalingssystem
Taylor & Todd	Understanding information technology usage: a test of competing models	1995	Her har de testet tre modeller i forhold til å forstå informasjonsteknologi. TAM ble testet opp mot to variasjoner av TPB. Holdning er operasjonalisert gjennom Perceived usefulness og Perceived ease of use

Tabell 1: Studier med bruk av TAM

I 2006 utførte Jeyaraj, Rottman og Lacity en litteratur studie, hvor de gir leseren en oversikt over ulike variabler som er brukt i 51 empiriske studier på organisasjonsnivå og 48 studier på individnivå om IT-innovasjon og aksepteringen av denne. De kom frem til at holdninger ble brukt som uavhengig variabel 13 ganger, i ni av tilfellene resulterte dette i signifikante sammenhenger. Det var to andre uavhengige variabler

som var mer brukt i disse undersøkelsene, dette var ”Ease of Use” (brukervennlighet) og ”Perceived Usefulness” (oppfattet nytte). Selv om problemstillingene i eksemplene er annerledes enn den vi har, så nevner vi disse for å vise at holdning er et kjent begrep innenfor teorien rundt informasjonsteknologi. Vi vil nå gå videre å knytte dette sammen og relatere det til vår problemstilling.

2.4 Holdninger til informasjonssikkerhet

I de foregående kapitlene i oppgaven har vi definert begreper som er sentrale og nært knyttet opp mot vår problemstilling. Vi har nå kommet til et punkt hvor det er hensiktsmessig å se på hvordan disse begrepene fungerer sammen. I mange studier er det påvist at sikkerhet er et følsomt tema, selv om det ifølge Meese (2007:2) finnes store mørke tall i forbindelse med offentliggjøring av sikkerhetsbrudd. Dette ser man til stadighet at det blir skrevet om i ulike aviser og tidsskrifter. Offentlige organisasjoner som f.eks. sykehus skal behandle opplysninger om pasienter konfidensielt, mens andre bedrifter skal tjene penger. På denne måten kan det oppstå konflikter mellom kost og nytte av ulike sikkerhetsløsninger.

Mange hevder at de må leve uten sikkerhetssystemer for at systemene deres skal fungere optimalt, hos enkelte regnskapsfirmaer så er det slik at de må skru av sikkerhetssystemene for at regnskapssystemene skal fungere. Når dette er tilfellet så skaper sikkerheten en begrensning i det å tjene penger i en bedrift (Søiland, 2007). Systemene bør også være så brukervennlige at ansatte eller personer som benytter sikkerhetssystemer ser fordelen ved å bruke dem. I følge Braz og Robert (2006:199) har det vært et problem mellom sikkerhetsnivå og brukervennlighet, og her bør man prøve å finne et balansepunkt.

2.4.1 Forskjellige temaer innenfor informasjonssikkerhet

Innenfor emnet informasjonssikkerhet finnes det mange aspekter, som tidligere beskrevet består det både av en teknisk del og en menneskelig del. Vi har hentet en tabell fra MIS Quarterly (Knapp, Marshall, Rainer og Ford, 2005:6). I tabell 2 har de rangert hvilke ulike sikkerhetstemaer som er viktigst for deltakerne i undersøkelsen, som er henvist til i forhold til tabell 1. I tabellen under har vi en liste med 10 punkter hvor holdningsrelaterte temaer er rangert som nr 6.

Rangering	Informasjonssikkerhetstema
1	Støtte fra toppledelsen
2	Trening og opplæring i brukeroppmerksomhet
3	Ødeleggende programvare
4	Oppdateringsrutiner
5	Sårbarhets- og risikoadministrasjon
6	Holdningsrelaterte temaer
7	Organisasjonskultur
8	Tilgangskontroll og identifiseringsadministrasjon
9	Trusler innenfor bedriften
10	Forretningskontinuitet og forberedelser i forhold til katastrofer

Tabell 2: MIS quarterlys rangering over hva som blir sett på som mest viktig i forbindelse med sikkerhet innenfor IT sikkerhet

Vi ser i tabell 2 at det er flere sikkerhetsaspekter og at disse aspektene er både på organisasjons- og individnivå. På toppen av listen ser vi at det er toppledelsen som er høyest rangert. Dette er noe som er interessant ifm. vår problemstilling, ettersom vi skal intervjue ledelsen i den norske helsesektoren.

De som arbeider og forsker på informasjonssikkerhet, er helt klare på at det ikke er bra nok å ha gode tekniske sikkerhetsløsninger. Dette fordi det er den menneskelig delen som er den viktigste, og da er det sett både innen- og utenfra bedriften. Ut i fra MIS Quarterlys sin rangeringstabell ser vi at trusler innad i bedriften er nevnt. Steele og Wargo (2007:23) mener at det er i forhold til "insiders" at utfordringen til sikkerhetstruslene ligger. Steele og Wargo (2007) definerer "insiders" som betrodde mennesker som besitter fortrolig kunnskap om indre anliggender i bedriften med tilgang til bedriftens sensitive data og ressurser. Hackere bruker ifølge Adams og Sasse (1999:41) mer tid på den menneskelig delen av sikkerhetskjeden enn hva sikkerhetsdesignere gjør.

”Sikkerhetsløsninger er ikke sikrere enn det svakeste leddet i kjeden, og ved å øke folks bevissthet ift bruk og innhold i systemene, vil deres ønske om å ettersøke bedre innføring øke og de vil lettere krever forbedring eller tilbaketrekning av systemene.” (Rogerson, 2002:2).

I følge sitatet over er informasjonssikkerhet først og fremst et menneskelig problem, dette blir også bekreftet av sjefsredaktør i ”Computers & Security”. I en artikkel skriver han at det nå finnes så mange gode tekniske sikkerhetsløsninger at det ikke behøver å være så stor fare for sikkerhetsbrudd. Likevel så stiller han spørsmålet, hvorfor er det allikevel slik? Sjefsredaktøren mener han vet svaret*: “I suspect that the primary reason is that information security is primarily a people problem, not a technical problem.”* (Schultz, 2005:425). På bakgrunn av dette etterlyser han mer forskning på temaet: *“A good start would be to publish more papers on this subject; I strongly encourage you, the readers, and your colleagues to submit such papers.”* (Schultz, 2005:426).

2.4.2 Ulike studier innen informasjonssikkerhet

Artikkelsøket på vårt temaområde var ikke enkelt, men til slutt så fant vi en review av en artikkel publisert innenfor vårt temaområde. Studien dreide seg om artikler som var blitt publisert i Nord-Amerika, hvor artiklene ble publisert i fem tidsskrifter:

- Communication of the ACM
- Information & Management
- Informations systems Management
- Journal of Management Information Systems (over en to års periode).

Forfatterne av artikkelen hadde delt litteratursøket inn i to deler:

1. Artikler som omhandler informasjonssikkerhet
2. Artikler som omhandler personvern

Vi hadde stor nytte av å lese artiklene på området, ettersom artiklene konkluderte med noe av det samme som oss. Konklusjonen vår er at det er gjort for lite undersøkelser på området, det er derfor behov for mer forskning, spesielt på organisasjonsnivå (Sinclaire, 2005:202).

Det finnes også en mer tradisjonell form for informasjonssikkerhet. Den tradisjonelle informasjonssikkerheten har vært på den tekniske siden, dvs. at man kan ha oversett den menneskelige delen, og at det er mennesker som er hoveddelen i et informasjonssystem. Derfor er det ikke alltid like logisk at det er menneskelig svikt som er årsaken. I følge Hitchings (1995:377) så søkes det etter en metode som tar for seg det menneskelige aspektet i et helthetlig perspektiv.

I tabell 3 har vi tatt for oss noen eksempler på studier som dreier seg om sikkerhet i forbindelse med informasjonssystemer, hvor begrepet holdninger er tatt med som et målbart begrep. Som vi ser i tabellen så er TAM brukt som utgangspunkt, samtidig som det også er andre tilnærminger fra de andre artiklene. Det er veldig interessant å se hvilke vinklinger ulike forskere bruker når de skal tilnærme seg begrepet sikkerhet i sine studier. En annen ting som er interessant er å se hvordan de har valgt å fremstille begrepet holdninger og hvilke spørsmål de har valgt å ta med i undersøkelsene.

Årstall	Tema	Tittel Forsker
2006	Empirisk studie. Bruker en kombinasjon av kvalitativ og kvantitativ tilnærming. Tar for seg holdninger i forhold til sikkerhet ved bruk av mobiltelefon. *"The aim of the survey was to explore the relationship between the mobile phone user's awareness, attitude and adoption of mobile phone security functions among different adopter categories. Do the end-users understand security functionality? To what extent is security functionality used? What interest is there in existing and future security functionality*".	"Customers's awareness of, Attitudes Towards and Adobtion of Mobil Phone Security". By: Stewart Kowalski og Mikael Goldstein.
2006	Dette studiet tok for seg TAM og ser på kunders holdninger (intensjoner) om å akseptere nettbank.	"Adoption of Internet Banking: An Empirical study in Hong Kong" By: Cheng et al.
2005	Dette er en teoretisk artikkel som forteller om en undersøkelse som ikke er gjort ennå. Artikkelen sier at undersøkelsen skal ta for seg TAM og skal se på hvordan organisasjoner kan påvirkers til å investere mer i sikkerhet.	"The Technology Acceptance Model and the Decisions to invest in Information Security". By: Alice M. Johnson
2004	Denne studien tar for seg det menneskelige aspektet ved sikkerhetsløsninger, ved at de mener at effektive løsninger ikke bare baserer seg på tekniske egenskaper, men også på menneskelige muligheter til å forstå og bruke dem. Holdning blir diskutert under uttrykkene Ftustration, Futility and Pragmatisem.	"Security in the wild: user strategies for managing security as an everyday, practical problem". By: Paul Dourish et al.

Tabell 3: Oversikt over ulike studier innenfor IS, hvor holdning er en variabel

2.4.3 Er begrepet bevissthet synonymt med begrepet holdninger innenfor informasjonssikkerhet?

I vårt litteratursøk om informasjonssikkerhet, fant vi ut at det var flere studier som tok for seg begrepet "awareness". Etter en diskusjon med vår rådgiver i CSC og andre referanser kom vi frem til at dette betydde bevissthet, dette blir bekreftet av definisjonen under.

Korb, Gorell og Van De Riet (1989:5) definerer ”awareness” som ”*individets oppmerksomhet på seg selv og omgivelsene, samt på relasjonen mellom seg og omgivelsene”.*

Videre ser vi derfor på kombinasjonen mellom ”security” og ”awareness”.
Wikipedia definerer (2013) “security awareness” som:
”Is the knowledge and attitude members of an organization possess regarding the protection of the physical and, especially, information assets of that organization”.

Vi fant også en definisjon på *The Information Security Forum*, hvor de definerer bevissthet i forbindelse med informasjonssikkerhet som: “*An ongoing process of learning that is meaningful to recipients and delivers measurable benefits to the organization form lasting behavioral change.”* (ENISA, 2007:3)

En annen definisjon vi fant på området dreide seg om bevissthet ifm. informasjonssikkerhet, hvor begrepet forståelse også var tatt med: *”Specific activities should be preformed to promote security awareness (the extent to which staff understand the importance of information security, the level of security required by the organization and their individual security responsibilities – and act accordingly) across the Enterprise”* (ISF, 2005:78)

Hvis man sammenligner begrepene bevissthet og holdning, ser vi at begrepet holdning kan være litt for ”enkelt” når det gjelder behandling av spørsmål rundt informasjonssikkerhet. Hvis du ser på den engelske varianten av begrepet, ser vi her at det går mer inn på om man er positivt eller negativt stilt til noe, mens bevissthet er noe som er bredere. Når man er bevisst på noe så betyr det at man har kunnskap om noe, man spør om hva som skjer og hvorfor. I vårt tilfelle er vi i tvil om det vil være tilfredsstillende å kun spørre om intervjuobjektene våre har en positiv eller negativ holdning til informasjonssikkerhet innenfor Cloud Computing.

Undersøkelser som er gjort i forbindelse med å måle bevissthet ovenfor informasjonssikkerhet, viser at bedrifter og organisasjoner som deltok i undersøkelsen la ned mye arbeid i å øke bevisstheten rundt informasjonssikkerhet. Videre brukte de dette for å forbedre holdningene mot informasjonssikkerhet. Dette er interessant fordi

det bekrefter våre antakelser om at bevissthet er kunnskap. Dette kan igjen bidra til bedre holdninger.

Innenfor temaet informasjonssikkerhet blir både bevissthet og holdninger brukt, mens begrepene i enkelte studier brukes om hverandre. ENISA gjorde i 2008 en undersøkelse i EU-land blant offentlige og private bedrifter, hvor de tok opp temaet awareness i sikkerhetsspørsmål. Videre snakker Straub og Welke (1998:29) om *"education/training in security awareness"*. Mathisen (2004) har gjort en undersøkelsen ift. å måle bevissthet overfor informasjonssikkerhet. Vi har derfor valgt å bruke en kombinasjon av begge begrepene.
I vår problemstilling så har vi valgt å bruke begrepet holdning, mens vi i intervjuguiden også har valgt å bruke begrepet *"awareness"*, for å få frem alle aspektene i problemstillingen.

2.4.4 Hvordan måles holdninger til informasjonssikkerhet?

Som vi tidligere har vært inne på er informasjonssikkerhet et sentralt og dagsaktuelt tema. Tradisjonelt har forskningen og arbeidet med feltet, vært rettet mot den tekniske delen I følge Nordby og Hansen (2005:5) dreier den "harde delen" seg om overvåkning/kontroll og teknologiske løsninger. I senere tid har det blitt lagt mer fokus på den myke delen, som omhandler mennesker, deres atferd, holdninger og sikkerhetskulturen i diverse organisasjoner. Ettersom vi ønsker å se på holdninger til informasjonssikkerhet, atferd og kunnskap, har vi valgt å fokusere på den "myke delen" av figur nr. 9.

Figur 9 : Komplementære prinsipper i harmonisk sikkerhetsarbeid (Nordby og Hansen, 2005:6)

I følge Mathisen (2004:5) finnes det svært få hjelpemidler for å måle holdninger og bevissthet ift. informasjonssikkerhet. Det finnes heller ikke mye informasjon om studier som er gjort innenfor dette området, verken i Norge eller andre land. I 2005 ble det gjort en undersøkelse blant 49 europeiske virksomheter, for å avdekke ulike måter å måle informasjonssikkerhet på, undersøkelsen ble utført av Bakås (2005:48). Etter at undersøkelsen var utført, konkluderte Bakås (2005) med at informasjonssikkerhet var målt i 67 % av virksomhetene. Videre konkluderte Bakås (2005) med at de viktigste vurderte effektene av måling, er økt involvering av toppledelsen og forbedrede holdninger til informasjonssikkerhet.

2.4.5 Avsluttende kommentar

Vi har i dette kapittelet belyst den teorien som vi anser som relevant for å besvare våre forskningsspørsmål. Vårt teorikapittel har blitt utviklet fortløpende i vår oppgave, dette må sees i sammenheng med at vi har en kvalitativ studie. Vi ser at begrepene defineres på mange måter, ettersom hvilket fagfelt de brukes i, men også innenfor det samme feltet. Vi ønsker å ha et spesielt fokus på holdninger til sikkerhetsaspektet ved Cloud Computing innenfor helsesektoren. Dette mener vi er relevant i forhold til vår problemstilling, bl.a. fordi det er et vesentlig element i all bruk av Cloud Computing. Dette er spesielt viktig i de sammenhengene hvor informasjonen som behandles eller lagres har sensitive elementer i seg. Vårt valg er å se på informantenes holdninger i lys av trekomponentmodellen. Dette valget begrunner vi med at holdninger ikke bare kan ses på som negativt eller positivt til noe. Mennesker påvirkes av egen kunnskap, følelser og hva man gjør, før en kan definere sine holdninger til ulike temaer. Nå vil vi i neste kapittel diskutere vår forskningsstrategi for vår studie. Her må vi foreta en del valg, fordi ulike forskningsstrategier fører til ulike måter å løse en problemstilling på.

3. Metode og forskningsstrategi

I foregående kapittel tok vi for oss teorien som er aktuell for vår oppgave, samt definerte de viktigste begrepene. I dette kapittelet ønsker vi å belyse forskningsstrategien som er mest relevant for å besvare våre forskningsspørsmål.

Valget mellom kvalitativ eller kvantitativ forskningsmetode, datainnsamling og analyse avhenger av hva man skal studere, og hva forskningsspørsmålet vårt er ute etter å få svar på (Grønmo, 2007).

Med utgangspunkt i vår problemstilling føler vi at en kvalitativ forskningsstrategi vil egne seg best, ettersom informasjonen vi er ute etter besittes av enkelte personer. Informasjonen er sensitiv, og det ville vært vanskelig å få nok respondenter til å besvare en spørreundersøkelse. Det ville også vært vanskelig for oss å trekke konklusjoner med et lavt antall respondenter. Dette bekreftes i tidligere forskning. Kotulic og Clarck (2004) måtte gi opp sitt opprinnelig prosjekt da svarresponsen var for lav til å trekke konklusjoner.

Vitenskapelige metoder er *"et sett av retningslinjer som skal sikre at vitenskapelig virksomhet er faglig forsvarlig"* (Grønmo, 2007:28). Kvale og Brinkmann (2009) sier at *"begrepet metode betyr opprinnelig veien til målet",* dette er forskningsprosjektets strategi/plan for å nå målet.

Valg av metode og hvilke data som skal innhentes og analyseres avhenger først og fremst av hva slags forhold som skal studeres og hva forskningsspørsmålet søker å besvare (Grønmo, 2007). I dette studiet utforskes bedrifters holdninger til Cloud Computing, og forskningsprosjektet er av eksplorerende art. En eksplorerende studie har som mål å søke ny forståelse eller å betrakte fenomenet man studerer i et nytt lys (Saunders, Lewis & Thornhill, 2007). Vår studie er empirisk, ettersom vi undersøker bedrifters holdninger til Cloud Computing (Grønmo, 2007).

Hva er egentlig kvalitativ metode/forskning? Mehmetoglu (2004) mener at kvalitativ metode som et begrep, ikke gjenspeiler en hel kvalitativ studie. Videre sier Mehmetoglu (2004) at ved å kalle det for metode, blir dette ofte begrenset til kun selve datainnsamlingsmetoden, men man vil jo også innbefatte analysen og skrivingen. Man bør derfor heller kalle den metodiske tilnærmingen innenfor studien for kvalitativ forskningsstrategi.

I boken til Mehmetogu (2004) beskriver han Creshwells definisjon av kvalitativ forskning som *"en forskningsprosess som er basert på klare metodologiske forskningstradisjoner som utforsker et sosialt eller humant problem. Forskeren bygger opp et kompleks, holistisk bilde, analyserer ord, gir informantens detaljert syn, og gjennomfører studien i en naturlig setting".*
Mehmetogu (2004) mener man bør velge kvalitativ forskningsstrategi fremfor kvantitativ, på grunnlag av åtte punkter:

1) Problemstillingens natur
2) Om man skal studere et tema det er forsket lite eller ingenting på fra før
3) Om forskeren er interessert i å få og presentere en detaljert oversikt over et fenomen, ikke et større bilde
4) Om man ønsker å studere individer i deres naturlige setting.
5) Om forskeren er mer bekvem eller interessert i den litterære skrivestilen
6) At forskere har tilstrekkelig tid og ressurser til datainnsamling og analyse av dataene
7) At publikummet man skriver for er vant til den kvalitative måten
8) Om man ønsker å understreke forskerens rolle som aktiv lærer, som kan formidle informantenes syn

Dersom punktene over passer godt til studiet, er det anbefalt å bruke en kvalitativ tilnærming. Dette betyr at vi ikke vil få inn store mengder data på området, men at vi snarere vil få en dyp forståelse av bedrifters holdninger til Cloud Computing. Ved bruk av et spørreskjema i kvantitativ metode vil enkelte aspekter være vanskelige å fange opp. Kvalitativ metode kan derfor gi en bredere og mer detaljrik forståelse, og egner seg bedre når vi skal studere hva som ligger i et begrep eller fenomen.

I dette kapittelet vil vi videre se på hva vi ønsker med vår studie, forskjellene på interpretivisme og positivisme, og til slutt drøfte induktiv kontra deduktiv tilnærming. Etterhvert vil vi gå inn på vårt valg av forskningsdesign, valg av setting, utvalg og informanter, i tillegg til datainnsamlingsteknikk. Videre i dette kapittelet vil vi diskutere våre analysemetoder, koding, datakvalitet, relabilitet, validitet og etikk. Vi vil avslutte dette kapittelet med en oppsummering.

3.1 Oppgavens formål

I vårt tilfelle ønsker vi å bidra med en forståelse av hvordan man kan initiere en markedsutvidelsesbasert ekspansjon av et teknologiprodukt fra privat til offentlig sektor. Dette gjør vi ved å gå inn i offentlig sektor og gjennomfører intervjuer blant potensielle fremtidige kunder for å avdekke hvorvidt de har "antakelser/kunnskap, holdninger/følelser og atferdsintensjoner" som gjør de mottakelige for det nye produktet. Dette er interessant fordi vi ønsker å finne ut noe om faktorer som må på plass hos potensielle kunder m.h.t. produktkunnskap (f.eks. hva er Cloud Computing?), følelser til produktet (f.eks. er datasikkerheten på et godt nok nivå?) og ikke minst intensjoner om å ta det i bruk.

02.05.2012 publiserte VG en artikkel om at hele journalsystemet til Vestre Viken brøt sammen (Nilssen, 2012). Journalsystemet var nede på fire sykehus, som førte til at de ansatte ikke hadde tilgang på informasjon i over seks timer. Pågående og planlagte operasjoner måtte da stoppe eller utsettes. En overlege sier dette om den manglende tilgang til pasientjournalene: *"Det betyr at vi ikke hadde noen opplysninger om menneskene som er på sykehuset eller som kom til oss. Det er snakk om kritiske opplysninger som for eksempel om noen har en alvorlig allergi"*. Videre sier han "*Vi har måtte improvisere før og har gode nødrutiner på å skrive dokumentasjon. Men det hjelper ikke når vi ikke har tilgang på journalene. Det virker som at det blir mer og mer ustabilt" (Nilssen, 2012)*. Ifølge tillitsvalgt for overlegene på Vestre Viken, Tom Henri Hansen, snakkes det stadig om at IKT er viktig i helsevesenet, men at man da må få disponere stabile systemer. Sykehusene må ha back-up løsninger fordi det i en gitt situasjon kan være helt avgjørende for liv og helse, at man får de opplysningene man trenger (Nilssen, 2012). Da denne artikkelen ble skrevet var driftssikkerheten i disse systemene meget høye, med et snitt på 99,98 % de siste seks månedene. Dette eksempelet fra Vestre Viken viser oss hvor viktig det er med sikkerhet og stabile tjenester.

Vi har valgt å følge det som kvalitative metodeforskere har beskrevet som tre hovedformål for forskningen: *"å utforske, å forklare eller å beskrive fenomenet"*, og *synonymer for dette kan være "å forstå, å utvikle eller å oppdage fenomenet"* (Marshall & Rossmann, 1993). Vårt mål er *"å beskrive"* og *"å sammenligne"* helsesektorens holdninger til Cloud Computing med et spesielt fokus på holdninger til

sikkerheten i forbindelse med dette teknologkonseptet. Ut i fra dette vil CSC få et bedre innsyn i hva som skal til for å lykkes med en eventuell offentlig ekspansjon.

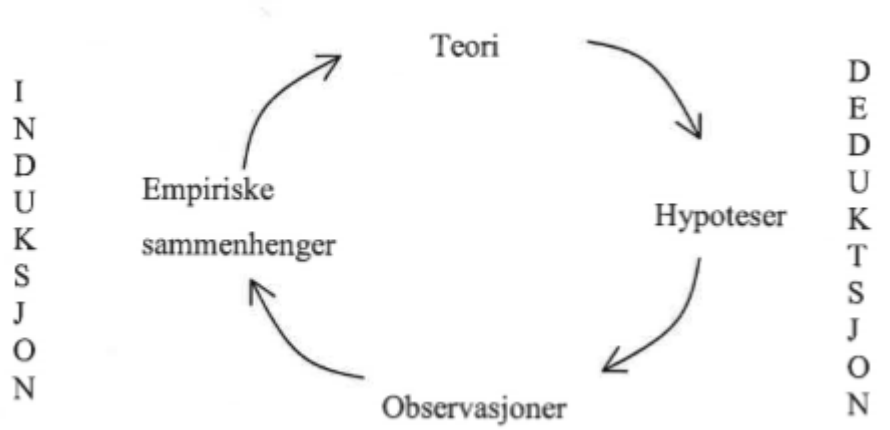
3.2 Interpretivisme eller positivisme

Kvalitativ forskning går under rammen av interpretivisme, mens kvantitativ forskning blir sterkt påvirket av positivisme. Interpretivisme er teoribyggende, altså utvikling av teori mens positivisme er teoritestende. Kvantitativ forskning begynner med hypoteser, mens kvalitativ forskning ender opp med hypoteser (Mehmetoglu, 2004). Gephart (1999:2) forklarer hovedfokuset til positivisme og interpretivisme slik: positivisme er ”*search for contextual and organizational variables which cause organizational actions*” , mens interpretivisme er ”*search for patterns of meaning*”.

Målet med denne oppgaven er å finne ut hva slags holdning sykehusene har til Cloud Computing. Det vi da er ute etter er å fortolke og forstå det informantene våre forteller oss. Klein og Myers (1999:67) påstår at interpretivistisk forskning kan bidra til å forstå menneskers tanker og handlinger i sosiale og organiserte settinger. Ettersom vår masteravhandling faller inn under det fortolkende paradigmet, mener vi at dette er relevant for oss. Videre forklarer positivistisk forskning at mennesker har disposisjoner som er forårsaket av atferd, mens fortolkende forskere antar at mennesker har disposisjoner som kan, men altså ikke må realiseres i form av atferd.

3.3 Induktivt eller deduktivt

Ettersom vi har definert vår forskning som interpretivistisk, ønsker vi nå å forklare forskningen i henhold til en induktiv og deduktiv tilnærming. Vanligvis karakteriseres kvalitativ forskning som induktiv, mens deduktiv karakteriseres som en kvantitativ tilnærming. Ifølge Ringdal (2007) tar induktiv forskning utgangspunktet i empirien for å utvikle ny teori, mens deduktiv forskning er ifølge Mehmetoglu (2004:102): *" I utgangspunktet en kvantitativ analyseprosess som begynner med en allerede utviklet teori."*



Figur 10 : "Vitenskapssirkelen" av Wallace, 1971

Vår masteravhandling tar både i bruk den deduktive og induktive. Vi benytter oss av den deduktive tilnærmingen når det kommer til holdningsteori. Dette kommer frem i kapittel to og ved modellene som er anerkjent innenfor denne forskningstradisjonen. De ulike modellene som har skapt holdningsteori er testet gjennom ulike hypoteser, vi ser derfor på den deduktive siden av vitenskapssirkelen til Wallace fra 1971 (i Ringdal, 2007:41). Vi kan derfor ikke påstå at forskningen vår er uten utgangspunkt i allerede eksisterende teori.

Vi har også valgt å benytte tidligere forskning som er gjort innenfor sikkerhetsrelatert IS-forskning og sett på spørsmål som er blitt stilt i kvalitative undersøkelser, men også hvordan informasjonssikkerhet er blitt målt i kvantitative undersøkelser.
Dette har bidratt til å støtte vårt valg av egne data. I vårt tilfelle er det ikke bare snakk om å forstå, men om å undersøke og sammenlikne holdninger som mennesker har i forhold til nye produkter og tjenester. Videre er det heller ikke blitt utarbeidet hypoteser for å støtte vår studie. Noe som fører til at vår empiriske forskning er induktiv, ettersom vi har som mål å gi innsikt i sammenligningen av de ulike casene vi foretar oss. Det kan med dette være mulig å utforme hypoteser med bakgrunn i våre funn.

3.4 Forskningsdesign

I de foregående delkapitlene har vi tatt for oss bakgrunnen for valg av forsknings-strategi og hva vi nå ønsker å ta for oss angående valg av forskningsdesign.

Forskningsdesign blir definert av Ringdal (2007:22) *"som en grov skisse for gjennomføring av konkret undersøkelse"*. Innen kvalitativ forskning finnes det flere typer forskningsdesign som er knyttet opp mot kvalitative strategier, mens det også er noen som tradisjonelt sett er knyttet opp mot kvantitativ forskningsstrategier. Dersom man velger en kvalitativ forskningsstrategi åpner man også opp for valg mellom ulike design avhengig av hva man ønsker å undersøke. Valg av design vil vi fremstille som et valg gjort på grunnlag av den overordnede strategien for å gjennomføre en studie. I følge Myers (2008) finnes det fire ulike design innenfor rammene av en kvalitativ forskningsstrategi. Disse er som følgende:

Design	Egenskaper
Aksjonsforskning	Problemløsning Kunnskapsutvikling Organisasjonsutvikling Opplæring Ikke mye brukt innenfor informasjonssystemer, men økende interesse det siste 10-året.
Casestudier	Det mest brukte designet innenfor informasjonssystemer. Studerer aktuelle fenomen i det virkelige liv spesielt når det ikke er et klart skille mellom fenomen og kontekst. Avdekke forskjeller, likheter.
Etnografiske studier	Forskeren bruker mye tid ute i feltet. Plasserer fenomenet som studeres i dets sosiale og kulturelle kontekst. Det er gjort mye interessant arbeid i forhold til evaluering og design av informasjonssystemer med utgangspunktet i samarbeid mellom etnologer og designere.
Grounded Theory	Utvikle teori-Induktiv tilnærming. Er økende innenfor IS-forskning fordi den er nyttig i forhold til å utvikle kontekstbasert, prosessorienterte beskrivelser og forklaringer av fenomenet som skal studeres.

Tabell 4 : "Myers oversikt over hoved design innenfor kvalitativ forskning

Videre vil vi ta for oss vårt valg av design og de valg som naturlig følger av det. Dette vil da være i form av analyse, informanter og intervjuform.

3.4.1 Vårt valg av design

Vi har tidligere i kapittelet gitt en beskrivelse på hoveddesign innenfor kvalitativ forskning, og vi vil nå begrunne hvorfor vi mener at case design er riktig for vår studie. Når man skal bestemme seg for hvilke type design man ønsker å bruke, bør man se på hva som er hensikten med studien. Hvis studien vil ha svar på ”hvordan og hvorfor” kan et casestudie være riktig design. Valg av design blir basert på formuleringen av forskningsspørsmålet, som igjen påvirker valg av setting, analysemetode og utvalg.

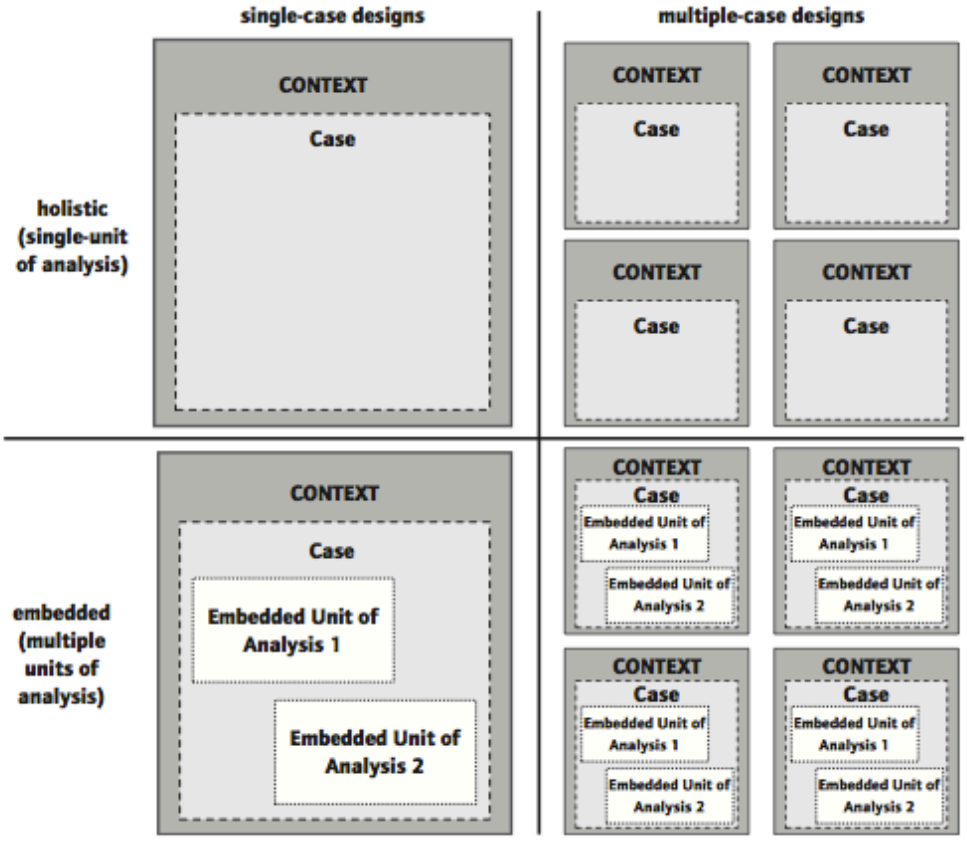
Et case defineres og avgrenses av forskeren, og kan være personer, grupper, begivenheter etc., det er opp til forskeren å definere og avgrense det. Ifølge Yin (2003:3) kan et case være eksplorerende (utforskende), deskriptivt (beskrivende) eller forklarende. Videre beskriver Yin (2003) tre vilkår som er essensielle når det kommer til valg av forskningsdesign:

1) Hvilket forskningsspørsmål man stiller.
2) I hvilken grad forsker har kontroll over den faktiske atferden/situasjonen.
3) I hvilken grad man fokuserer på samtiden/nåtiden eller historiske hendelser.

Vi har definert våre forskningsspørsmål som et ”hvilke/hva” spørsmål. Dette betyr at vi bør holde oss til en kvalitativ casestudie. Vi har ikke kontroll over hendelser som vil forekomme og vår studie vil fokusere på tilfeldige hendelser. Når man ser dette i sammenheng med punkt 2 og 3 er casestudie å anbefale. I følge Yin (2003:8) er det at man kan forholde seg til mange ulike typer ”datamateriale” en styrke når det kommer til casestudie. Ulike typer ”datamateriale” kan blant annet være intervju, dokumenter, arkivdata og egen kunnskap (Yin, 2003:8).

Ifølge Klein og Myers (1999:68) er casedesign innenfor IS-forskning blitt godtatt som en gyldig forskningsstrategi, på grunn av at det har blitt utviklet metodologiske prinsipper innenfor denne typen strategi. Videre mener Myers (2008) at casestudier egner seg bra til IS-forskning. Dette er begrunnet i at denne retningen er basert på studier innenfor informasjonssystemer i organisasjoner. Vi har derfor valgt case som

forskningsdesign på bakgrunn av punktene over. Dette fører oss til nye valg ettersom man kan dele casedesign inn i fire ulike typer.



Figur 11 : Yins fire casedesign

Yin (2003:40) presenterer disse fire typene av casedesign;

- Single case holistisk
- Single case embedded
- Multiple case holistisk
- Multiple case embedded

Matrisen til Yin (2003) illustrerer først at alle typer design som vil inkludere ønsket rundt det å studere kontekstuelle forhold i relasjon til casen. Den stiplede linjen i matrisen viser at avgrensningen mellom case og kontekst mest sannsynlig ikke er veldig sterk. Grunnen til dette er fordi et casestudium må både dekke fenomenet som er av interesse og konteksten som dette fenomenet befinner seg i (Yin, 2003).

I en singlecase har man kun et case og går i dybden på dette. I multiple case velger man flere singlecase i en forskning. I en holistisk case er det en enhet som blir analysert, og man ser på helheten ved dette caset. Dette gjør man hvis det ikke er noen naturlige undergrupper. I et single case holistisk ser man f.eks. kun på et sykehus, mens man i en multiple case holistisk ser på flere sykehus og sammenligner observasjonene mellom disse. Ved en embedded case ser man på undergruppene innenfor caset. Dette casedesignet gir en større mulighet til å fange opp endringer i miljøet og omgivelsene i forhold til problemstillingen. Men dette kan igjen virke inn negativt hvis man kun ser på underenhetene og glemmer helheten. Det er å foretrekke holistisk når det ikke er noen undergrupper og når teorien i bunn er holistisk (Yin, 2009). I et single case embedded ser man på sykehusledelsens holdninger, mens i en multiple case embedded ser man på de ulike sykehusene og ulike lederes holdninger.
En bør velge singlecase hvis det:
1) Representerer et kritisk case i testing av en velformulert teori, her vil man bruke caset for å bekrefte eller utvide teorien.
2) Caset representerer et ekstremt eller unikt tilfelle.
3) Caset er representativt eller typisk, og ser på hverdagslige hendelser.
4) Caset er revelatory, en får altså tilgang til et fenomen som en ikke har hatt mulighet til å studere tidligere.
5) Caset er longitudinell, her ser man på om forholdet endrer seg over tid.
Disse fem punktene fremstår som hovedårsakene til å velge singelcase.

Flere forskere diskuterer fordeler og ulemper når det kommer til bruk av single case og multiple case. Yin (2003) mener at multiple case design er det beste fordi det er mer robust og det er lettere å rettferdiggjøre konklusjonene. Ved multiple case design kan man også finne bevis som er mer anvendbart og generaliserende. Eisenhardt (1989:547) mener man bør ha mellom 4 til 10 case for å kunne skape nye testbare hypoteser, og for å kunne generalisere resultatene. Dyer og Wilkins (1991:613) er uenig i dette og mener at dybdeforståelsen vil forsvinne ved så mange case, samt at man da beveger seg mot en mer kvantitativ forskning.

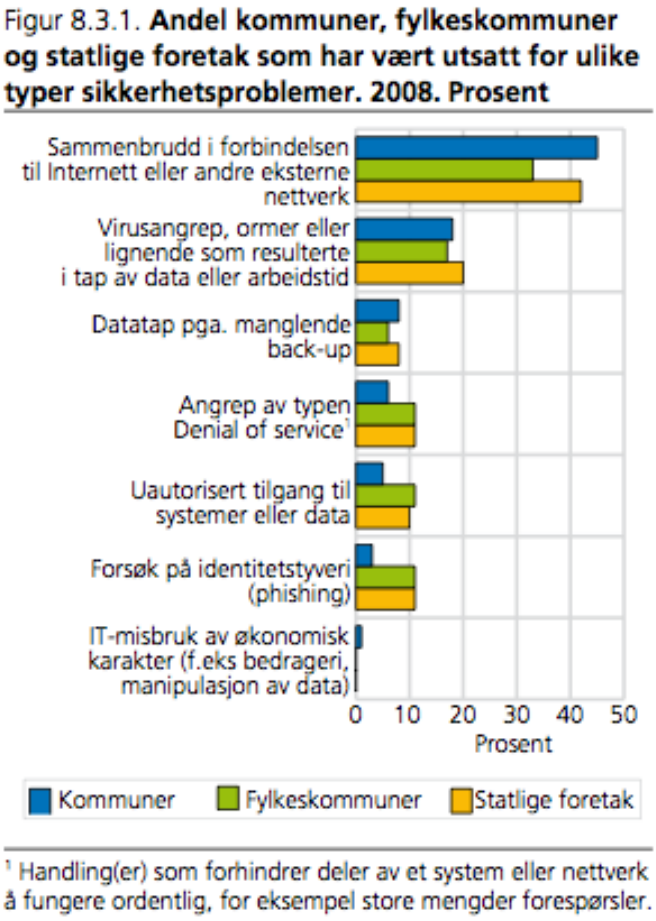
Vi finner det hensiktsmessig å velge multiple casestudie, ettersom dette gir større grunnlag for å forklare teorien på tvers av kontekstene. På denne måten vil vår studie belyse og skape teoretiske konstruksjoner, samtidig som det vil gi overbevisende og

helhetlige resultater. Casene har respondenter fra ulike nivåer i ulike deler av helsesektoren. Vår case er et multiple case holistisk. Dette begrunnes med at vi har gjennomført intervjuer med ansatte på ulike nivåer ved flere sykehus, samt ved helsedirektoratet. For oss er det vesentlig å kunne sammenligne de ansattes holdninger for å besvare vår problemstilling.

3.4.2 Valg av setting

Nå som vi har valgt forskningsstrategi til vår studie, må vi nå velge setting. For vår del vil settingen være ledelsen i helsesektoren. Grunnen til at vi har valgt dette er med tanke på CSC sitt ønske om å ekspandere inn i sykehussegmentet med sin Cloud Computing løsning. Innenfor helsesektoren er informasjonssikkerhet ekstremt viktig.

Lov om behandling av personalopplysninger §13 dreier seg om informasjonssikkerhet og sier: ”*Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.*
For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlings-ansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda.
En behandlingsansvarlig som lar andre få tilgang til personopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd.” (Personopplysningsloven, 2000).
Sikkerhetsaspektet er viktig, og Statistisk sentralbyrå har foretatt ulike undesøkelser som ser på sikkerhet og informasjons- og kommunikasjonsteknologi (IKT) i kommunale, fylkeskommunale og hos statlige foretak.



Figur 12 : Oversikt over sikkerhetsproblemer hos foretak i kommunene, fylkeskommunene og staten.

Ifølge figuren over har Engdal et al. (2009) kommet frem til at *"Virusangrep, ormer eller lignende som resulterte i tap av data eller arbeidstid"* har oppstått blant 18, 17 og 20 prosent av henholdsvis kommuner, fylkeskommuner og statlige foretak i 2008. Vi ser at det også har vært sikkerhetsproblemer innenfor *"Uautorisert tilgang til systemer eller data"*. Ved den økende bruken av informasjons- og kommunikasjons-teknologi har dette medført flere utfordringer når det kommer til sikkerheten rundt bruken av IKT-system, nettverk og systemer tilknyttet dette. En uheldig konsekvens for utbredelsen av internett er at informasjon kan bli endret, gå tapt eller bli stjålet (Engedal et al., 2009).

I Norge er alle de offentlige sykehus delt inn i fire regionale helseforetak: Helse Sør-Øst RHF, Helse Vest RHF, Helse Midt-Norge RHF og Helse Nord RHF (Helse- og omsorgsdepartementet, 2011). For å kunne øke IKT- sikkerheten i disse fire regionale helseforetakene, er det nødvendig å bevisstgjøre trusler og sårbarhet, og påvirkning av holdninger når det kommer til bruk av IKT. Den manglende sikkerheten er en viktig barriere når det kommer til utvikling av et elektronisk tjenestetilbud, og ansvaret for å skjerme sikkerheten ligger både hos forbruker og produsent (Engedal et al., 2009).

3.4.3 Utvalg og nøkkelinformanter

Nøkkelinformanter har ifølge Campell (1955) to klare karakteristika. Den første er at de skal inneha roller som vil gjøre dem kunnskapsrike når det kommer til området som skal bli undersøkt. Den andre er at de skal være villige og ha mulighet til å kommunisere med forskeren. Det har vært gjort flere studier der det har blitt vist at enkeltinformanter ikke kan representere store organisasjoner (Seidler, 1974). Dette blir støttet av Phillips (1980, 1981) der han illustrerer at ved noen tilfeller vil enkeltinformanter være utilstrekkelig, spesielt når komplekse sosiale vurderinger skal gjennomføres. Ketokivi og Schroeder (2004) viser til at singelinformanter kan bli påvirket av stillingen de har i bedriften når de skal svare på undersøkelser. Dette vil kunne påvirke empirien og de fraråder bruken av singelinformanter.

I en studie utført av John og Reve (1982), ser de nærmere på nøkkelinformanter i et dyadisk forhold. De finner støtte for at dersom forskeren foretar en omhyggelig utvelgelse av nøkkelinformanter, vil en få reliable og valide data.
Et viktig element når det kommer til den overnevnte teorien om nøkkelinformanter, er at studiene som har blitt gjennomført baserer seg på kvantitative studier og målinger. Man får dermed et annet bilde og andre måter å måle validitet og reliabilitet enn i vårt kvalitative studium. I vår studie skal vi utvikle og generalisere til teori, ikke til empiri. Likevel mener vi at teorien som fremlegges også vil være gjeldende for vår studie, men at vi da har med de teoretiske prinsippene i teorien enn de konkrete validitets-målingene som vi finner i disse artiklene.

Vi er avhengige av å treffe de riktige personene i forhold til vårt forskningstema, og vi legger derfor vekt på Campell (1955) sine to krav. Vi mener det er viktig at vi prøver å oppnå en interaksjon med våre nøkkelinformanter, og at det blir lagt til rette for at de føler at de er med på et samarbeid, kontra en deltagelse. Dette vil nok være sentralt for oss, slik at vi får fram gode data og får tillit fra informantene. I tillegg til at vi legger vekt på Campell (1955) sine krav, så støtter vi oss også på utsagnet til Thagaard (1988:51): *"I kvalitative studier benyttes strategiske utvalg, det vil si at informantene velges ut på en måte som er hensiktsmessig i forhold til problem-stillingen"*. Vi velger også å støtte oss til hennes andre utsagn når det kommer til

antall informanter: ”*når studier av flere enheter ikke synes å gi ytterligere forståelse av fenomenene som studeres, kan utvalget betraktes om tilstrekkelig stort”*.

Valg av nøkkelinformanter har vi i stor grad tatt utgangspunkt i tips fra vår kontaktperson i CSC og veileder angående hvem vi bør kontakte. Vi endte opp med syv nøkkelinformanter. Fra Vestre Viken HF har vi intervjuet to personer. Den første av disse er Henriette Henriksen, som er informasjonssikkerhetsansvarlig og personvernombud innenfor Teknologi og eHelse. Videre har vi Robert Nystuen som er avdelingssjef innenfor teknologi og eHelse. På Akershus universitetssykehus har vi intervjuet to personer. Her snakket vi med Kjell Borthne som er direktør i divisjonen for diagnostikk og teknologi og vår andre informant, Sverre Knutsen, som er IKT-leder. I Helse Sør-Øst RHF intervjuet vi Ketil Are lund, som er leder for teknologiutvikling. I Helsedirektoratet fikk vi intervjuet to senior rådgivere i eHelse og IT-divisjonen, Helge T. Blindheim og Truls E. Losnegaard.

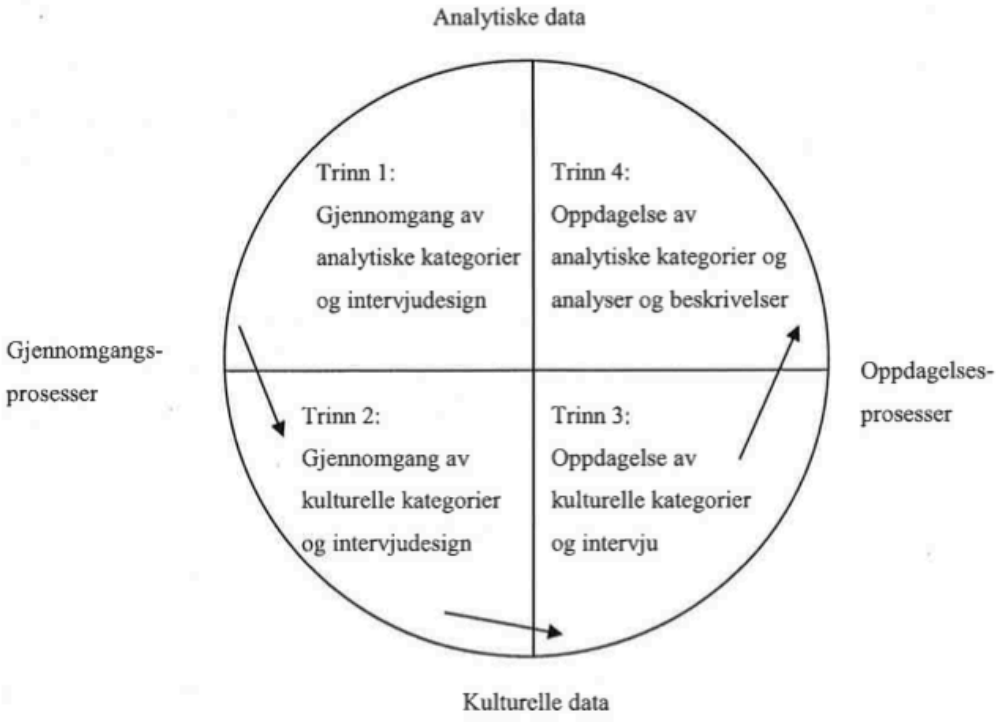
3.5 Datainnsamling

I forbindelse med vår datainnsamling tar vi utgangspunkt i intervju. Vi har som tidligere nevnt bestemt oss for å intervjue fem ansatte innenfor de regionale helseforetakene og to ansatte i helsedirektoratet. Vi satte oss en grense på 80 km, med hensyn til tidsbruk per intervju. Etter å ha gått igjennom ulike studier rundt Cloud Computing og informasjonssikkerhet, kan vi si at det er vanskelig å få svar på informasjonssikkerheten innenfor Cloud Computing. I forhold til at dette er et relativt nytt felt og det ikke har vært mye diskusjoner rundt dette i den offentlige sektoren. Vi utviklet en intervjuguide (Vedlegg 1) i forhold til vår teori og empiri. Hensikten med dette var å samle data som var relevant for å belyse våre forskningsspørsmål.

Forberedelsene til intervjuene ble gjort ut i fra McCracken (1988) sin bok *The Long Interview.* Lange intervjuer krever spesielle forberedelser og struktur, og er designet for å gi forskeren et effektivt og produktivt instrument for undersøkelsen/forskningen (McCracken, 1988). Den teoretiske tilnærmingen til datainnsamlingen gir oss en solid plattform, og bidra til at vi får frem et tett samarbeid med våre respondenter og får gode data. Vi har oversatt ni viktige forhold i McCracken (1998) som det er viktig å ta hensyn til og ha en forståelse for, før en starter med intervjuet:

1) Samfunnsvitenskapens forskningsmiljø; det er viktig at kvalitativ forskning står på egne ben og systematiserer sin viten slik at det vil bli lettere å gjenta prosessene.
2) Objektet i samfunnsvitenskapen; krever alminnelig samarbeid.
3) Hva er kvalitativ/kvantitativ forskning og deres forskjeller:
    a) Hvordan de behandler analytiske kategorier.
    b) Datarapporteringsmulighetene til respondenten.
    c) Seleksjon av respondenter.
    d) De er ikke substitutter, de utfyller hverandre.
4) Forskeren som instrument, samt forstå rollen denne har.
5) Invaderende/ikke-invaderende balanse; viktig å ha en god intervjuguide eller gode stikkord å bruke underveis.
6) Skape distanse; både respondent og forsker må gis mulighet å se ting på en ny måte.
7) Spørreskjemaet, som innehar flere funksjoner:
    a) Alle blir spurt om (omtrent) det samme.
    b) Skape distanse.
    c) Skaper kanaler for retninger og rekkevidden av samtalen.
8) Forholdet mellom forsker og respondent; som er kompleks på bakgrunn av flere forhold:
    a) Inntrykk av forsker påvirker respondenten – viktig med en balanse mellom formell og uformell.
    b) Inntrykket forskeren har av respondenten – her må en huske at etikk er viktig.
9) Multiple fremgangsmåter; intervjuet bør ikke sees isolert, bruk det gjerne sammen med andre (og kvantitative metoder).

Videre viser McCracken (1988:29) hvordan intervjuet kan deles opp i fire steg.



Figur 13: McCrackens prosesser for det lange intervjuet (McCracken, 1988)

Steg 1: Gjennomgang av analytiske kategorier og intervjudesign.

Forskeren må her foreta en litteraturgjennomgang. Dette for å kunne vite hva som er forsket på tidligere og hva andre forskere har funnet ut om temaet man forsker på. I dette steget kan en dra fordeler av tidligere forskning, det gir en oversikt over hva intervjuet bør bestå av. Dette kan kalles grunnmuren i intervjuprosessen (McCracken, 1988:31). Dette hjelper oss som forskere med å finne gode begreper som antagelsene bygges på, og bidrar som sagt til å utarbeide en god intervjuguide. For oss har det vært en fordel å kunne se på tidligere forskning rundt holdningsteori. Dette har resultert i at vi har valgt å se på begrepene kognisjon, affekt og atferd som utgangspunkt for vår analyse. Vi har sett på andre studier ved forberedelsene til intervjuguiden, og spørsmål som har blitt stilt i andre undersøkelser, og tilpasset disse til vår setting med hjelp fra CSC og veileder.

Steg 2: Gjennomgang av kulturelle kategorier og intervjudesign.

Her benytter forskeren seg selv som et instrument i sin undersøkelse, og spør seg selv hva man vet om fenomenet. Det er ifølge McCracken (1988:33) tre motiver ved dette trinnet:

1) Forberede seg til konstruksjon av intervjuguide.
2) Forberede seg til søket som vil skje under dataanalysen.
3) Opparbeide evnen til å etablere distanse til sine egne antagelser slik at en unngår forutinntatthet.

Steg 3: Oppdagelse av kulturelle kategorier og intervjuer.

I denne fasen beveger en seg fra gjennomgangsprosessen over til oppdagelses-prosessen. Her handler det nå om å formalisere og ferdigstille spørreskjemaet, samt gjennomføre intervjuene. Det er to viktige punkter en skal ha fokus på ved dette tidspunktet i prosessen:
1) La informantene få fortelle sin historie med egne ord.
2) Hvordan en foretar utvelgelse av informanter.

Det første punktet ivaretar vi ved å formulere spørsmålene så generelle og lite ledende som mulig. Det andre punktet er godt beskrevet i kapittelet over. Ifølge McCracken er det anbefalt å starte et intervju med biografiske spørsmål for å "varme opp" informanten. I vårt tilfelle var ikke dette interessant. Vi brukte denne oppvarmings-perioden som en mulighet til å presentere oss selv og informere rundt vår problemstilling.
Videre i utarbeidelsen av intervjuguiden måtte vi ta et valg når det kom til hvordan vi skulle føre samtalene med informantene. Skulle vi sette opp strukturerte spørsmål eller legge det opp til en samtale uten noen retningslinjer? Valget falt på et strukturert intervju hvor spørsmålene er nedskrevet og rekkefølgen er gitt på forhånd. Thagaard (1998:80) sier at:*"Fordelen med en strukturert tilnærming er at svarene er sammenlignbare, fordi intervjuene gir informasjon om de samme temaene, men fra forskjellige personer".*

Vi utarbeidet vår intervjuguide etter det Mehmetoglu (2004:69) omtaler som et semistrukturert intervju og som bidrar til at en *"kan avvike fra den planlagte intervjuplanen og diskutere temaer som faller utenfor de opprinnelige temaer eller spørsmål, men som likevel vil være nyttig i forhold til problemstillingen".* Dette resulterer i at vi får en plan og mal for hvordan vi skal føre intervjuene. Dette gir oss muligheten til å være relativt åpne, men også muligheten til å gå dypere inn i

tematikken hvis dette skulle være nødvendig. Vi har også muligheten til å stille spørsmål i intervjuene som vi i utgangspunktet ikke hadde med, for å få dypere svar.

McCracken (1988) beskriver også andre måter rundt planlegging av samtaler med informantene. Eksempler på dette er å bruke en ”grand-tour” der forskeren stiller spørsmål som ikke innehar en spesiell retning, eller stille planlagte spørsmål. Det er også viktig å legge inn såkalte ”floating prompts”. Dette er skjulte instrukser som ikke respondenten reagerer på. F.eks. å heve øyebrynet, eller ha spørsmålstegn ved diverse ord i svaret. Andre ”prompts” man kan legge til er såkalte ”planned prompts”, noe som vil være mer direkte oppfølgingsspørsmål slik at respondenten må svare mer utdypende.

Vi har som tidligere nevnt, forholdt oss til at vi har et semistrukturert intervju. Vi har planlagt ulike kategorier hvor vi har ulike spørsmål, og er åpne for uforutsette temaer/kommentarer som våre informanter kan komme med. Vår intervjuguide er utformet med bakgrunn i McCracken (1988) og inneholder følgende deler: en introduksjon som presenterer vår tematikk, innledende spørsmål angående rolle i bedriften og tidligere erfaring, forskningsspørsmål som skal besvare problem-stillingen, samt en avslutting hvor respondenten snakker litt løst rundt temaet hvis det er noe han føler vi har utelatt.

Steg 4: Oppdagelse av analytiske kategorier, analysene og skriving.

Ifølge McCracken (1988:41) er dette steget det mest krevende og minst studerte området i forskningsprosessen. Med dette mener McCracken (1988) at en ikke kan planlegge alt på forhånd. Ulike problemer krever ulike løsninger og problemer må ofte løses når det dukker opp. Det er viktig å ikke avslutte analysen for tidlig. Forskeren skal gjennomføre arbeidet til en har kommet i mål, ettersom man skal benytte de funnene en har fra tidligere i prosessen og identifisere viktige temaer. En skal konkludere på bakgrunn av alle intervju som en har foretatt. McCracken (1988:41) påpeker noen konkrete hjelpemidler:

1) Ta opp intervjuene på tape

   For oss var dette et naturlig valg, ettersom vi ikke ville klare å få med oss alt informanten ville fortelle oss i intervjuet.

2) Transkriber intervjuene ordrett

Ifølge McCracken bør denne jobben settes bort til andre slik at man unngår at man blir for familiær med dataene. Vi velger å transkribere selv på bakgrunn av at vi vil bli godt kjent med våre data og at kostnaden ved at andre transkriberer for oss vil bli for stor. Selv om dette motstrider McCracken sine anbefalinger, føler vi at vi har hatt god nytte av å transkribere selv.

3) Foreta analysen gjennom fem trinn

Hensikten ved å foreta analysen er å bestemme de ulike kategoriene, sammenhengene og antagelsene som påvirker våre informanters generelle syn på verden, og spesielt det undersøkte temaet. Analysen gjennomføres i fem trinn:

a) Se på de enkle uttalelsene uten å lete etter sammenhenger.

b) Utvikle disse uttalelsene ved hjelp av deres egen betydning, så i forhold til det man finner i transkriberingen.

c) Se etter sammenhenger knyttet til litteratur og kultur.

d) Sammenligne alle observasjoner samlet.

e) Sette sammen mønstrene og stiene inn i den endelige analysen.

4) Bruk databaserte hjelpemidler i analysen. Dette er det siste punktet og skal hjelpe oss til å lette arbeidet.

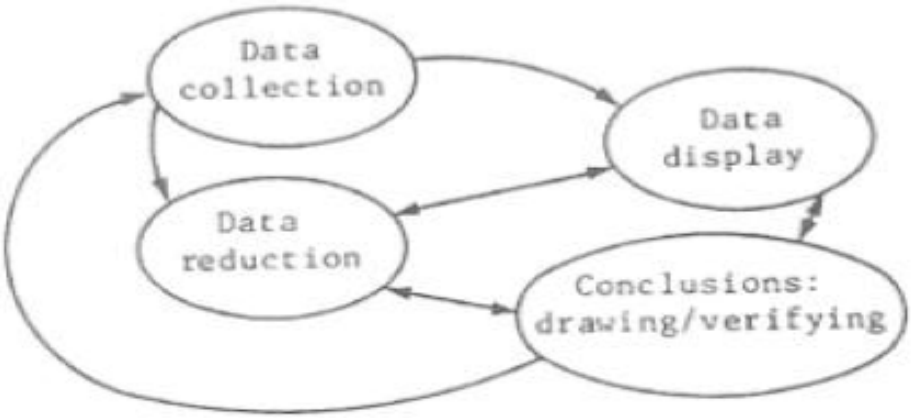
Innenfor kvalitativ forskning har det kommet flere programmer som kan benyttes. Vårt valg har falt på programmet WeftQDA som vi tidligere har brukt i metodekurs ved Høgskolen i Buskerud og Vestfold.

Å ta utgangspunkt i McCrackens sirkel for intervju har vært viktig for å utvikle intervjuguide og ved utførelsen av de ulike intervjuene. Videre vil vi ta for oss dataanalysen.

3.5.1 Dataanalyse

En analyse innenfor kvalitativ metode er annerledes enn i en kvantitativ metode. I kvalitativ forskning forholder en seg til tekst og ikke tall, slik det er i en kvantitativ studie. McCrackens fjerde steg tar for seg analysefasen. I vår studie forholder vi oss til mennesker og hva de forteller oss. Klein og Myers (1999:74) har gitt en god definisjon på dette: *"The researchers needs to see people as the producers and not just products of history and the description of the historical context should reflect this in the write-up of the research study"*.

Thagaard (1998:107) beskriver tre måter å foreta en kvalitativ analyse på, men det finnes også mange andre måter: analyser av beretninger og historier, personsentrerte analyser og temasentrerte analyser. Mehmetoglu (2004:98) diskuterer rundt analysen av kvalitative data og beskriver hvordan en kan analysere i empiribasert teori, i etnografi og i casestudie.



Figur 14: Komponentene i dataanalysen: Den interaktive modellen
(Miles og Huberman, 1994:12)

Figuren til Miles og Huberman (1994) fremstiller tre varianter av analyseaktiviteter, samt selve datainnsamlingen i en interakterende syklisk modell. Her kan en som forsker bevege seg mellom disse ”nodene” etter som en har behov og fremdrift i forskningen. Videre viser Miles og Huberman (1994) at selve undersøkelsen kan endres underveis ut i fra de funn som dukker opp.

For å ikke gjøre analysearbeidet for komplisert, har vi valgt å følge McCrackens tankegang. Vi har sett etter sammenhenger i litteratur og kultur, og ser på Thagaards temasentrerte analyse hvor vi grep fatt i hennes tanker omkring sammenligninger. Det blir påpekt av Thagaard (1998:163) at det er viktig at en klarer å skifte fokus under analysen, ha fokus på den enkelte analyseenhet og et skifte til fokus for å kunne finne mønster i materialet.

Etter at vi har gjennomført intervjurundene sitter vi igjen med store mengder data på lydfiler som må transkriberes og analyseres. Nedenfor viser vi en tabell over de intervjuene som vi har foretatt. Denne tabellen viser bedriften de jobber for, informant, stillingsnivå, tidspunkt for intervju og lengde på intervju.

Bedrift	**Informant**	**Stillingsnivå**	**Tidspunkt**	**Lengde**
Vestre Viken HF	Henriette Henriksen	Informasjonssikkerhetsansvarlig/ Personvernombud- Teknologi og eHelse	18.februar 2014	41 minutter
Akershus universitetssykehus HF	Kjell Borthne	Direktør, divisjon for diagnostikk og teknologi	21.februar 2014	32 minutter
Akershus universitetssykehus HF	Sverre Knutsen	IKT-leder	21.februar 2014	27 minutter
Helse Sør-Øst RHF	Ketil Are Lund	Leder, teknologiutvikling	6.mars 2014	42 minutter
Helsedirektoratet	Helge T.Blindheim Truls E.Losnegaard	Senior rådgiver i eHelse og IT-divisjonen Senior rådgiver i eHelse og IT-divisjonen. (Juridisk bakgrunn)	10.mars 2014	1 time og 30 minutter
Vestre Viken HF	Robert Nystuen	Avdelingssjef – Teknologi og eHelse	20.mars 2014	37 minutter

Tabell 5: Oversikt over våre informanter

Et passende antall respondenter må sees opp mot bredden av det vi undersøker og at respondentene gir oss tilstrekkelig informasjon. En datainnsamling bør foregå til metningspunktet er nådd, det vil si hvor det ikke lengre avdekkes noe ny informasjon (Ryen, 2002). Vi er klar over at syv respondenter kan være noe begrenset for å kunne oppnå et fullstendig metningspunkt. Inntrykket vi likevel fikk av respondentenes svar var at de delte et likt syn på tematikken og begrunnet svarene sine med relativt like påstander.

Vi har kategorisert dataene våre etter holdning som det overordnede begrepet, som igjen ble delt inn i kognisjon, affekt og atferd. Vi har videre tatt for oss kategoriene i forhold til informasjonssikkerhet. Noen eksempler på dette er behandling av pasient-

opplysninger, og andre sikkerhetsmessige utfordringer omkring Cloud Computing. Disse har vi sett på i forhold til de tre holdningsdimensjonene.

Ifølge Langdridge (2004) er transkriberingen av datamaterialet den første delen av analyseprosessen, dette bidrar til at vi som forskere blir bedre kjent med den innsamlede empirien. Videre viser King og Horrocks (2010) at vi som forskere selv må vurdere hvor mye en skal transkribere, basert på hvor mye tid som er tilgjengelig. Ettersom vi er uerfarne som forskere har vi valgt å transkribere alt.

3.5.2 Koding

Når det kommer til fasen etter datainnsamling er det mange forskere som føler at de sliter med å se "skogen for bare trær" (Miles og Huberman, 1994). Ettersom det ikke er tall vi skal analysere, men ord så kan dette framstå som massivt og komplekst. Vår prosess starter med å benytte dataprogrammet WeftQDA. Vi foretar våre analyser ut i fra den transkriberte teksten. Videre vil vi bruke analysen for å avdekke funn og svare på vårt forskningsspørsmål.

Datamengden er ustrukturert og stor, det er derfor et behov for å redusere kompleksiteten ved forenkling og strukturering. Ifølge Miles og Huberman (1994) er koding analysering. Koding kan anses som noter eller merkelapper som samler informasjonen innenfor et studium. En anvender kodene for å organisere og samler informasjonen som hører sammen. En starter gjerne med å se etter likheter og ulikheter før man så lager generelle kategorier, og etterhvert danner flere underkategorier (Miles og Huberman, 1994). Som nevnt i kapittelet over har vi brukt holdningsbegrepet og inndelingen av dette i kognisjon, affekt og atferd. Vi har videre delt opp i ulike underkoder:

- Forståelse
- Generell holdning
- Gevinster/risikomomenter
- Utfordringer i offentlig sektor
- Sikkerhetsmessige utfordringer
- Sikkerhet i nåværende systemer vs. sikkerhet i Cloud Computing

- Beliggenhet/lovverk
- Kollegaer
- Kostnadseffektivisering
- Brukervennlighet
- Brukerstøtte
- Effektivisering
- Videre planer

Vi vil i kapittel fire begrunne de enkelte underkodene. Nå skal vi beskrive data-kvalitet, relabilitet, validitet og etikk, som er fire vesentlige aspekter ved forskning.

3.6 Datakvalitet

Datakvaliteten må sees i forhold til hva datamaterialet skal brukes til. Hensikten med datamaterialet er at det skal brukes til å belyse vår problemstilling og besvare våre forskningsspørsmål. Datamaterialets kvalitet er høyere jo mer velegnet materialet er til å belyse problemstillingen. Det at datamaterialet har en tilfredsstillende kvalitet, er en avgjørende forutsetning for å komme frem til analyseresultater som er holdbare og fruktbare (Grønmo 2007:217). Ifølge Grønmo er de to viktigste kvalitetskriteriene relabilitet og validitet. Reliabilitet referer til datamaterialets pålitelighet, mens validiteten viser i hvilken grad undersøkelsesopplegget egner seg til å samle inn data som er relevant for problemstillingen (Grønmo, 2007:220-221). Som overordnede kriterier for vurdering av datakvalitet kan relabilitet og validitet overlappe hverandre. Dette fordi høy relabilitet er en forutsetning for validitet, mens relabilitet er uavhengig av validitet.

3.6.1 Reliabilitet.

Reliabilitet forteller oss hvor pålitelig datamaterialet er. Reliabilitet defineres hovedsakelig som samsvaret mellom ulike innsamlinger av data, basert på samme undersøkelsesopplegg (Grønmo, 2007:222).

Troverdigheten man får av høy reliabilitet kommer til uttrykk ved at vi får identiske data, dersom vi bruker det samme undersøkelsesopplegget ved ulike innsamlinger av data om det samme systemet (Grønmo, 2007:220). Jo høyere reliabiliteten er, jo høyere er samsvaret mellom de innsamlede dataene.

Dersom en stor del av variasjonene i datamaterialet henger sammen med utformingen av undersøkelsesopplegget eller gjennomføringen av datainnsamlingen, tilsier dette at reliabiliteten er lav. Dersom reliabiliteten er høy, tilsier dette at det ikke er mye variasjon ifm. det metodiske.

På bakgrunn av forskjellene mellom kvalitativ og kvantitative studier, blir det hevdet at begrepet relabilitet ikke er relevant eller fruktbart for kvalitetsvurderinger av kvalitative data (Grønmo, 2007:228).

3.6.2 Validitet

Selv om reliabiliteten er høy og dataene er pålitelige, behøver det ikke å bety at dataene er relevante i forhold til det vi studerer. Datamaterialet kan ha lav validitet selv om reliabiliteten er høy. Validitet referer til datamaterialets gyldighet ift. det problemstillingen skal belyse (Grønmo, 2007:231). Validiteten er høy dersom undersøkelsesopplegget og datainnsamlingen resulterer i data som er relevant ift. problemstillingen. Validitet er et uttrykk for hvor godt det faktiske datamaterialet samsvarer med forskerens planer med undersøkelsesopplegget og datainnsamlingen (Grønmo, 2007:221).

Ekstern og intern Validitet

Grønmo (2007) sier at ekstern validitet er et uttrykk for at resultatene av eksperimentene er realistiske og kan generaliseres til vanlige situasjoner i samfunnet. Årsakssammenhengen er da ikke bare er gyldig under kunstige undersøkelses betingelser, men også under reelle samfunnsmessige forhold (Grønmo, 2007:233). Videre sier Grønmo (2007) at intern validitet dreier seg om hvorvidt eksperimentet i seg selv er gjennomført på en tilfredsstillende måte, slik at konklusjonen om årsakssammenheng ikke bare er gyldig under de kontrollerte omgivelsene (Grønmo, 2007:233).

Vi har utformet et spørreskjema med tanke på den norske helsesektoren sine kriterier til sikkerhet, kombinert med deres holdninger til det nye teknologiske konseptet Cloud Computing. Hensikten med dette er å få ledelsen til å fortelle hva som skal til for å få Cloud Computing inn i helsesektoren, sett i forhold til deres egne holdninger til sikkerhetsaspektet og norsk lovgivning. Det kan oppstå misforståelser rundt

begrepene og spørsmålene, dersom respondenten oppfatter dette på en feilaktig måte, eller dersom spørsmålene er dårlig formulert. Dette kan resultere i at det ikke blir samsvar i forbindelse med forskningsspørsmålene eller problemstillingen. Vi har derfor vært nøye med å utforme spørsmålene på en presis måte som vi mener måler det de skal måle i forbindelse med forskningsspørsmålenes- og problemstillingens formål. Dersom vi oppfatter at respondenten har misforstått spørsmålet eller feiltolket noe, så stiller vi oppfølgingsspørsmål.

Ifølge Grønmo (2007:237) er validitet mindre presist, men også mer komplekst enn reliabilitet. Derfor blir det som regel en vurderingen om validitet er mer komplekst enn reliabilitets vurderinger. Videre sier Grønmo (2007):

"I praksis er det ikke mulig å oppnå perfekt validitet i samfunnsvitenskapelige studier, og det finnes ingen enkle kriterier for hva som kan betraktes som tilfredsstillende validitet. Det finnes heller ingen, og det er ikke mulig å teste eller beregne validitet på en eksakt måte."

Kommunikativ validitet er en type validitet som blir fremhevet innen kvalitativ forskning. Dette er en type validitet som bygger på dialog og diskusjon mellom forskeren og andre, om hvorvidt materialet er godt og treffende i forhold til problemstillingen og forskningsspørsmålene. Her er det vanlig at materialet diskuteres med kildene, altså respondentene som har blitt intervjuet (Grønmo, 2007:235). Dersom intervjupersonene kjenner seg igjen i forskerens fremstilling og "godkjenner" fremstillingen, så kan validiteten betraktes som tilfredsstillende. Dialog med kilden om materialet kan også avdekke problemer og svakheter som forskeren dermed kan få muligheten til å rette opp i, dette er noe som styrker validiteten. Denne prosessen kalles aktørvalidering. En svakhet ved denne valideringen er at respondenten og forskeren kan legge ulike synspunkter og perspektiver til grunn for vurderinger av materialets kvalitet eller validitet (Grønmo, 2007:235-236). Ettersom det er normalt å diskutere datamaterialet med respondenten, ga vi dem muligheten til å få tilsendt transkriberingen av datamaterialet. Dette gjorde vi for å unngå eventuelle misforståelser. Fire av sju informanter valgte å lese gjennom transkriberingene.
Det vil si at halvparten av datamaterialet vårt er kommunikativt validert, og at den andre parten kan inneholde fortolkningsfeil fra forskerens side. Etter at vi hadde sendt

ut transkriberingene, var det en av fire som valgte å kommentere tilbake igjen, for å vurdere eller utdype hva de hadde sagt eller ment. Noe som bidrar til å styrke validiteten.

Det finnes også to andre typer validitet, nemlig kompetansevaliditet og pragmatisk validitet. Kompetansevaliditet dreier seg om forskerens kompetanse ved innsamling av kvalitativ data. Dersom forskeren har mye kunnskap på området, bidrar dette til høy validitet. Videre har vi pragmatisk validitet, som tar for seg i hvilken grad datamaterialet og resultatene i studien danner grunnlag for bestemte handlinger. Dersom handlingsgrunnlaget er godt, styrker dette validiteten.
Dette kommer vi tilbake til i kapittel 6.1.2 som omhandler praktiske implikasjoner.

3.7 Forskningsetikk

Forskningsetiske retningslinjer er utarbeidet for å hjelpe forskere og forskersamfunnet med å reflektere over sine etiske oppfatninger og holdninger. Dette for å bli mer bevisst på normkonflikter, styrke godt skjønn og evnen til å treffe velbegrunnede valg mellom motstridende hensyn (Sandvik, 2013). I følge Kunnskapsdepartementet (2009) er formålet ved forskning at det skal bidra til ny kunnskap, teknologi og metoder som vil utvide grensene for hva som er mulig å tenke. Betydelig frihet er viktig for forskeren og forskning. Den individuelle akademiske friheten er så viktig for at man skal oppnå uavhengig og pålitelig forskning, at det i 2008 ble lovfestet gjennom universitets og høgskoleloven. Dette resulterer i ulike problemer i henhold til at forskerne må finne seg i begrensninger, prioriteringer og reguleringer som blir innført til det beste for individ og samfunnet som helhet (Kunnskapsdepartementet, 2009). Forskningsetikk skal bidra til å organisere og regulere forskningen, og dreier seg derfor om individuell og institusjonell moral, og viser til flere sett av verdier, normer og ordninger.

Kunnskapsdepartementet (2009) har utviklet tiltak for utfordringer innenfor forskningsetikk. Disse tiltakene er som følgende:

- Sørge for at etiske perspektiv integreres i satsning knyttet til teknologi og forskning.
- Fortsette å støtte det forskningsetiske arbeidet som skjer i internasjonal regi.

I punkt.1 ser man i praksis resultatet gjennom utvalg, lover og retningslinjer. I 2006 kom forskningsetikkloven. Denne loven dreier seg om behandling av etikk og redelighet i forskning. Senere kom Granskningsutvalget som er en nasjonal ressurs for bedrifter, oppdragsgivere, universiteter og forskningsinstitusjoner i henhold til forskningsetikkloven. Videre har NESH (Den nasjonale forskningsetiske komite for samfunnsvitenskap og humaniora) utviklet forskningsetiske retningslinjer for samfunnsvitenskap, humaniora, juss og teknologi. Det er viktig å merke seg at disse retningslinjene ikke har samme funksjon som lover, men skal være et hjelpemiddel som viser hvilke hensyn forskere bør ha i sin forskning (Forskningsetiske komiteer, 2012). Vi vil nå diskutere de retningslinjene vi må ta hensyn til i vår forskning.

Nr. 8 – Krav om å informere dem som utforskes

"De som er gjenstand for forskning, skal få all informasjon som er nødvendig for å danne seg en rimelig forståelse av forskningsfeltet, av følgene av å delta i forsknings-prosjektet og av hensikten med forskningen" (Forskningsetiske komiteer, 2012)

Et resultat av for lite informasjon rundt forskningsfeltet kan føre til at man som forsker vil tolke respondentenes svar på feil grunnlag, i forhold til det svaret respondentene har gitt. Forskeren kan også tolke feil hvis han/henne velger å kamuflere forskningsområdet. Får respondentene for mye informasjon vil dette påvirke svarene informanten gir, ved at de svarer det de tror forskeren vil at de skal svare. Utfordringen ved å gi tilstrekkelig informasjon er ikke å gi for mye informasjon. Resultatene av intervjuet vil bli svekket ettersom svarene ikke reflekterer den egentlige situasjonen.

For å forsikre oss om at respondentene hadde tilstrekkelig informasjon, valgte vi å intervjue personer som jobbet innenfor IKT i norske sykehus. Vi sendte også ut en mail hvor vi kort forklarte om forskningsområdet, vår hensikt bak forskningen og konsekvensen av respondentenes deltagelse.

Nr. 14 – Krav om konfidensialitet

"De som gjøres til gjenstand for forskning, har krav på at all informasjon de gir om personlige forhold, blir behandlet konfidensielt. Forskeren må hindre bruk og formidling av informasjon som kan skade enkeltpersonene det forskes på" (Forskningsetiske komiteer, 2012).

Norge er et lite land, og det er noen utfordringer man kan møte. Et eksempel på dette kan være at informasjonen vi får kan spores tilbake til bedrifter eller nøkkelpersoner i bedriftene. Dette kan være spesielt utfordrende i kvalitativ forskning, da utvalget er lite og man får personlig informasjon fra respondentene. Tiltak vi gjorde for å forebygge dette var å opplyse i intervjuet at all data vil bli behandlet konfidensielt og at vi har taushetsplikt som forskere dersom de ønsket det.

Nr. 20 – Hensyn til private interesser

"Forskeren skal respektere de legitime grunner private bedrifter, interesse-organisasjoner o.l. har til ikke å få offentliggjort opplysninger om seg selv, sine medlemmer og sine planer" (Forskningsetiske komiteer, 2012). I denne delen av oppgaven tar vi blant annet for oss Cloud Computing og respondentens holdninger til informasjonssikkerhet rundt dette produktet. I offentlig sektor er det mye sensitiv informasjon, som krever høy sikkerhet. Hvis sikkerheten rundt systemet er svakt kan dette ha store konsekvenser for et sykehus. Hvis sykehusene må oppgi detaljer om sine sikkerhetssystemer og rutiner, kan dette være et aspekt som bidrar til at sykehusene ikke deltar. Dette er en av grunnene til at sykehusene har legitime grunner til å nekte videreformidling av informasjonen (Forskningsetiske komiteer, 2012). I vår undersøkelse er det ingen hensikt å avsløre noen kritiske punkter i sykehusenes sikkerhetssystem, ettersom vi kun er ute etter å se på ledelses holdninger til Cloud Computing og hva som skal til for at sykehusene tar dette i bruk.

Andre utfordringer ved dette, som i større grad er et dilemma for forskere, er at forskere kan fatte mistanke at sykehusene holder tilbake informasjon av ikke legitime årsaker. Dilemmaet for forskeren er da om man skal gå videre med denne informasjonen/mistanken, selv om dette kan medføre konsekvenser for sykehuset forskeren har tilgang til. *"Forskeren har den samme rettslige plikt som andre borgere til å avverge alvorlige lovbrudd"* (Forskningsetiske komiteer, 2012).

Nr. 30 – Etterprøving og etterbruk av forskningsmaterialet

"Forskningsmateriale bør gjøres tilgjengelig for andre forskere for etterprøving og etterbruk" (Forskningsetiske komiteer, 2012).

Dataene vi får inn fra intervjuene vil bli transkribert før vi begynner å analysere dataene. For at andre forskere skal kunne benytte seg datamaterialet og for at

datamaterialet skal bli mest mulig troverdig, valgte vi å etterprøve resultatene. Dette gjorde vi ved å sende ut mail til våre intervjuobjekter, hvor vi spurte om de ville lese gjennom våre transkriberinger i tilfelle det var blitt noen misforståelser.

Vi har benyttet oss av god henvisningsskikk ved å dokumentere hvor vi har tatt de ulike sitatene ifra i tillegg til å vise til "forfatteren" av de ulike teoriene som har vært med å danne bakgrunn til vår oppgave samt bidra til inspirasjon.

3.8 Oppsummering.

I metodekapittelet har vi illustrert hvordan studien er konstruert ut i fra de ulike valgene vi har tatt i forbindelse med vår forskningsstrategi. Ettersom vi tidligere i oppgaven fremstilte ulike design innenfor studier om informasjonssystemer, endte vi selv opp med et casestudie. Vi har intervjuet syv personer fra ledelsen i helsesektoren. Dette gjorde vi for å finne ut mer om deres holdninger til produktet Cloud Computing og informasjonssikkerhet.

Videre har vi gjort en rekke valg, disse valgene er basert på metodikk av en rekke ulike forskere. Dette er noe som har hjulpet oss i forbindelse med oppgavens struktur, samt hvordan vi skal forholde oss til dataene vi har samlet inn. Selve dataanalysen vil komme i neste kapittel.

4. Analyse av datamaterialet

"Analyser av kvalitative data er en fortløpende prosess, som kan knyttes til de beslutningene forskeren foretar i løpet av datainnsamlingen. De valgene forskeren tar, kan betegnes som analytiske valg, i den forstand at de kan knyttes til den forståelsen forskeren utvikler i løpet av feltarbeidet, slik at forskeren kan vurdere om de fremgangsmåtene som benyttes, gir relevant informasjon. Begrepet analyseprosess henspiller på det arbeidet forskeren utfører for å utvikle en forståelse av materialet" (Thagaard, 2002:109).

I tidligere kapitler har vi beskrevet teorier som utgjør hovedessensen i vår empiri. Dette gjelder våre metodiske valg når det kommer til valg av informanter og fortolkningen av de empiriske innsamlede dataene. I dette kapittelet vil vi nå analysere, fortolke og kategorisere det empiriske materialet vi har tilegnet oss gjennom intervjuer.

Vår intervjuguide inneholder 13 kategorier som er relatert til sikkerhet, teknologi-konseptet Cloud Computing og holdningskomponentene i trekomponent-modellen. Vi vil videre beskrive kategoriene i intervjuguiden og dagens situasjon i forhold til Cloud Computing i norske sykehus. Vi vil deretter gjennomføre selve analysen ved beskrivelse og tolkning av datamaterialet.

4.1 Kategoriene som er brukt i intervjuguiden

Innen temaet etablering av Cloud Computing innenfor offentlig sektor, er det mange temaer vi kan ta med i en undersøkelse. I og med at vi ikke hadde ubegrenset med tid var vi bevisst på at vi ikke kunne ta med for mange temaer, og vi beregnet ca. 1 time med intervjutid pr informant. Dette begrunner vi med at informantene i hovedsak er ledere som har knapt en time til overs i en travel arbeidshverdag. Vi kom frem til de ulike temaene gjennom intern diskusjon i gruppen, samt veileder. Vi så også på andre undersøkelser innenfor lignende temaer for å få ideer til gode spørsmål. Disse har vi diskutert med veileder og kontaktperson i CSC for å få de formulert på en best mulig måte. Vi har valgt å dele de ulike kategoriene inn i de forskjellige komponentene, resultatet av dette er tabellen under.

Kunnskap og persepsjon (Den kognitive komponenten).	**Følelser (Affektkomponenten)**	**Intensjon (Atferds komponenten)**
Forståelse	*Generell holdning*	*Videre arbeid*
	Kollegaers holdning	
	Gevinster og risikomomenter	
	Kostnadseffektivisering	
	Effektivisering	
	Utfordringer innenfor offentlig sektor	
	Beliggenhet og lovverk	
	Sikkerhet i nåværende systemer vs sikkerhet i Cloud Computing	
	Sikkerhetsmessige utfordringer	
	Brukervennlighet	
	Brukerstøtte	

Tabell 6: De ulike kategoriene til de forskjellige komponentene

I den kognitive komponenten vil vi ta for oss begrepet *"forståelse"*, dette fordi vi ønsker å kartlegge hvordan kandidatene definerer Cloud Computing. Dette igjen for å forsikre oss om at vi har den samme oppfatningen av Cloud Computing, slik at vi kan unngå eventuelle misforståelser.

I den affektive komponenten kan flere av kategoriene oppfattes som antakelser-/kunnskap, men vi velger å fokusere på intervjuobjektenes følelser relatert til for eksempel sikkerhetsmessige utfordringer og de andre kategoriene. For å finne ut hva ledelsen i helsesektoren tenker om Cloud Computing, så har vi valgt å ta med kategorien *"generell holdning"*. Dette for å se om ledelsen har en positiv eller negativ holdning til konseptet. Hvis ledelsen har en positiv holdning, vil det si at produktet

har en reel sjanse på markedet til tross for eventuelle hindringer som skulle dukke opp, men dersom ledelsen har en negativ holdning til konseptet så skal det betraktelig mer til for å gjennomføre implementeringen.
Videre tok vi med en kategori som heter *"gevinster/risikomomenter"*. Dette for å se hva ledelsen i helsesektoren mener Cloud Computing kunne bidra med, eventuelt hvilke risikoer det innebærer.

Vi har også tatt med kategorien *"utfordringer i offentlig sektor"*. Dette punktet tar for seg tanker og følelsesmessige holdninger knyttet opp mot sikkerhetsmessige utfordringer til Cloud Computing.

Ettersom sikkerhet er et viktig aspekt så ønsker vi å sammenligne sikkerheten til nåværende systemer vs. sikkerheten i Cloud Computing. Dette for å eventuelt avdekke positive eller negative sider rundt systemene. Denne kategorien kalte vi for "*Sikkerhet i nåværende systemer vs. sikkerhet i Cloud Computing"*

Siden det offentlige blir styrt og kontrollert gjennom lovverk, valgte vi å kalle denne kategorien for *"Beliggenhet/Lovverk"*. Dette gjorde vi for å få avklart hva som må være tilstede når det kommer til norske lover, for at en implementering av Cloud Computing skal være mulig.

Neste kategori tar for seg kollegaene til de forskjellige lederne i helsesektoren Dette for å kartlegge deres følelsesmessige holdninger til bruk av Cloud Computing. Denne kategorien kalte vi for *"kollegaer"*.

En annen kategori er *"brukervennlighet",* denne kategorien tar for seg kandidatens følelsesmessige holdninger til brukervennlighet innenfor Cloud Computing. Dette var et punkt vi synes var relevant å ha med, ettersom sykehusenes nåværende systemer ikke er spesielt brukervennlige.

"Brukerstøtte" er også en kategori vi anser for å være viktig, ettersom den tar for seg deres følelsesmessige holdninger til brukerstøtte i Cloud Computing. Noe som igjen er viktig ettersom det er et essensielt punkt i helsesektoren.

”Effektivisering” dreier seg om informantenes følelsesmessige holdninger og synspunkter når det kommer til effektivisering av deres nåværende IKT system ved hjelp av Cloud Computing.

En annen kategori som vi anså for å være relevant er *”kostnadseffektivisering”*. Denne kategorien ser på kostnadsaspektet på sykehusenes nåværende systemer kontra det å ta i bruk et Cloud Computing produkt.

Den atferdsmessige komponenten kommer til slutt, her har vi valgt å ta med en kategori som het *”videre planer”*. Denne kategorien tar for seg informantenes intensjon om bruk av Cloud Computing i nærmeste fremtid.

Det kunne antakeligvis vært med flere kategorier, men pga. oppgavens størrelse, valgte vi å stoppe her. Nå skal avhandlingen analyseres, men før det skal vi begynne med å beskrive dagens situasjon i analyseenheten med tanke på Cloud Computing i den norske helsesektoren.

4.2 Dagens situasjon i forhold til Cloud Computing i norske sykehus

Det finnes et stort potensiale for å utnytte Cloud Computing tjenesten i offentlig sektor i Norge. Ved at Cloud Computing blir levert som en ”on-demand tjeneste” og man bare betaler for den faktiske bruken, utvikles tjenesten raskt til et seriøst alternativ til tradisjonelle IT-anskaffelser (Møller, 2013). Cloud Computing innenfor sykehus kan inneholde en rekke løsninger, alt fra den daglige pasientbehandlingen til rene administrative systemer. Det er allerede blitt tatt i bruk Cloud Computing innenfor Helse Sør-Øst, dette er på mindre områder som ikke er virksomhetskritiske. I norske sykehus er det utfordrende å ta dette i bruk på mer virksomhetskritiske løsninger ettersom helsetjenesten er styrt og regulert av forskrifter og lover. Dette setter spesifikke krav til hvordan pasientopplysninger behandles, dette er en stor utfordring når det kommer til å kunne ta i bruk Cloud Computing på en trygg og effektiv måte for helsetjenesten i dag. Etterhvert som tjenester og løsninger blir etablert i markedet, vil dette åpne opp for nye muligheter (Christensen, 2013). Sikkerhet er en av de største barrierene når det kommer til bruk av Cloud Computing i offentlig sektor.

4.3 Analyse med utgangspunkt i trekomponentmodellen.

Vi har tatt vårt utgangspunkt i Rosenberg og Hovlands trekomponentmodell. Denne modellen omhandler holdning i form av en disposisjon som gjør at når man fortolker et stimuli (f.eks informasjon evt. atferd), så reagerer man følelsesmessig (affect) og/eller utvikler antakelser (cognition) og/eller utfører en bestemt atferd/handling (behavior). Videre i dette kapittelet vil vi illustrere og forklare holdningene informantene har til Cloud Computing i den norske helsesektoren. Dette vil vi gjøre med tanke på komponentene *følelser, kunnskap og atferd*. Når vi videre i oppgaven skal sitere informantene våre, så har vi fått deres aksept til å bruke fullt navn.

4.3.1 Kunnskap angående Cloud Computing

Trekomponentsmodellen til Rosenberg og Hovland tar for seg komponenten kunnskap. Dette innebærer tanker, meninger og tro som påvirker menneskers holdninger. I vårt tilfelle ser vi hvordan informantens holdninger påvirkes av denne komponenten innenfor de ulike kategoriene. Vi ønsker å kartlegge om kunnskapene angående Cloud Computing påvirker informantenes holdninger i forhold til sikkerhet, forståelse, holdning etc.

Ettersom kunnskap er en sentral indikator i forhold til oppgavens tema, valgte vi å spørre informantene hvordan de oppfatter begrepet Cloud Computing. Enkelte av våre informanter var svært konkret når det kom til en definisjon. Cloud Computing er relativt nytt og er ikke konkret innenfor helsesektoren. En av informantene påpekte dette *"Umiddelbart tenker jeg tåkeheimen, fordi det er veldig udefinert for oss i helsesektoren."* (Henriksen). En annen usikker informant sier *"Nei, ikke noe annet enn at dataene ligger et eller annet sted, på en eller annen server, hvor som helst som ikke er definert, så når du disse tjenestene. Det er vel snakk om tjenestestyring og tilganger, du får tak i informasjonen der ute i skyen, ute i internett. Det er jo internett liknende vil jeg tror."* (Knutsen). Enkelte av de andre informantene var mer detaljerte når det kom til en definisjon rundt forståelsen av Cloud Computing *"Jeg definerer Cloud Computing som mobiliteten og tilgjengeligheten til informasjonen der du er, når du trenger det."* (Nystuen). *" Det er jo muligheten for å bruke skya, kall det en ressurs, hvor du faktisk får en tjenester levert gjennom skyen, uten at du nødvendigvis henger deg oppi hvordan den skya ser ut. Du kan kjøpe tjenester, lagringskapasitet, applikasjoner og andre ting gjennom skya og ha det der ute, og alt som skjer der inn*

behøver du ikke som bruker å bry deg om. Du har de tjenestene tilgjengelig uavhengig av hvor du selv fysisk er, men fordi du er den du er så har du tilgang til det du skal ha." (Lund).

Det ser ut til at våre informanter har en variert forståelse av begrepet Cloud Computing, men vet generelt hva det innebærer og hvilke muligheter man har *"Jeg tenker på Cloud Computing som løsninger, tjenester som er skalerbare, fleksible i alle retninger og som rent teknisk sett skiller lagrene på en slik måte at vi ikke trenger å tenke på tjenestene som ligger i bunnen eller hvilken hardware man kjøper inn. Man har en tjeneste på toppen som man kjøper også bruker man den."* (Blindheim).

Konseptet Cloud Computing blir ikke bare sett på som en lagringsbasert skytjeneste, men også en skalerbartjeneste med varierte muligheter. Kunnskapen om infrastruktur, tilleggsapplikasjoner og beliggenhet er også tilstede "*Da tenker jeg jo at vi har IKT tjenester i skyen, hvor du også har det underliggende. Å med det underliggende da mener jeg altså både infrastruktur og programvarer som ligger andre steder, det kan ligge hvor som helst i verden."* (Borthne).

Informantene i intervjuene har gjort rede for sin forståelse av Cloud Computing, og dette tyder på at konseptet er relativt nytt, men at informantene har en generell forståelse av begrepet. Ettersom teknologien ikke er anvendt innenfor sykehusene så medfører dette usikkerhet, noe som igjen antyder at de ikke kan nok om konseptet. Informantene har forståelse for teknologien, men mangler den tekniske kompetansen og stoler derfor på kompetansen til IT tjenesten *"Jeg er mer den forretningsmannen og har forretningsforståelsen, for hva virksomheten trenger i forhold til kjerne-virksomheten. Men jeg hviler meg jo selvfølgelig på kjernekompetansen som ligger i Sykehuspartner."* (Nystuen).

4.3.2 Følelser angående Cloud Computing i norske sykehus

Ut i fra Rosenberg og Hovlands modell forklarte vi at følelseskomponenten omhandler følelser og drifter. Dette er i følge forfatterne den komponenten som er mest evaluert, da man gjerne har komponenter som har positive og negative følelser i forhold til objektet som utgangspunkt.

Generell holdning

En sentral indikator i informantenes holdning til Cloud Computing relaterte spørsmål, er hvorvidt de har positive eller negative følelser til Cloud Computing og mulighetene rundt det. Derfor har vi spurt etter deres generelle holdning til Cloud Computing. Vi så fort at alle informantenes holdninger tok utgangspunkt i sikkerheten rundt Cloud Computing *"Altså Cloud Computing er jo i utgangspunktet en veldig spennende teknologi sånn sett. Vi har fått mange forespørsler, men vi er regulert av lovgivning, så det pålegges at vi har kontroll, spesielt på informasjonssikkerheten."* (Henriksen). Videre sier en annen informant noe av det samme *"Jeg vil tro at vår holdning er på en sånn sunn skepsis, dette i forhold til å etterspørre leverandører, i forhold til hva slags avtaler de har med sine underleverandører igjen. Nettopp i forhold til dette med personvern og data-behandling som er viktige avtaler for oss i helsesektoren, med tanke på personvernet."* (Nystuen).

De fleste av informantene har et åpent sinn mot Cloud Computing, noe som tilsier at de er nysgjerrige, men ikke helt trygge på det som er nytt med tanke på sikkerhet, kontroll og lovverk *"Jeg er forsiktig nysgjerrig, jeg bruker ikke mye tid på å sette meg inn i Cloud Computing, så lenge vi ikke får noen føringer fra regionen. For vi styres jo veldig IT-messig av det regionale foretaket, og det er jo sykehuspartner som har de tekniske løsningene. Og når det begynner å materialisere seg eller når de skal begynne å utvikle seg, så vil vi komme inn og se på hvordan dette vil påvirke oss da. Jeg tror jo ikke det vil påvirke oss i noen særlig grad, annet enn at jeg håper tjenestene blir billigere, så håper jeg den tjenesten blir mer stabil kanskje, og at tjenestene vår ikke blir så personavhengige som det har vært."*(Knutsen).

Enkelte av informantene er positive til Cloud Computing og tror at det kan bidra positivt på enkelte områder. Samtidig er de redde for at dette vil bidra til nye trusler "*Jeg er grunnleggende optimist, og er da positiv. Cloud Computing er et interessant alternativ som vi vil se at vil kunne ha fordeler på flere av områdene som du nevner, men ikke nødvendigvis alt. Cloud Computing introduserer nye muligheter på ulike områder, det er for så vidt nøytralt og introduserer andre risikobilder, andre trussel scenarioer og det introduserer andre forretningsmodeller. Det er ikke gitt at Cloud Computing er billigere."* (Blindheim).

I sitatet under så kommer en av informantene med to klare punkter på hvorfor han ikke tror Cloud Computing blir brukt i norsk helsesektor ”*Skytjenester generelt bruker jeg i jobb til daglig, og en god del til privat bruk. Og det er jo det jeg også ser, at de som jobber i sykehuset privat, de bruker jo tlf sine, bruker nettbrettene og alt mulig annet. Særlig når de unge kommer inn, så blir de jo frustrert over at vi har det så gammeldags på mange måter. Men jeg tror nok at her i Norge, at årsakene til at vi ennå ikke bruker skytjenester, går først og fremst på to ting:*

1) sikkerhet: Vi har ikke god nok innsikt i hvordan sikkerhetsproblematikken er løst, verken på lagring eller på hacking av systemene, eller hva det nå enn skal være for noe. I tillegg til det så er det så vidt jeg vet ennå en vis usikkerhet, tror jeg, forskningsmessig også rundt konsistensen.

2) Konsistens: Med det så mener jeg: Hvis man stiller det samme spørsmålet fra to forskjellige steder i verden mot en skytjeneste så er man ikke 100% sikker på at man vil få samme svar ut fra de to stedene, slik jeg har oppfattet det.

Så konsistensen er en problemstilling, sikkerhet er helt klart en problemstilling. Men om det er en reel trussel som er større enn det vi har i dag av sikkerhetsproblemer i de systemene vi bruker lokalt, distribuert i regionen mellom sykehusene i dag, det er jeg usikker på.” (Borthne).

Kollegaer

Videre ønsker vi å se hvordan de forskjellige informantene ser på sine kollegaers holdning til bruk av Cloud Computing i norske sykehus. Dette for å se hvordan informantene tolker sine kollegaers holdning.

”Det var et veldig godt spørsmål, det er nok alt etter hvor i regionen og i Norge man snakker med folk, og mange har forskjellige definisjoner over hvor man legger lista. Helse Sør-øst har nok definitivt den strengeste tolkningen.” (Henriksen).

Ut i fra utsagnet til informanten over så er det veldig spredt mellom hva ulike kollegaer tenker om produktet, men at det varierer fra region til region.

”*Dette kommer nok av at vi har veldig mye mer kontroller fra datatilsynet enn for eksempel de i Helse Nord. Så de har senket terskelen litt på hvor mye de aksepterer og ikke aksepterer, mens innad i Helse-Sør Øst så er det vel Vestre Viken, A-hus, OUS som har de strengeste mekanismene, men det er jo fordi at vi er noen av de største foretakene og forvalter vanvittig med opplysninger, og det er vel også litt forskjell på åssen fokus de ulike helseforetakene har hatt på sikkerhet. Noen sitter i en*

sikkerhetsstilling som nesten som et lite alibi for sykehuset. Så er det noen som har blitt satt inn med litt mindre kompetanse og dermed velger de å distansere seg litt, eller bare sier seg enige med Vestre Viken, OUS og A-hus." (Henriksen).

Enkelte av informantene er mer tydelig på hva de vil ha *"Altså, hvis vi ser på avdelingene mine og mine ansatte. Så er jo jeg informasjonssikkerhetsansvarlig og personvernombudet i avdelingene mine. Så her har vi jo både en gass og brems funksjon. Så sånn sett så får vi jo den dynamikken i det, men også da som kjernevirksomheten og der ute i sykehusene. De vil jo ha det, fordi de ser hvilken fleksibilitet de har til Cloud Computing hjemme og i privates affære. Så holdninger til det er jo at, dette her, vil vi ha."* (Nystuen).

Men igjen så er ikke alle like åpne for konseptet ennå, enkelte mener at konseptet ikke er modent nok til å bli tatt inn i det offentlige. Dette er fordi de mener at det ikke er utviklet nok i forhold til sikkerhet etc. *"De som jobber med dette her, de er på samme bane, de skjønner det. Utfordringene for oss er at loven setter de begrensningene som den gjør, og vi har en foreldet uhensiktsmessig infrastruktur i dag."* (Lund). Videre finnes det også noen av kollegaene som ikke tenker stort på dette med Cloud Computing og at det lite omdiskutert *"Nei jeg tror ikke de har noen tanker om dette, bortsett fra kanskje han som driver med sikkerhet. Men jeg tror de ikke har tenkt noe på det, det er ikke noe tema i våre avdelingsmøter eller i våre gruppe."* (Knutsen).
"Det diskuteres veldig lite. Så du kan si internt i sykehuset så er ikke noen levende debatt. Jeg har heller ikke opplevd at det har vært noen levende debatt i de relasjoner jeg har hatt i forhold til sykehuspartner eller i de relasjonene jeg har hatt til Helse Sør-Øst. Vi er liksom milevis unna den tenkningen, vi har nok med det daglige strevet med de systemene som vi faktisk har, som begynner å bli utdatert på mange områder." (Borthne).

Gevinster og risikomomenter

Under denne kategorien ønsker vi å ta for oss informantenes holdning til gevinster og risikomomenter ved bruk av Cloud Computing. Informantene sier at det finnes både positive og negative sider ved bruk av skytjenester. Ettersom kunnskapen varierer er det spennende å se hvordan deres holdninger gjenspeiles i forhold til tanker og følelser. Først vil vi se på eventuelle gevinster, før vi går over til risikomomenter.

Informantene er enige om at det er store fordeler ved bruk av Cloud Computing, spesielt i forhold til samhandling, effektivisering og informasjonsdeling ”*Det kan jo bidra til en god samhandling, spesielt inn og ut på kommune nivå. Der man ønsker og ha en sterkere og effektiv samhandling, det gjør det uten tvil.”* (Henriksen). Dette blir brekreftet av Nystuen *”Jeg tenker helt klar det kan bidra mye. Dette med tanke på å jobbe mer effektivt, og med å ha raskere og mer skalerbare søkbare løsninger. Kommer litt bort fra det proprietære bedriftsmiljøene, til å få det til å ha den skalerbarheten og få det trøkket og den ytelsen ut.”* (Nystuen).

I følge Lund er det å få en Cloud Computing tjeneste fra en ekstern aktør noe som kan bidra til skalerbarhet og effektivisering *”Det er jo skalerbarhet. Utgangspunktet er jo at IKT ikke er noe helsevesenet skal drive med. IKT er noe vi gjør fordi det er såpass viktig for foretaket, for pasienter, det har med effektivisering å gjøre.”* (Lund). Noen av informantene ser på kombinasjonen av tjenester og forretningsmodeller for å oppnå en optimal kostnadseffektivisering *”Med kombinasjonen av riktig tjenester og riktig forretningsmodeller så kan vi få gjort mer for en billigere penge. Men det avhenger av område.”* (Blindheim).

Flere av våre informanter tenker at Cloud Computing vil bidra til kostnads-effektivisering sammenlignet med deres nåværende systemer. Grunnen til dette er at deres nåværende systemer ifølge informanten er ineffektive og dyre *”Kostnads-perspektivet er veldig viktig, for vi ser jo at kostnadene på IKT siden nesten har eksplodert. I tillegg til dette har vi etter min mening alt for store vanskeligheter med den ordningene fra Mal-tjenesteleverandør, hvor vi nok etter mitt syn får for dårlige tjenester og alt for dyre. Når jeg kom hit i 1999, før vi outsourcet til sykehuspartner, så var årsbudsjettet for IKT 91 mill og nå er vi oppe i 300 mill, med dårligere tjenester som jeg ser det. Det ville definitivt vært kostnadseffektiv”* (Borthne).

Gevinstene er i hovedsak kostnadseffektivisering, skalerbarhet, fleksibilitet og effektivisering. Men det er også store risikomomenter og mulige begrensninger når det kommer til Cloud Computing innenfor sykehusene *”Helsesektoren er jo en veldig spesielt sektor. Vi skal jo forvalte opplysninger om våre ansatte som også kan være sensitiv informasjon, i tillegg har vi jo også den pasientinformasjonen. Kommer denne på avveie så er det jo kjempe kritisk. Det er jo mange som vil ha tak i den, alt*

fra kriminelle til bank til forsikringsselskap. NAV vil jo alltid ha mer opplysninger enn det de har krav på. Inkludert Politiet, vi har de ofte nede i akutt mottaket der de står å "fisker" og vil ha ut mer informasjon enn det de er berettigete til å ha. Vi er nok sikkert litt paranoide, men konsekvensene hvis det kommer ut er enorme." (Henriksen). Det kommer fort frem at det største risikomomentet er at andre kan få tilgang til sensitiv pasientinformasjon, og at den kan komme på avveie "*Deling av opplysninger er en fordel, men vi har den lov barrieren som vil stanse oss, slik det er i dag."* (Henriksen).

I tillegg til informasjonssikkerhet så er kunnskap og konsistens også en viktig risikofaktor *"Jeg tror sikkerhet og kunnskap om hva det egentlig dreier seg om er det viktigste. Så tenker jeg også ut i fra det jeg har lest, men som jeg ikke har presis kunnskap om. Dette med konsistens, altså at man er sikker på at når man gjør en spørring innen skytjeneste at man da faktisk får det det riktige svaret tilbake igjen. Hvis dette ikke er 100 % så er det en stor risiko."* (Borthne).

Kostnadseffektivisering

Vi spurte våre informanter om hvilke holdninger de hadde til kostnadseffektivisering ved bruk av Cloud Computing i norske sykehus *"Det er jo mange av det, ikke sant! Men jeg tror jo at det aller viktigste, er dette med at du har den skalerbarheten. At du kan på en måte si at nå er det to måneder at nå vil jeg ha den "power'n" og de neste to månedene så trenger jeg den ikke. Så kan du på en måte justere og styre mer etter behov."* (Borthne). Enkelte av informantene mener at det ville blitt besparelser når det kommer til både tid og penger *"Jeg tror at kostnadene ville sunket betraktelig, og vi hadde blitt spart for mye plunder og heft."* (Knutsen).

Videre tar en av informantene opp at sykehusene ikke skal drive med IT, det er kun et hjelpemiddel som skal bidra til effektivitet *"Kostnadseffektivisering er absolutt et tema. Dette med kompetanse, sårbarhet på kompetanse er noe vi vet at vi vil løpe inn i. Det å slippe å gjøre det selv, det er det som ligger i det jeg sier at vi ikke skal drive med IT."* (Lund).

To informanter mener at det ikke er gitt at Cloud Computing representerer noe form for kostnadseffektivisering *"Det er ikke gitt at Cloud Computing representerer en kostnadseffektivisering"*. (Blindheim). Dette blir bekreftet av kollegaen som er

tilstede *"Jeg tenker at hvis dataene ender opp med å kunne ligge potensielt i to forskjellige land, og dette skal inneholde personsensitiv informasjon, for eksempel i Amsterdam. Så når vi da ivaretar vårt oppfølgingsbehov og oppfølgningsforpliktelser i forhold til revisjon etc. Så kan det hende at vi må reise ut dit med litt frekvens for å følge dette opp. Så har du gjerne typiske nyttetap på det at vi får ikke tilpasset løsningen helt sånn som man gjerne skulle hatt det, man må gjerne ofre noe. Å da blir spørsmålet hvor godt det som er ute i markedet våre behov, hvis nytten er sånn "bob bob" eller tilpasningen sånn "bob bob" så har det kanskje en ren økonomisk effekt, men så taper man på andre punkter, man får litt tyngre arbeidsprosesser fordi man kanskje må flytte ting via de eksterne og interne systemene."* (Losnegaard).

Effektivisering

Vi spurte informantene om deres holdninger til effektivisering av deres nåværende IT system ved hjelp av Cloud Computing som et supplement til dette

"Skulle vi innført en skytjeneste så ser jeg for meg at noen hadde syntes at dette var en meget lettvint måte å kommunisere pasientopplysninger på. Dermed ville man f.eks. hatt en epikrise på to steder, det vil si at vi hadde fått en dobbellagring av journaldokumenter, i tillegg ville det også bli ansett som et nytt helseregister hvis noen hadde begynt å legge pasientdata i skyen, eller persondata. Da hadde det plutselig blitt et personregister som igjen er konsesjonspliktig." (Henriksen)

Samhandling av pasientinformasjon er i dag ikke et aktuelt tema, selv om dette hadde vært veldig effektivt *"Samhandling av pasientinformasjon er i dag ikke et aktuelt tema, selv om dette hadde vært veldig effektivt. Det hadde ikke fungert at alle sykehusene i Norge hadde samme informasjon i ett system, det er faktisk litt av utfordringen som vi har i dag, samhandlingen går litt smått og tregt. Vi får faktisk ikke lov til å sammenblande data slik lovgivningen er i dag. Igjen så er det dette med informasjonssikkerhet og skillemekanisme som kommer å slår inn."* (Henriksen).

Vi kom med dette eksempelet til informanten: La oss si at en pasient som var fra Sør hadde vært på ferie i Hønefoss og blitt skadet her, så i stedet for at det hadde blitt sendt en forespørsel til sykehuset på Sørlandet, hadde dere hatt all informasjon liggende her. Dette resulterte i at vi fikk vite litt om kjernejournalen som er under progresjon *"Ja, og det er jo der den nasjonale kjernejournalen kommer inn og skal "redde" oss med en løsning som gir et sett med grunndata om pasienten tilgjengelig*

for helsepersonell uansett hvor man befinner seg i Norge." (Henriksen). Informantene mener at effektiviseringsmulighetene ved Cloud Computing er store innenfor helsesektoren. Dette blir bekreftet av Nystuen "*Jeg tror at mulighetene ved Cloud Computing er store innenfor effektivisering". Mye med tanke på forsering når det kommer til oversikt, montering og skalerbarheten."* (Nystuen).
Cloud Computing gir en effektiv mulighet til å prøve ut nye løsninger som krever betydelig med kapasitet *"Jeg tenker det innenfor å drive innovasjon. Prøve ut nye løsninger, samtidig som man får den fleksibiliteten man trenger."* (Nystuen).

Ettersom dette er en forholdsvis ukjent teknologi innenfor helsesektoren så er ikke alle potensialene synlige *"Jeg tror det ligger et potensiale der, innenfor Cloud Computing, som vi ikke evner å utnytte i dag."* (Lund). Det er leverandøren som legger opp til hvor effektiviserende løsningen skal være *"Skal man kjøpe nettskyløsninger i dag så er det ganske store forskjeller mellom aktørene, hva de tilbyr i totalitet. Totalitet går da på teknologi i bunnen og robusthet, det går på hvilke egenskaper de har bygget inn."* (Blindheim).

Utfordringer innenfor offentlig sektor

De ansatte i sykehus sektoren jobber til daglig med sensitiv informasjon, arbeidsoppgavene kan variere alt fra å behandle personnummer til helsemessige problemer. Vi spurte informantene hva de tenkte ville være den største utfordringen innen offentlig sektor, dersom Cloud Computing hadde blitt innført. Som vi tidligere har forstått på informantene så er den offentlige helsesektoren i Norge beskyttet av personvernloven og pasientsikkerhetsloven *"Jeg tror den største utfordringen er vår kompetanse og forståelsen vår, når det gjelder hva er det vi oppfatter med at løsningen er sikre."* (Nystuen). Et tema som kom frem var "Snowden effekten" og implementeringen av skyløsningen *"Implementere er sånn sett ganske lett, det er i hovedsak sikkerhet med CMS på å ta vare på informasjonsaktiva som ligger i skya, og samt den fysiske delen av det."* (Henriksen). Etter Snowden saken har myndighetene sett hvordan NSA (National Security Agency) jobber, og dette har gitt et bilde av hvilke utfordringer personvernet nå står ovenfor *"Vi har jo hatt den Snowden saken, alle har jo vært borti han. Så her er spørsmålet hvor mye av kildekoden til disse skytjenestene som ligger ute tilgjengelig, for eksempel amerikansk forsvar NSA etc, som gjør at de kan komme seg inn i løsningen våres, hvis vi skulle brukt noe sånt. Så*

igjen så havner vi tilbake til dette med sikkerhetsaspektet, det gjør vi altså. Det er i grunn det som stopper oss slik det står i dag." (Henriksen)

"Snowden saken har jo brakt frem spionasje og det at noen stater tar seg til rette ovenfor firmaer som juridisk hører til dem, og kan ta som NSA har vist seg villig til å gå inn i andre lands informasjon og hente ut den på lovlig og ikke lovlig måte, det er mye spekulasjon. Men da snakker vi om persepsjon og tillit." (Blindheim).

"Jeg tror at det er kompetansen som bestemmer om vi skal være redde eller være vennligstemt til løsningene. Da går det både på leverandørsiden, de skal forstå hvordan vi jobber, hvorfor vi er så redd for det vi har, å ha god forståelse for at de tekniske løsningen faktisk er sikre." (Nystuen).

En annen kritisk faktor i helse Norge er tap og misbruk av pasientsensitivinformasjon. Dette blir bekreftet av informantene *"Det er tap av informasjonen som er helt klart frykten, så er det tap og misbruk av informasjon. Også er det hvor langt er det man ønsker å gå i forhold til overvåking, for det er jo noe man da må gjøre. Man beveger seg inn i et samfunn hvor tekniske løsninger faktisk åpner for stor grad av overvåking eller kontroll, så det går litt på hvor langt vil du strekke den, kontra den helse gevinsten man oppnår ved å være tilgjengelig. Jeg tror at utfordringen er å finne den rette balansen på det."* (Nystuen)
Dette blir påpekt av flere av informantene, samtidig som de mener Cloud Computing er den rette veien å gå *"Ja for helsesektoren så er jo det den største faktoren at vi opererer med så mye sensitiv informasjon, som du ikke kan eksponere på nett, på lik linje med alt mulig annet. Ligningsinformasjonen din og skatteinfo er ikke like sensitivt som opplysninger om tidligere abort eller ungdom som har vært innlagt med en eller annen mystisk sykdom, det er sensitiv informasjon. Dette er informasjon som er regulert av egne lover og kan by på utfordringer. Men det vi må leve med er at helseinformasjon alltid kommer til å være definert som noe sensitivt, noe som må håndteres unikt. Men i offentlig sektor så mener jeg Cloud Computing er en vei å gå. Det skjer jo allerede, det er jo allerede bevegelser på det."* (Lund).

Et annet problem som dukker opp er hvordan man skal differensiere informasjonen om pasienten mellom de forskjellige ansatte i sykehusene. Skal sykepleiere få like

mye informasjon som for eksempel legen på akutten *"Men jeg mener jo at det i første rekke er et skaleringsproblem, vi har jo det samme problemet inne i sykehusene, så det er jo ikke slik at journalen skal være åpen for alle som jobber innenfor sykehuset, tvert imot, vi skal ha en stram styring her også. Greier vi å få det til for et sykehus, så må det også gå an å få til for en region eller et land, så det tror jeg bare et skaleringsproblem, ikke et reelt et."* (Borthne).

Beliggenhet og lovverk

Norsk lovgivning er veldig streng når det kommer til lagring av personopplysninger og annen sensitiv informasjon. Et essensielt tema er hvor disse dataene lagres og hva lovgivningen rundt dette sier. Vi spurte informantene om deres holdning til lagring av data sett i sammenheng med lover og regler *"Helsevesenet er regulert av egne lover og regler. Det betyr at all informasjonen som vi har her må lagres i Norge. Vi får ikke lov til å flytte pasientinformasjon utenfor Norges grenser."* (Lund). Videre gikk vi inn på temaet om lagring av pasientopplysninger i Norge, og enkelte mente det ville bli lettere dersom opplysningene var lagret i Norge *"Det hadde forenklet det på noen punkter , rett og slett fordi vi hadde ikke hatt for eksempel en bekymring for USA. Skal vi ha lagret data i USA, så er vi avhengig av å ha den Safe Harbor avtalen. Allikevel, hvis vi skulle hatt det i Norge som står sortert under norsk lovgivning, så ville det allikevel vært utfordrende fordi det er jo krav til hvordan vi kan dele data og hvilket data vi kan sende ut. Det er krav til kontroll, så vi ville fortsatt vært avhengig av DLP for å bruke en nasjonal Cloud Computing,"* (Henriksen).

Safe Harbor-avtalen var også et tema som ble nevnt av flere informanter. Losnegaard tar også opp "Snowden" *"Nå har vi for så vidt handelsavtaler med EU, Safe Harbor avtalen sier at i utgangspunktet skal man kunne handle med den type tjenester innenfor EU men også innenfor enkelte virksomheter i USA. Det er ikke gitt at et politisk nivå ville sagt det at det ikke er godt nok hvis man klarer å ivareta teknisk sikkerhet godt nok og avklarer alle de juridiske spørsmålene rundt dette her. Men særlig i disse Snowden tider er det ekstra mye fokus på risiko."* (Losnegaard). Videre tar Blindheim for seg et eksempel rundt det med lagring i utlandet *"I disse "Snowden tider", hvis vår data hadde vært i utlandet, Sverige har nettopp etablert eller skal etablere en løsning basert på Microsoft HealthVault som er en skytjeneste med datalagring i Irland og Amsterdam. Da har de god beskyttelse på mange måter rent*

juridisk, men det kan være variasjoner i regelverket innenfor EU, vi har foreløpig ikke skaffet oss oversikt over typer av dette med etterretningsregelverk som kommer på tvers av personvernregelverket som begrenser rekkevidden av dette her." (Blindheim).

Et annet aspekt av temaet er sekundære lagringslokasjoner og sikkerhet, dersom det skulle oppstå komplikasjoner *"Skytjenester trigger disse spørsmålene i sin fulle bredde. I sin natur vil de spende på tvers av nasjonale grenser. En norsk aktør som ønsker å bygge en skytjeneste i Norge ville av veldig naturlige grunner i etter utviklingsperspektiv søke å ha minst en sekundær lokasjon hvis noe skulle gå ned, og sekundære transport veier, en del av det NSA har gjort er å lytte på informasjon som er på vei til Google sine store datasentre før Google har fått tak i det, Google visste det ikke, men NSA lyttet på fiberlinjene. Vi er midt inne i det med at veldig mye av vår internett trafikk går via Sverige, og Sverige bruker mye av den informasjonen som kommer fra Norge. Det trigges i alle skyløsninger med tanke på redundansen, skalerbarhet, elastisitet som skal bygge inne i dem. Det trengs å tenke utover geografien på en slik måte at en bruker det internasjonale nedslaget som internett representerer."* (Blindheim).

Videre kommer en av informantene med et eksempel fra Software Innovation "*Hva om det er sånn som for eksempel med eksempelet med Software Innovation, så tror jeg de tilbyr bruk av Microsoft sine datasentre, da er det Dublin, Irland, Amsterdam og Nederland. Og juridisk sett har vi fått på det rene at på et hvert sted i Europa og for så vidt også i USA med aktører som er en del av den såkalte safe Harbor avtalen , at det er juridisk lovlig å kjøpe tjenester. Også putte personlig helseopplysninger, altså sensitiv informasjon."* (Blindheim). Det er ulike aspekter som informantene mener bør være tilstede hvis informasjonen skal lagres i utlandet *" Det må være personvernlovgivning som passer overens, og det er en del andre mekanismer. Men det som også er tilfelle er risikobildet, og denne Snowden saken har jo brakt frem spionasje og det at noen stater tar seg til rette ovenfor firmaer som juridisk hører til dem, og kan ta som NSA har vist seg villig til å gå inn i andre lands informasjon og hente ut den på lovlig og ikke lovlig måte."* (Blindheim).

Informantene gir inntrykk av at det er viktig med kontroll og risikovurdering i helsesektoren *"Dette handler jo om kontroll og risiko, i veldig stor grad. For å samle trådene litt, datatilsynet sier i forbindelse med alle typer driftsløsninger som skal håndtere personvern sensitiv informasjon, at man må gjøre en konkret risikovurdering og det er det alt brenner ned til her. Når man gjør denne vurderingene kan man bruke den type løsninger. Så må man gjøre en konkret vurdering av risiko."* (Losnegaard).
Når det gjelder lagring av data, så mener informantene at det er lettere om dataene er stasjonert i Norge kontra utlandet. Informantene mener at det vil resultere i en mer positiv holdning, dersom dataene er lagret i Norge *"At dataene er lagret i Norge vil helt klart endret holdningen, fordi det tilpasser seg det lokale lovverket. Altså den store frykten er å få det ut av EU. Innenfor EU så har vi iallfall noen lover og regler å stille oss bak."* (Nystuen). Informanten legger til at den store frykten er at dataene skal lagres i USA. "*Men frykten er jo å få dette over til statene da."* (Nystuen).

Videre blir det nevnt problemer med utenlandske firmaer som er lokalisert i Norge, og om disse føler seg pliktig til å følge norsk lovgivning *"Det kan jo være det, det spørs i forhold til hvordan det firma er regulert til det lovverket som de da har i det landet som de faktisk har opphav i, eller om det da styres av norske lover og regler. Også er det å etablere avtaler på en ansvarlig måte som gjøre at de leverer den tjenesten, leverer i forhold til hva det er de faktisk har avtalt".* (Nystuen). Informanten påpeker at det hadde vært politisk lettere dersom dataene hadde vært lagret i Norge *"Dersom dataene hadde blitt lagret innenfor landets grenser så hadde det vært lettere. Det er det politiske aspektet egentlig, det er lettere for publikum å synes at det er trygt nok. Det juridiske er enklere, da er vi innenfor norsk jurisdiksjon, vi vet hvilken regler som gjelder. Et amerikansk firma, for enkelhetsskyld si at det er et heleid amerikansk underleverandør som ligger i Norge, så er de underlagt norsk lovgivning og sånt, men vi vet jo ikke i hvilken grad de føler seg forpliktet til av for eksempel amerikansk lovgivning. Eller tilsvarende hvis det er et hel eid kinesisk selskap i Norge. Da er de underlagt norsk lovgivning, de er registret som et norsk selskap, et norsk AS. Men hele er 100 % kinesisk heleid. Hvilke lojalitet vil de føle ovenfor det norske samfunnet?"* (Losnegaard).

Informantene er klare på at det ville vært enklere dersom man hadde plassert Cloud Computing dataene innenfor EU kontra USA *"Så lenge vi klarer å ha et avtale verk som tilsier at de da leverer og opererer etter det som vi da har som nasjonale føringer eller EU regulativ. Da tenker jeg; da er det jo greit."* (Nystuen). Videre sier en annen informant at det ikke er tilstrekkelig at dataene blir lagret innenfor EU *" Nei, det holder ikke at dataene blir lagret innenfor EU! Ikke i dag nei. Ikke sånn som regelverket er i dag"*. (Lund). Mye av grunnen til dette er personvernet *"Personvernet er sterkt altså, og alle sykehus har en personvernskonsulent eller rådgiver."* (Knutsen). Enkelte av informantene har ikke noen formening om hvor dataene lagres så lenge sikkerheten er ivaretatt, men at lagring i Norge er å foretrekke *"Jeg har ikke noen prinsipiell motforestilling mot å lagre informasjonen noen steder, bare sikkerheten er til stede. Grunnen til at jeg kanskje sier ja til å fortsatt ha det i Norge er at vi har en holdning til personvernet og en holdning som kanskje noen ganger er for streng."* (Knutsen). En annen informant påpeker at man må vite hvor dataene lagres og dette er et krav til aktørene *"Da må vi vite blant annet hvor dataene lagres, vi må vite eksplisitt, hvor geografisk det er . I en nettskyløsning så kan jo det i prinsippet være vanskelig å si, men det er et krav til aktørene. Det skal til en hver tid kunne peke på hvor dataene befinner seg."* (Blindheim).

Det er ifølge en av informantene et juridisk- og politisk aspekt hvis dataene skal lagres i utlandet. Videre drar han inn befolkningens syn på dette *"Da må jeg begynne med å si at en ting er det juridiske aspektet av dette, for så vidt det neste jeg hadde tenkt å si er at er det bare et juridisk spørsmål? Eller er det et politisk spørsmål? Ville Norges befolknings synes at det er greit at deres helseopplysninger, på tvers av hele landets befolkning lagres i utlandet. Dette er en av tingene vi diskuterer her, det er godt mulig hvis vi skulle laget en stor løsning hvor data ville bli oppbevart i utlandet så måtte det løftes til politisk nivå."* (Losnegaard). Det påpekes at det er positive og negative sider ved å lagre dataene i utlandet. *"At dataene blir lagret i utlandet tror jeg har to sider. På den ene siden så vil det jo kunne beskytte dataene bedre hvis du har spredt data på flere steder i utlandet. Da er det større sannsynlighet for at du ikke mister all dataene dersom noe skulle gå galt. På en annen side så man jo da ha gode garantier for sikkerheten de stedene hvor dataene er lagret, og ha gode innbruddsmekanismer, vite hvordan policyen i forhold til de medarbeiderne som tross alt må være der å jobbe med systemene. Men i prinsipp så har vi jo de samme*

problemene nå, jeg vet jo ikke hva medarbeiderne i sykehuspartner kan finne på." (Borthne).

Informantene mener den største utfordringen er lovverket *"I utgangspunktet har vi jo noen sterke føringer i personopplysningsloven med forskrift som setter krav til at vi skal ha kontroll på informasjonssikkerheten våres*". (Henriksen). Videre påpeker en annen informant at det er mange som bruker lovgivningen som en unnskyldning. *"Nei altså, det har jo vært vanlig å skylde på personvernet og personvernlovgivning i alle år, men jeg mener at det er feil, for jeg tror at det går an å få til moderne tjenester med en stram personvernlovgivning. Jeg tror ikke det er noe i motstrid, men det har vært vanlig å bruke den formen for, jeg vil kalle det, "unnskyldning" for å gå inn i fremtiden."* (Borthne).

Sikkerheten i nåværende systemer vs. Cloud Computing

Sikkerhet er et veldig omdiskutert tema i helsesektoren og et punkt som våre informanter diskuterte under intervjuene. I denne kategorien er vi ute etter å se hvilken holdning informantene har til deres nåværende systemer vs. Cloud Computing i helsesektoren *"Hvis du ser på journalsystemet våres så er dette veldig sikre, det vil si at noe står lokalt og noe står sentralt. Det er ingen deling mellom andre foretak. Det går noe XML meldinger til og fra legekontor. Vi har litt "second opinions" som går til andre sykehus men allikevel så er det veldig sterke skillemekanismer og forsendelsesmekanismer. Så slik det står i dag så vil nok det være en mye sikrere løsning."* (Henriksen).

Det er en del restriksjoner rundt tilgangen til sensitiv informasjon *"I tillegg så har vi jo krav til logging, da snakker jeg ikke om logging om hvem som har brukt systemet, for det er jo enkelt. Men krav til utlevere f.eks. logger til pasienter, hvem som har vært inne å sett på opplysninger. Da differensieres det så langt ned at vi er nødt til å logge hvert eneste journal notat. Så klart hvis en skytjeneste skal begynne å gjøre disse jobbene så blir det mye prosessering av data, det gjør det jo. Å i tillegg er det jo en integrasjon med andre kliniske fagsystemer som er på samme sikkerhetsnivå. Så slik skytjenesten er i dag så vil nok ikke Cloud Computing konkurrere ut den sikkerheten.*" (Henriksen).

En av informantene mener det ikke er noen vesentlig forskjell når det kommer til sikkerhet innenfor Cloud Computing sammenlignet med nåværende datasystemer *"Jeg ser ikke Cloud Computing som en kjempe utfordring, eller at det er mye mer usikkert enn det vi har av nåværende systemer. Men igjen da så er det at vi er opptatt av helsenett, norsk helsenett, og visst du baserer skytjenestene på det så tenker jeg det er helt problemfritt, da er det like sikkert."* (Nystuen). Men skepsisen til å lagre personopplysninger i skytjenester er tilstede *"Men det å bruke det frie og åpne internett til lagring av personopplysninger det er jeg fortsatt litt skeptisk til. Og det er en grunn til at det kan du si det norske personvernet kan være en nisje bransje for oss."* (Nystuen).

Det finnes andre sektorer som har tatt i bruk Cloud Computing løsninger og dette har vist at løsningene fungerer. Men informasjonen i privatsektor, er ikke like sensitivt som i helsesektoren *"Jeg tror jo at nå som vi ser at finans eller banksektoren kan bruke Cloud Computing og har løsninger, så begynner vi å nærme oss noe som vi kan bruke også. Den dagen du ser at forsvaret gjør, da er vi virkelig på vei, fordi de også operer på informasjon som er sensitiv."* (Lund). En annen informant mener at det er mye av de samme sikkerhetsproblemene som vil dukke opp i et Cloud Computing system *"Det blir mye av de samme sikkerhetsproblemene. For vår del så ser ikke jeg noen stor forskjell på det, hvis sikkerheten er i varetatt på dataene som vi og legene bruker, eller som blir produsert i medisin teknisk utstyr så er det greit. Men ettersom mer og mer blir automatisert og kommer inn i forskjellige databaser, og med ulik beliggenhet så må vi være sikker på at det er sikkert nok og ikke kommer på avvei."* (Knutsen).

Sikkerheten rundt systemene er av og til for strenge, mener enkelte informantene *"Noen ganger synes jeg det er for strengt. Fordi vi er veldig rolle basert, så en lege på kirurgen kan også se og få tak i deler av journalen og på en medisinsk en annen del. Eller hvis pasienten har vært inne på medisinsk eller psykologisk, men da må han bruke blå lys på hele tida å dokumentere hvorfor han har behov for å se deler av journalen. Sykepleieren har det ikke. Alle får ikke den totale oversikten. Og så er det utrolig strengt hvis man blir innlagt på et annet sykehus. Så det bør gå an å sende en forespørsel fra det ene sykehuset til det andre om å få ut informasjon om pasienten, og da går det på anonymisert faks eller papir i drosje eller ikke på mail i hvert fall.*

Hvert fall ikke på mail det er strengt forbudt, vi har strenge prosedyrer på." (Knutsen).

Det kommer også frem at det er store sikkerhetsmessige utfordringer i de eksisterende sykehussystemene *" Vi har helt klart store sikkerhetsutfordringer i dagens system, sett frem i mange perspektiver. Den største risikoen kommer antakeligvis internt i sykehusene, fordi medarbeideren ikke alltid følger reglene. Så det er kanskje det mest nærliggende av de største sikkerhetsrisikoene"* (Borthne). Det skjer en del glipp blant de ansatte som blir sett på som et sikkerhetsproblem. Det finnes ulike ordninger på sykehusene som skal ivareta sikkerheten *"Men så er det jo også sikkerhetsproblemer med at folk bruker gule lapper med passordene sine eller til å bruke for enkle passord eller låne vekk kortene sine. Vi har i å for seg gode ordninger på det her, for pålogging og dørløsning, du kan ikke bevege deg rundt i sykehuset dersom du ikke har kortet med deg."* (Borthne). Informanten tar opp et eksempel rundt sikkerheten i deres nåværende systemer *"Vi så jo for noen måneder siden en sak om at det var en ansatt i sykehuspartner som hadde brutt seg inn, for de har jo også med lønnsutbetalinger å gjøre, så hadde han overført penger fra sykehusansattes sine kontoer til seg selv. Det har jo stått i avisene og er offentligkjent. Så heller ikke med det systemet som man har i dag så kan man ha 100 % sikkerhet for utro medarbeidere, dårlig programvare systemer etc."* (Borthne). Men informanten påpeker at han antar at det er lik type risiko når det kommer til Cloud Computing sett i sammenheng med nåværende systemer *"Så er det jo selvfølgelig trusler uten ifra, innbrudd, hacking, ondsinnet programvare og alle disse tingene. Men prinsipielt så vil jeg jo anta at det er samme typen av risiko på Cloud Computing, som det vi allerede har i dag, hvor vi har store og omfattende systemer, vi har bare ikke tatt skrittet helt ut i skyen."* (Borthne)

Sikkerhetsmessige utfordringer

Det vil alltid være utfordringer rundt sikkerhet når det dreier seg om lagring av sensitiv informasjon innenfor ny teknologi.

Det kommer tydelig frem at informantene mener at sikkerhetsaspektet og personvernloven er det store hinderet *"Ja, sikkerhetsaspektet er den store barrieren.* (Henriksen). Dette bekreftes av flere av informantene.

”*Ja, personvernloven og informasjonssikkerhet er kjempeviktig. Cloud Computing handler jo i stor grad om å sprenge grenser, sprenge rammer for å bedre fleksibilitet. Så i forhold til dette med informasjonssikkerhet så er det definitivt en av de største utfordringene, en av tingene som går mest på tvers av Cloud Computing tankegangen.”*(Losnegaard).

”Du har personvernet, du har pasientsikkerhet, ehm ja jo. Vi er jo redd for selvfølgelig at pasientinformasjon skal komme på avveie. Så det er det vi er mest opptatt av, sikkerheten rundt dette, at det er helt 100 %.” (Knutsen).

”Og der er det jo innenfor Europa et personverndirektiv som legger listen omtrent på nivå med det norske. Det er et helt essensielt element i dette med personvern og sensitiv informasjon.” (Losnegaard).

Et annet tema som blir tatt opp er et skalering- og differensierings problem ”*Hvis vi skulle lagt pasientinformasjonen inn i en skytjeneste, så ville det dukket opp et problem, at de som behandler ulike saker får for mye informasjon rundt pasienten, sånn som det er i dag*.” (Henriksen). Det viser seg at man har ulike krav når man driver med personopplysninger *”I tillegg har vi jo krav til at så lenge en driver med personopplysninger generelt så har man plikt til å utlevere alt omkring hva det er brukt til , hvem som har sett det osv. , så man har dette sikkerhetsaspektet i tillegg som skal prosesseres.”* (Henriksen).

Det blir påpekt at DLP bør legges inn i Cloud Computing, fordi man da har bedre kontroll på hva som sendes ut i skyen *”Vi rett og slett på at vi ikke har kontroll på de opplysninger som blir sendt ut til skyen. Klart den dagen, som jeg har snakket med de andre som har tilsvarende rolle rundt omkring i helseforetakene. Den dagen vi får innført DLP så kan man være mer åpne for skyløsninger. For øyeblikket så sitter vi å blomster og venter på at DLP skal bli innført i norsk helsesektor. DLP gir tilgang til et verktøy som kan sees på som et sikkerhetssystem, som bidrar til å kartlegge omfanget av uønsket bruk. DLP logger hva som skjer, slik at man er i stand til å plukke opp eventuelle brudd på reglene.”* (Henriksen).

Det er flere store utfordringer ved implementering av Cloud Computing *"Hvis vi begynner med det enkle, altså løsninger som ikke medfører forvaltning av sensitiv personlig informasjon, altså sensitive opplysninger. All helseinformasjon regnes for å være noe av det aller mest sensitive personlige informasjonen vi har. Du kan ha løsninger som er enklere, som f.eks. navn, adresse etc. Det skal ikke så veldig mye til før man på en måte har med sensitiv informasjon å gjøre. Får man personlig informasjon inn i en løsning så er det allerede da det juridiske rammeverk som kryper inn som for eksempel personopplysningsloven og forskrifter*." (Losnegaard). Videre påpeker informanten at det er innholdet i skyen som er den stor utfordringen *"Den store utfordringen er det med innhold, det innholdet man legger i skyen, selv om det ikke er personliginformasjon så kan det være konkurransesensitivt informasjon, det kan enten være informasjon vi sitter med om markedet, om priser for eksempel, sånne type ting. Det kan også være informasjon som for vår egen del er informasjon vi kanskje ikke ønsker å skal bli spredt for vindene. Utfordringene der er jo det med innsyn i det, hvilke rammer settes for denne informasjonen, hvor trygge er vi på at denne informasjonen er tilstrekkelig beskyttet. Og forbeholder leverandørene seg retten til å kunne gjenbruke ting for eksempel*." (Losnegaard).

Som tidligere nevnt er det mye spekulasjoner rundt NSA og spionasje *"Det spekuleres i at amerikanske myndigheter, NSA, de har en eller annen bakdør til Microsoft som selskap. Vi vet ikke om de har det, Microsoft og alle disse aktørene bedyrer at de ikke gir ut informasjon automatisk, det må være eksplisitt."* (Blindheim). Dette understøtter informanten med et eksempel
"Microsoft er livredde for den manglende tilliten som denne type løsninger representerer etter Snowden avsløringene, men vi sier at det kan sikkert være riktig det. Men vi vet jo ikke, vi vet jo at NSA opererer med å sende brev til mennesker på lavt nivå i organisasjonen med trusler om straffeføringer hvis de sier noe til sjefene sine. Så sjefene vet ikke at noen går inn på vegne av amerikanske myndigheter og henter data, sånt har skjedd, i hvert fall ifølge Snowden avsløringene." (Blindheim).

Avslutningsvis påpeker en av informantene at det ikke skal være noe problem ved implementering av Cloud Computing, dersom sikkerhetsmekanismene er gode nok *"Det er jo ingenting i veien for at vi ikke kan benytte oss av Cloud Computing, men de Cloud Computing tjenesten måtte inkluderes i sikkerhetsmekanismer som vi dag*

ikke ser er tilstrekkelig gode nok. Bla. Sertifiseringsordninger, dette med at du skal kunne, du må være sikker på at stabiliteten i nettverk og løsninger er god nok." (Lund).

Brukervennlighet

Cloud Computing bidrar til bedre tilgjengelighet, fellessystemer, differensiering, bedre ytelse og effektivitet. Dette påpeker to av informantene *"Hmm, det ville nok blitt mye lettere, det ville det nok. Meeen kanskje litt for lett å, med betraktning av hva som skal være tilgjengelig og hva som ikke skal være tilgjengelig og hvordan vi skal differensiere det."* (Henriksen). *"Sånn som vi har forstått det så er det mulighet for å sortere data og legge det inn i sykehussystemene på en mer ryddig og brukervennlig måte"* (Nystuen).

Enkelte av informantene har ikke noe spesielt synspunkt på brukervennligheten når det kommer til Cloud Computing *"Det er vel også noe man ikke kan si på generell basis, Cloud Computing er jo programvare som på akkurat samme måte som programvare innomhus."* (Blindheim). Når det kommer til privatbruk så har enkelte av informantene et positivt syn på brukervennligheten *"Når jeg bruker Cloud Computing privat, så er jeg jo overveldet over effektivt det er og hvor enkelt det er å komme inn på den typen løsninger uavhengig av hva slags plattform man sitter på. Sitter man for eksempel i bilen eller på trikken så kan man komme inn i en Cloud Computing løsning og få de svarene, og du får de effektivt og greit."* (Borthne).

Brukerstøtte

Vi er ute etter å få vite informantenes holdning når det kommer til brukerstøtte i forhold til Cloud Computing. Informantene hadde varierte svar når det kom til dette punktet *"Jeg vet egentlig ikke hva jeg skal svare på det med brukerstøtte. Det er jo veldig avhengig av de leverandøravtalene du har knyttet til deg. Og hvis du tenker helt sånn kommersielle tjenester som ligger fritt der ute, så krever jo det en vis kunnskap om IT som ikke nødvendigvis alle ansatte har."* (Lund).

Cloud Computing ville nok redusert den daglige oppfølgningen men at man muligens måtte hatt noen IT ansatte tilstede hvis det skulle dukke opp komplikasjoner *"Sannsynligvis så ville det blitt mindre behov for daglig oppfølging, men allikevel så*

er det jo sånn at noen brukere er nye, noen er klønete, noen tukler det til og da trenger du noen type superbrukere, noen som har IKT bakgrunn og som forstår systemet og kan komme inn å bistå med daglige problemer" (Borthne).

Informanten påpeker at en fjern representasjon av IKT-medarbeidere ikke er godt nok, ettersom det er slik Sykehuspartner opererer i dag*"Det som jeg savner med i dagens ordning, hvor vi bare har fjern representasjon i sykehuspartner som skal være de som gir oss brukerstøtte. Så tenker jeg at det viktigste på et sykehus er å ha en lokal støtte med IKT medarbeidere som vet hva vi har av tjenester som kan strukturere arkitekturen og vet hva som kan gå galt og vet av erfaringsmessig hva som kan skje"* (Borthne). Informanten føler det er viktig med en lokal stasjonert tjenesteperson med IKT bakgrunn "*Og selv om vi går over til skytjenester så er det viktig å ha en lokal tjeneste med gode IKT folk som kan gå rundt akkurat som de gjorde i gamle dager."* (Borthne).

4.3.3 Atferd i forhold til Cloud Computing

Trekomponentmodellen til Rosenberg og Hovland tar for seg komponenten atferd. Dette er den komponenten det har vært forsket minst på, og Rosenberg og Hovland sier at atferd er minst brukt som hovedindeks for holdning. Dette steget i prosessen tar for seg reel atferd og intensjonen om handling. Vi har valgt å se på intensjon fordi det er mer reelt for oss i denne avhandlingen.

Videre arbeid.

Vi har nå tolket informantenes svar, både fra følelse- og kunnskapskomponenten. Vi får her et innblikk i hva de tenker og føler rundt konseptet Cloud Computing. Med dette så ønsker vi å se på informantenes intensjoner om å bruke Cloud Computing i nærmeste fremtid *"Per tidspunkt, nei, det har vi ikke. Det betyr allikevel ikke at vi ikke skal snakke om det i foretakene, for det er jo et høyt aktualisert tema, det er det jo. Så vet jeg f.eks. at en del offentlige anskaffelser har jo lyst til å ha noe i Cloud Computing tjenester, levering etc. Detaljer rundt dette kjenner jeg ikke til, for det er jo ikke jeg som styrer. Men forskning snuser jo sånn sett på Cloud Computing tjenester."* (Henriksen). Mens noen er helt klare på at det ikke kommer til å bli noe bruk av Cloud Computing i nærmeste fremtid *"Nei, ikke pr dags dato."* (Borthne)

Informantene påpeker at de ikke har til hensikt å bruke Cloud Computing i første omgang, men at det ikke er utelukket i fremtiden. Mens andre informanter er mer bevist og klare på hva de ønsker *" Svaret er vel ja. Altså, vi jobber jo nå sammen med sykehuspartner for å se på hvordan man kan bruke Asher løsningen til Microsoft. Vi tenker da innenfor forskningen og innovasjon. Oslo universitetssykehus er de som har det absolutt største behovet rundt forskningsparken. Da med tanke på all den forskningsdataene som de har, i forhold til både sikkerhet av bedriften, men også nettopp av den skalerbarheten og faktisk få søkbarheten og søkbarkraften."* (Nystuen).

Andre informanter er mer diffuse når det kommer til dette spørsmålet *"Nei, men det er ikke riktig å si at det ikke blir i nærmeste fremtid, for nå jobber vi blant annet med å se på norsk helsenett fra bunnen av, de leverer deler på noe av det vi gjør."*(Lund).

Men selv om de ulike informantene vi har intervjuet til nå har gitt oss veldig forskjellige svar, så påpeker denne informantene at det er opp til regionen å bestemme *"Nei hvis det kommer, så blir det fra regionen, slik situasjonen er nå ved at de styrer og det er de som har et sett av midler til IKT løsninger. Vi henger oss på en måte på og tar i bruk det vi får fra regionen."* (Knutsen).

4.4 Oppsummering etter analysen

Vi har nå gjennomgått og beskrevet de tre komponentene i Rosenberg og Hovlands modell. Dette innebærer at vi har beskrevet informantenes kunnskap, følelsesmessige holdninger og intensjoner. Neste del blir å drøfte og tolke informantenes holdninger blant de ulike kategoriene.

5. Drøfting

I det forrige kapittelet har vi tolket og beskrevet informasjonen vi fikk fra intervjuene med våre informanter. Vi vil nå drøfte informasjonen vi har fått, opp mot vår problemstilling. Vi har laget tre tabeller som oppsummerer informantenes svar innenfor hver komponent. Først vil vi drøfte kategorien *"forståelse"* som inngår i den kognitive delen av trekomponentmodellen, deretter vil vi ta for oss 11 kategorier som inngår i den affektive komponenten, mens vi til slutt avslutter med kategorien "*videre planer"* som inngår i atferdskomponenten.

5.1 Kunnskap angående Cloud Computing

Kognitive	**Funn**
Forståelse	Generell forståelse når det kommer til det funksjonelle og detaljene rundt konseptet. Begrenset forståelse på det tekniske aspektet.

Tabell 7: Funn innenfor den kognitive komponenten

Informantene sett under ett hadde en generell, men forskjelligartet forståelse av begrepet Cloud Computing. Vi spurte om informantenes definisjon av Cloud Computing for å kartlegge deres forståelse av begrepet. Det viste seg at informantene hadde en generell forståelse av konseptet, når det kom til det funksjonelle og detaljene rundt konseptet. Ettersom det teknologiske aspektet er relativt nytt, er det et lite omdiskutert tema i helsesektoren. Informantenes generelle forståelse innebærer at de har kjennskap til at det er skalerbart og at det er et lagringsområde som er lokalisert i skyen. Det var lite kunnskap rundt det tekniske aspektet, spesielt med tanke på de ulike typene av Cloud Computing og Cloud Computing-applikasjoner. Informantenes funksjonelle forståelse innebærer at de vet at de kan kjøpe tjenester, lagringskapasitet og applikasjoner i skyen. Ettersom teknologien ikke er anvendt innenfor sykehusene medfører dette usikkerhet, noe som igjen antyder at de ikke kan nok om konseptet. Vi

mener dette indikerer at ledelsen ved helsesektoren trenger en mer eksakt forståelse av konseptet.

Nå har vi beskrevet den kognitive komponenten i forhold til begrepet *"forståelse"*. Videre vil vi beskrive følelseskomponenten i forhold til de ulike kategoriene i tabellen under.

5.2 Følelser angående Cloud Computing i norske sykehus

Affekt	**Funn**	**Positiv/negativ innstilling**
Generell holdning	Holdningen til Cloud Computing på fritiden er greit, men det er stor skepsis til Cloud Computing i offentlig sektor.	I hovedsak negativ til bruk i offentlig sektor.
Kollegaers holdning	Holdningene er varierte.	Noen er positive, mens andre er negative.
Gevinster og risikomomenter	Knyttes opp mot informasjonssikkerhet og lovverk.	I hovedsak positiv til gevinstene, men påpeker det negative rundt risikomomentene.
Kostnadseffektivisering	Delte meninger. Flertallet mener det vil være kostnadseffektiviserende.	Positiv til effekt på kostnader.
Effektivisering	Effektivisering er avhengig av lovgivning og sikkerhet.	Heller mot negativ innstilling på bakgrunn av bekymringer for sikkerhet.

Utfordringer innenfor offentlig sektor	Kunnskap, forståelse, spionasje, norsk lovgivning og differensiering av informasjonstilgang.	Negativ innstilling pga. risikomomenter.
Beliggenhet og lovverk	Geografisk plassering, norsk lovverk, Safe Harbor-avtalen og DLP.	Negativ innstilling pga. informasjonssikkerhet og lovverk.
Sikkerhet i nåværende systemer vs. Cloud Computing	Delte meninger. Ingen vesentlig forskjellig, det er mye av de samme sikkerhetsproblemene.	Både positive og negative innstillinger.
Sikkerhetsmessige utfordringer	Personvernloven, spionasje, informasjonssikkerhet, skyens innhold, skalering og differensieringsproblem.	I hovedsak negativ.
Brukervennlighet	Delte meninger.	Både positive og negative innstillinger.
Brukerstøtte	Delte meninger.	Både positive og negative innstillinger.

Tabell 8: Funn innenfor den affektive komponenten

Generell holdning

Mye tyder på at informantene skiller mellom privat- og jobb-relatert Cloud Computing bruk. Cloud Computing til privat bruk er greit, mens Cloud Computing i offentlig sektor er noe som blir sett på med stor skepsis. Grunnen til dette er at sykehusene opererer med mye sensitiv informasjon. Når informantene snakker om sin holdning til Cloud Computing innenfor den norske helsesektoren, kommer det klart frem at de er positive og nysgjerrige på konseptet. De mener det er kostnadseffektivt, skalerbart og effektivt, samtidig som de er usikre på hvordan sikkerheten og Norges lovverk, vedrørende blant annet personvern, skal bli ivaretatt. Enkelte av informantene innrømmer at de ikke vet nok om konseptet. Dette kan tyde på at usikkerheten som er omtalt følges opp av kunnskapskomponenten, som igjen går på at

de ikke forstår konseptet godt nok. De hevder at de ikke kan nok om Cloud Computing, at konseptet ikke er sikkert nok og at lovverket forhindrer dem i å bruke en slik løsning.

Kollegaers holdning

Som man ser ut i fra informantenes svar, er kollegaers holdninger varierte. Dette varierer fra region til region, hvor vi igjen ser at enkelte er skeptiske, mens andre er nøytrale og har ikke diskutert temaet ennå. Noen vil ha konseptet, da de ser fleksibiliteten i skyen. Dette er noe som kan tyde på at de ansatte i helsesektoren ikke har tilstrekkelig kunnskap om konseptet. Et annet punkt som ble påpekt, er at konseptet ikke er modent. Informantene mener Cloud Computing ikke er utviklet nok, med tanke på sikkerhet som kreves i offentlig sektor.

Gevinster og risikomomenter

Informantenes svar indikerer at det finnes både positive og negative sider ved bruk av skytjenester. Gevinstene som blir påpekt er samhandling, effektivisering, informasjonsdeling, skalerbarhet, fleksibilitet og kostnadseffektivisering. En kombinasjon av tjenester og forretningsmodeller kan føre til en optimal kostnadseffektivisering, sammenlignet med nåværende datasystemer.

Gevinstene som blir påpekt er i tråd med tidligere litteratur på området. Informantene mener skalerbarhet er en stor fordel. Dette er i tråd med Marston et al. (2011) sitt utsagn om at skalerbarhet er en av de store fordelene ved å benytte seg av Cloud Computing. Risikomomentene som blir påpekt er at sensitiv pasientinformasjon kan komme på avveie, og at andre kan få tilgang til denne informasjonen. Dette er et problem som blir tatt opp av Zissis og Lekkas (2010) og Marston et al (2011) som er skeptiske til tap av den fysiske kontrollen og infrastrukturen. Dette begrunner de med at det kan bli et åpent vindu for uautoriserte brukere. Svarene viser oss at gevinstene og risikomomentene som informantene tar for seg, er knyttet opp mot informasjonssikkerhet og lovverket. Dette gjenspeiles i deres atferd i forhold til å beskytte sensitiv pasientinformasjon.

Ettersom dette er et relativt nytt konsept, blir det påpekt at det er sikkerheten og kunnskapen det egentlig dreier seg om. Informantenes tanker rundt gevinster gjenspeiler positive følelser, mens risikomomentene gjenspeiler negative følelser.

Kostnadseffektivisering

Informantenes uttalelser gir oss grunn til å tro at Cloud Computing vil være kostnadseffektiviserende for sykehusene, selv om to av informantene var usikre på dette. Enkelte informanter mener det vil bli besparelser i både tid og penger, samtidig som man kan styre systemets kapasitet etter behov. Dette er i tråd med Zissis og Lekkas (2010) sine uttalelser om at man bare betaler for den faktiske bruken, og at man kan variere ressursbruken ved behov. To av informantene mener det ikke er gitt at Cloud Computing representerer noe form for kostnadseffektivisering. Dette er i tråd med Armbrust et al. (2009) som mener at en må merke seg at noen Cloud Computing leverandører tar betalt for hvor mye data som blir overført mellom deres tjeneste. Dette kan fort bli en stor kostnadspost. Flertallet av informantene hadde en positiv følelse til kostnadseffektivisering ved bruk av Cloud Computing.

Cloud Computing bidrar til økt kapasitet, samtidig som sykehusene sparer både tid og penger. Tidsbesparelser er noe som vil være essensielt på et hvert sykehus. Vi ser at informantene er usikre, men har en positiv holdning når det kommer til kostnads-besparelser.

Effektivisering

Hovedproblemet ved effektivisering ved hjelp av Cloud Computing peker tilbake til tidligere nevnt problem, nemlig lovverk og sikkerhet. Det virker som informantene ser på denne problematikken som avgjørende for konseptet og en mulig effektivisering. Enkelte av informantene påpeker at det er store muligheter for effektivisering ved bruk av Cloud Computing, med tanke på oversikt og skalerbarhet. Denne teknologien er relativt ny, og for mange er ikke potensialet like synlig. Informantenes følelser heller mot en negativ innstilling fordi usikkerheten er knyttet til sikkerhet. Ser man bort fra lovverk og sikkerhet, har informantene en positiv følelse når det kommer til effektivisering av Cloud Computing.

Utfordringer innenfor offentlig sektor

Informantene mener den største utfordringen ved Cloud Computing er kunnskapen og forståelsen rundt konseptet, spesielt når det kommer til oppfatningen av sikre løsninger. Et annet viktig moment som blir tatt opp er spionasje. Myndighetene har sett hvordan NSA jobber, og dette har gitt et bilde av hvilke utfordringer personvernet står overfor. Sikkerhetskravene har økt betraktelig etter "Snowden avsløringene". En kritisk faktor vil være pasientsensitivinformasjon på avveie som kan bli gjenstand for misbruk eller tap. "Tilgangs styring" dukker også opp som et problem, med tanke på hvordan man skal få skilt hvem som får tilgang på hvilken informasjon. Informasjonen i helsesektoren er regulert av egne lover og dette byr på utfordringer, ettersom de opererer med store mengder sensitiv informasjon. Informantene har negative følelser pga. skepsisen til spionasje og strengt lovverk.

Beliggenhet og lovverk

Ettersom helsevesenet er regulert av egne lover og forskrifter, må all sensitiv informasjonen lagres i Norge. De har ikke lov til å lagre pasientinformasjon utenfor Norges grenser. Det forenkler situasjonen når opplysningene lagres i Norge, ettersom man slipper bekymringen for USA. Safe Harbor-avtalen var også et tema som ble tatt opp av flere av informantene. Dette er en særavtale mellom EU og USA som regulerer overføring av personopplysninger fra EU/EØS-land til USA. Informantene er skeptiske til lagring av sensitive opplysninger i utlandet. Dette begrunner de med "Snowden-effekten" og NSA sin iver etter å innhente informasjon fra andre land. Det er mange utenlandske foretak som er lokalisert i Norge, og informantene er usikre på hvor forpliktet disse føler seg til å følge norsk lovgivning, selv om de er underlagt denne.

Flere av informantene var enig i at det ville vært enklere om dataene hadde blitt lagret innenfor EU kontra USA, så lenge leverandøren leverer og opererer etter nasjonal lovgivning eller EU-regulativ. Enkelte av informantene påpeker at det ikke er sikkert nok at dataene er lagret innenfor EU, basert på hvordan regelverket er i dag. Pr dags dato er personvernet for strengt.

Det er ikke bare et juridisk aspekt, men også et politisk aspekt dersom dataene blir lagret i utlandet. Det politiske aspektet drar inn meningen til den norske befolkning i forhold til om de mener det er greit at deres helseopplysninger er lagret i utlandet. Det

er en klar enighet om at den største utfordringen er lovgivningen, da det er sterke føringer i personopplysningsloven som krever at det skal være kontroll på informasjonssikkerheten. Alle informantene mener det er lovverket som byr på problemer ved implementering av Cloud Computing i offentlig sektor. Dette med tanke på hvor dataene blir lagret, samtidig som sikkerhetsperspektivet er viktig. Informantene har en negativ følelse til å lagre dataene i utlandet, fordi sikkerheten er såpass variert fra land til land.

Sikkerhet i nåværende systemer vs. Cloud Computing

Sikkerheten til journalsystemene pr dags dato er veldig sikre og det er ingen deling mellom andre helseforetak. Hvis noe informasjon deles er det veldig sterke skillemekanismer og forsendelsesmekanismer. I det nåværende systemet er det en del restriksjoner omkring tilgangen til sensitiv informasjon. Helsepersonell er blant annet nødt til å loggføre hvert enkelt tilfelle av innsyn i pasientjournaler.

En av informantene påpeker at Cloud Computing ikke vil utkonkurrere det sikkerhetsnivået som de allerede har. Andre mener at det ikke er noen vesentlig forskjell når de sammenligner sikkerheten i nåværende system kontra sikkerheten innenfor Cloud Computing. Det er mye av de samme sikkerhetsproblemene som vil dukke opp. Truslene informantene nevner er alt ifra innbrudd og hacking til ondsinnet programvare. Informantene er skeptiske til sikkerheten rundt lagring av personopplysninger i skytjenester. Det blir påpekt ulike sikkerhetsproblem i nåværende systemer, og disse er interne. Det skjer ofte en del glipp blant de ansatte, alt fra å skrive passord på gule Post-it lapper som er synlige for alle, til å låne bort ID-kort. Informantene har en negativ følelse til sikkerheten når det kommer til Cloud Computing kontra deres nåværende systemer. Dette er fordi konseptet er såpass nytt og kunnskapen rundt det er lav.

Sikkerhetsmessige utfordringer

Det kommer tydelig frem at informantene mener sikkerhetsaspektet og personvernloven er det store hinderet. Personvernloven og informasjonssikkerhet er viktig, ettersom pasientinformasjon er sensitivt. Det er kritisk dersom dette kommer på avveie. En annen utfordring som blir påpekt er skalering- og differensierings problemet. Informantene mener at det kan være vanskelig å skille mellom hvem som

skal få tilgang til informasjonen, og hvor mye informasjon de faktisk trenger å få tilgang til.

Ved en implementering av Cloud Computing blir det påpekt at behandlingen av sensitiv informasjon er en av de store utfordringene. Frykten for spionasje blir igjen påpekt av informantene som en utfordring. Spesielt dette med "bakdører", at leverandørene har designet en innsynsmulighet i systemet. Avslutningsvis mener informantene at dersom sikkerhetsmekanismene er gode nok, vil det ikke være noe problem å benytte Cloud Computing. Informantene har en negativ følelse til sikkerheten rundt Cloud Computing, ettersom det er såpass mange hindringer: personvernloven, spionasje, informasjonssikkerhet etc.

Brukervennlighet

Det er delte meninger når det kommer til brukervennligheten på Cloud Computing i offentlig sektor. Enkelte av informantene har ingen spesielle synspunkter til dette, mens andre påpeker at systemene ville blitt mer ryddig og lettere å bruke. Grunnen til dette er nok at informantene i offentlig sektor ikke har fått satt seg inn i bruker-vennligheten. Cloud Computing i privat sektor har imidlertid vært effektivt og enkelt. Informantene har varierte følelser når det kommer til brukervennlighet av Cloud Computing.

Brukerstøtte

Det er delte meninger blant informantene når det kommer til brukerstøtte innenfor Cloud Computing. Mye av grunnen til dette kan komme av at konseptet er relativt nytt og kunnskapen er variert. Enkelte mener at man er veldig avhengig av leverandøravtalen som er inngått. Cloud Computing ville antageligvis redusert behovet for daglig oppfølgning i helsesektoren. Informantene har varierte følelser når det kommer til brukerstøtte av Cloud Computing.

Nå har vi beskrevet den affektive komponenten i forhold til de 11 begrepene. Videre vil vi beskrive den atferdsmessige komponenten i forhold til kategorien i tabell nr.9.

5.3 Atferd i forhold til Cloud Computing

Atferd	**Funn**
Videre arbeid	Delte meninger

Tabell 9 : Funn innenfor atferds komponenten

Ut i fra informantenes svar ser vi at det er delte meninger når det kommer til intensjon om bruk av Cloud Computing innenfor helsesektoren. Det blir påpekt at de ikke har til hensikt å bruke Cloud Computing pr dags dato, men det er ikke utelukket når det kommer til et fremtidsperspektiv. Alt i alt sier flertallet nei til bruk av Cloud Computing i nærmeste fremtid. Dette fordi det er mye usikkerhet rundt sikkerhet, lovverk og plassering. En av informantene påpekte under kategorien *"Sikkerhet i nåværende systemer vs. Cloud Computing"* at den dagen forsvaret tar i bruk Cloud Computing-løsninger vil det ikke være noe i veien for at sykehusene kan begynne å bruke det. Dette begrunner informanten med at forsvaret også håndterer store mengder sensitiv informasjon. Selv om de sier dette så indikerer de at Cloud Computing er den rette veien å gå i fremtiden.

Informantene påpeker at det ikke er opp til hvert enkelt helseforetak å ta i bruk en Cloud Computing-løsning, det må komme fra regionen, ettersom det er regionen som bestemmer. Før regionen vil vurdere dette må Cloud Computing-tjenesten tilfredsstille sikkerhetskravene, norsk lovgivning, kravene rundt beliggenhet og kontroll.

Dette viser oss at informantene ikke har tydelige intensjoner om å ta i bruk konseptet Cloud Computing i sin sektor. Bakgrunnen for dette er i hovedsak de følelsene de har etablert i relasjon til Cloud Computing. Som vi så av følelseskategoriene var det stor usikkerhet rundt konseptet. Dette kommer av at den kognitive komponenten viser at informantene kun har en grunnleggende forståelse av konseptet.

6. Implikasjoner og videre forskning

Nå har vi kommet til det punktet i avhandlingen, hvor vi skal vurdere studiens bidrag opp mot vår problemstilling. Vi vil presentere de teoretiske og praktiske implikasjonene av vår forskning, for så å komme med forslag til videre forskning.

6.1 Studiens bidrag

Etter å ha arbeidet med temaet i en liten periode fant vi ut at det har blitt gjort få empiriske studier på området. Dette har vi sett på som både positivt og negativt i forhold til vårt arbeid. Det positive aspektet med dette er at vi har hatt muligheten til å gå inn med et åpent sinn, samtidig som vi har prøvd å ikke være forutinntatt.
Når det kommer til det negative er det vanskelig å finne andre kvalitative undersøkelser som tar utgangspunkt i trekomponentmodellen. Dette gjelder ikke på generell basis, fordi det finnes en del studier av mer positivistisk natur. Det er imidlertid som nevnt vanskelig når vi snakker om kvalitative undersøkelser. Dette er vanskelig når vi snakker om et så spesifikt tema som ekspansjonsstrategi og Cloud Computing.

Før vi kunne fortelle hva slags holdninger ledelsen i helsesektoren har til konseptet Cloud Computing, var vi avhengig av å avdekke komponentene forståelse, følelser og atferd rundt konseptet. I denne sammenhengen avdekket vi hvordan disse tre komponentene påvirker begrepet holdning. Vi fant ut at tematikken er kompleks og Cloud Computing er et relativt nytt konsept. Det har også vært lite forsket på området holdning og sikkerhet. I drøftingskapittelet har vi funnet en rekke faktorer som påvirker ledelsen i helsesektorens holdning til Cloud Computing. Nettopp derfor har vi lagt stor vekt på trekomponentmodellen som tar for seg begrepet holdning i tre steg. Interessante funn utover det vi har belyst i vårt teorikapittel er beliggenhet, lovverk, forståelse og fremtidig bruk. Disse fire faktorene representerer det man kan betegne som oppdukkende faktorer.

6.1.1 Teoretiske implikasjoner

Vi skriver om et IT-konsept med en strategisk vinkling, derfor har vi vært avhengig av å hente teori fra ulike fagfelt. Videre har vi kombinert holdningsteori, ekspansjons-strategi, teori om sikkerhet og Cloud Computing for å belyse vår problemstilling.

Det fenomenet vi studerer, bl.a. bestående av en leverandør av Cloud Computing og potensielle kunder i helsesektoren, representerer en kompleks og sammensatt virkelighet. I den forbindelse har vi valgt å bruke teori om holdning med utgangspunkt i trekomponentmodellen, kombinert med teori om ekspansjonsstrategi og Cloud Computing. Ettersom det har vært gjort lite forskning på Cloud Computing innenfor helsesektoren, har vi nå bidratt til å ta noen av de første stegene innenfor dette området.

6.1.2 Praktiske implikasjoner

Den praktiske relevansen av vår studie er at ledelsen i helsesektoren bør få et bedre innblikk og forståelse av konseptet Cloud Computing. For at en ekspansjon fra det private markedet og over til det offentlige skal være realistisk, må forståelsen av konseptet være tilstede. For å bedre forståelsen av Cloud Computing blant ledere i helsesektoren kan det være hensiktsmessig at leverandøren inviterer inn til en dag med foredrag. Det kunne f.eks. blitt gjort ved å invitere til et heldagsseminar med en blanding av eksterne og interne foredragsholdere. Dette kunne gitt deltagerne et detaljert innblikk i hva konseptet innebærer og hva det kan bidra med. Fordi konseptet er relativt nytt mener vi at ledelsen i helsesektoren bør få en mer eksakt forståelse av konseptet, dersom det skulle være relevant å ta dette i bruk.

Hvis det skal være relevant for helsesektoren å ta i bruk Cloud Computing, må det en holdningsendring til. Dette i forbindelse med at ledelsen i helsesektoren må ha et erfaringsgrunnlag og en referanseramme for å sin øke kunnskap og erfaring med den måten å jobbe på. Ved at helsesektoren får en bedre forståelse og økt kunnskap-/erfaring rundt det teknologiske konseptet, vil dette medføre en holdningsendring. Holdningsendring kan skje via samtale, samarbeid og veiledning, som bidrar til kunnskap og ferdigheter innenfor området.

I forhold til hvilken forståelse informantene har til Cloud Computing, er det interessant å se hvordan de ulike lederne i norsk helsesektor diskuterer konseptet, og hva de påpeker som er viktig for et slikt konsept. Dersom Cloud Computing skal inn i sykehusene, må sikkerheten dokumenteres, lovverket må være fulgt og plasseringen må være innenfor lovverket. En ”Safe Harbor-avtale” må være tilstede hvis opplysningene skal bli lagret i utlandet. Sykehusene er også avhengig av DLP dersom

de skal ha en nasjonal Cloud Computing-tjeneste. Vår informant, Henriksen, påpeker at DLP bør legges inn i Cloud Computing-tjenesten, fordi man da har bedre kontroll på hva som sendes ut i skyen. Den dagen DLP blir innført i skyløsninger, så vil helseforetakene være mer åpne for Cloud Computing. DLP er viktig, fordi dette er et verktøy som blir sett på som et sikkerhetssystem. Det bidrar til å kartlegge omfanget av uønsket bruk, DLP logger hva som skjer, slik at man er i stand til å plukke opp eventuelle brudd på reglene. Andre aspekter som informantene mener bør være tilstede hvis informasjonen skal lagres i utlandet, er at personvernlovgivningen må tilpasses. I tillegg må man vite eksplisitt hvor dataene er geografisk lagret. Dette er et krav til aktørene, de skal til enhver tid vite hvor dataene befinner seg.

Det blir presisert at ved bruk av Cloud Computing bør det være en IKT-medarbeider på huset, noe det ikke er i dag. Det blir påpekt at en fjern representasjon av IKT-funksjonen ikke er god nok, slik det for eksempel fungerer med Sykehuspartner i dag. Dersom helseforetakene skal ta i bruk Cloud Computing må dette komme fra regionen, ettersom det er regionene som bestemmer. Hvis en aktør vurderer en markedsekspansjon fra privat til offentlig sektor, må leverandøren oppfylle ulike krav i forhold til helsesektoren før en vurdering om bruk av produktet vil bli tatt opp.

Ettersom det eksisterer tre ulike typer av Cloud Computing, mener vi at en leverandør først bør fokusere på å presentere en Privat Cloud. Dette begrunner vi med at skyens infrastruktur drives utelukkende for en organisasjon. Privat Cloud kan bli administrert av organisasjonen eller en innledende tredjepart, noe som gir mer sikkerhet. En Privat Cloud vil ivareta sikkerheten knyttet til sensitive data. Cloud-infrastrukturen kan da stå i sykehusets datasenter, eller andre datasentre som oppfyller sykehusenes krav til sikkerhet. En Privat Cloud-infrastruktur bør kunne leveres som en ”pay-as-you-go” tjeneste, slik at man oppnår de samme økonomiske fordelene som ved f.eks. Public Cloud, altså rask skalering av kapasitet (både opp og ned) og betaling etter forbruk.

Sykehusene bør også kunne benytte både Hybrid og Public Cloud-tjenester der kravet til sikkerhet og personvern er mindre relevant. Det kan f.eks. være utviklings- og testmiljøer. Public og Hybrid Cloud-løsninger er rimeligere og vil sikre at man ikke betaler mer enn strengt tatt nødvendig. En leverandør bør anbefale helsesektoren å ha en privat Cloud, men kun der det er strenge krav til sikkerhet. En leverandør kan

eventuelt anbefale en Public og Hybrid Cloud der dette er tilstrekkelig. Det er ingen poeng å betale for Rolls Royce, hvis en Lada gjør samme nytten.

Valg av inngangsstrategi er en viktig del av en utviklingsstrategi. Det er nemlig ikke bare viktig å være opptatt av det nye markedet man skal inn i, men også hvordan man velger å entre dem (Lee & Lieberman, 2010). Videre bør leverandøren informere helsesektoren om de ulike teknologiske løsningene, dette for å bidra til en maksimal effektivisering. Det ville også vært hensiktsmessig av leverandøren å introdusere tjenesten "Infrastructure as a service". Dette er en tjeneste som innebærer outsourcing av utstyr som brukes til å støtte operasjoner, inkludert lagring, maskin-vare, servere og nettverkskomponenter (Techtarget, 2011). Dette er noe som kunne hjulpet helsesektoren med å samle sine infrastrukturer, samtidig som det ville bidratt til å samle deres servere.

En annen viktig løsning som ville fungert bra i helsesektoren er "Software as a service". Dette er en tjeneste der programmene er arrangert av en leverandør eller tjenesteleverandør og gjort tilgjengelig for kunder over et nettverk (Techtarget, 2011). Dette kunne bidratt til automatisk oppdatering av sykehusenes systemer osv. Dette hadde også bidratt til at helsesektoren i mindre grad hadde hatt behov for å drive med IT, noe som gir dem muligheten til å fokusere mer på kjernevirksomheten som er helse. En annen tjeneste som også er relevant er "Platform as a Service". Dette innebærer en tjeneste som er et paradigme for å levere operativsystemer og tilhørende tjenester over internett uten nedlastning, eller installasjon (Techtarget, 2011). Det vil med andre ord si at det er leverandøren som fortløpende oppdaterer sykehusenes operativsystemer så fort det dukker opp en nyere versjon av systemet.

6.2 Videre forskning

Det kan være flere emner som kan være interessant for videre forskning. Vi mener det kan være interessant å gjennomføre en studie på ledelsens holdninger til en fullt implementert Cloud Computing-løsning. Det kunne vært spennende å sammenligne holdningene før og etter implementeringen var gjennomført. Dette med bakgrunn i at alle informantene er positive og nysgjerrige til konseptet, men ettersom konseptet er relativt nytt bidrar dette til en rekke utfordringer.

Et annet interessant tema kunne vært å sett på holdningene til Norges befolkning hvis de fikk valget mellom å ha sensitive personopplysninger lagret i Norge, andre EU-land eller USA. Et annet forskningstema kunne vært å fokusert på ressursbasert teori, og se hvilke ressurser helsesektoren får, eller taper ved overgang til en skyløsning. Dette kan man se opp mot konkurransefortrinn. Det kunne vært interessant og forsket på de faktiske kostnadene ved å overføre eksisterende applikasjoner til Cloud Computing, for å se om det faktisk er lønnsomt å overføre eksisterende applikasjoner til skyen.

I dette kapittelet har vi forsøkt å definere vårt bidrag til forskning gjennom vår avhandling. Vi har også kommet med forslag til videre forskning. Ut i fra vårt perspektiv vil vi i neste kapittel kommentere studiens styrker og svakheter.

7. Styrker og svakheter ved vår studie

I starten av vår studie var det vanskelig å kartlegge tidligere forskning som hadde gått i detalj på akkurat det temaet vi ønsket å belyse, men vi mener likevel at vi har funnet relevant teori. Vi forstår at vi ikke har nådd et fullstendig metningspunkt når det kommer til datainnsamlingen, men vi vil ta opp forskjellen mellom en begrensning og en svakhet. Tematikken rundt konseptet er kompleks, noe som har gjort det krevende å skaffe informanter. Vi mener det er en nødvendig begrensning i vår studie at vi kun har sju informanter. Våre nøkkelinformanter har vært svært informative, og vi har vært heldige som har kommet i kontakt med disse. Dette er en masteroppgave der vi har begrenset med tid og ressurser, derfor mener vi at det ikke var nødvendig med flere informanter hvis vi skulle rekke å fullføre innenfor angitt tid. Informasjonen og argumentene vi fikk under intervjuene var relativt like og vi følte at vi ikke ville få noe mer informasjon med et større antall informanter. Begrensningen er derfor ikke en svakhet i vår studie

En utfordring for oss i denne avhandlingen har vært å begrense tematikken, siden det har vært relativt stort. Vi valgte å ikke ta med for mange aspekter når vi skulle utvikle intervjuguiden. Det kan godt hende det var andre kategorier vi også burde hatt med, men etter samtaler med CSC og veileder ble disse kategoriene valgt.

Vi vil påpeke at en styrke ved vår studie er at vi har vært helt ærlige når det kommer til opplysningene informantene har gitt oss. Alt vi har skrevet, er det som har blitt fortalt av informantene. I den forbindelse sendte vi transkriberingene til informantene, slik at de kunne bekrefte at vi ikke hadde misforstått noe i transkriberingsprosessen. Videre følte vi også at informantene var ærlige mot oss når det kommer til svarene de ga.

Vår studie er gjort med en kvalitativ forskningsstrategi, og dette er noe vi føler er en styrke for vår studie. Marshall & Rossmann (1999:43) har et sitat som vi følte passet her *"Although no qualitative studies are generalizable in the statistical sense, their findings may be transferable"*. Vi har fra starten av vært interessert i å få en dybdeforståelse for ledelsens holdning til Cloud Computing i helsesektoren og vi har

ikke vært ute etter å generalisere. Hvis dette hadde vært målet, måtte vi ha gjennomført en kvantitativ forskning og hatt vesentlig større antall respondenter.

En eventuell svakhet når det kommer til ekspansjon er at CSC er et amerikansk-eid selskap. Dette er noe som kan bidra til å svekke tiltroen til selskapet i form av spionasje. Et annet punkt som ble påpekt er hvor forpliktet utenlandske selskaper føler seg til å følge norsk lovgivning. Vi føler at de utfordringene vi har møtt er en styrke i denne oppgaven. Spanos og Lioukas (2001) påpeker at et foretaks ekspansjonsstrategi bør være bygget på de unike ressursene selskapet har. Vi mener at CSC har de ressursene som trengs for å imøtekomme en stor del av de utfordringene som har blitt påpekt rundt det tekniske aspektet.

Nå som vi har kommet til slutten av denne oppgaven, føler vi at vi har nådd målet vårt. Avhandlingen er gjennomført og vi har opparbeidet oss stor forståelse for Cloud Computing i helsesektoren.

8. Referanser

8.1 Artikler

Adams, A., Sasse, M.A., (1999) "Users are not the enemy", Communications of the ACM, December, Vol.42, No 12

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R. H., Konwinski, A., Lee, G., Patterson, A. D., Rabkin, A., Stoica, Ion. Zaharia, M., (2009). "Above the Cloud Computings: A berkeley view of Cloud Computing", *Science. Technical Report* No. UCB/EECS-28

Baldwin J. R & Yan. B., (2012). "Market Expansion and Productivity Growth: Do New Domestic Markets Matter as Much as New International Markets?" *The Economic Analysis Research Paper*

Bang VV, Joshi SL., (2008). Conceptualization of Market Expansion Strategies in Developing Economies. Academy of Marketing Science Review. Voumle 12 no.4

Barney J. (1991). Firm resources and sustained competitive advantage. *Journal of Management* **17**: 99–120.

Bhattacherjee, A., Prekumar,G., (2004). "Understanding Changes in Belief and Attitude toward Information Technology Usage: a Theoretical Model and Longitudinal Test", MIS Quarterly Vol.28 No 2, pp 229-254.

Bohner, G., Wänke, M., (2002). "Attitudes and Attitude Change", *Psychology Press.*

Braz, C., Robert, J-M., (2006) "Security and usability: The Case if the User Authentication Methods", ACM Press.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I., (2009). "Cloud Computing Computing and emerging IT platforms: Vision, hype, and reality for delivering Computing as the 5th utility‖". *Future Generation Computer Systems*, *25*(6), 599-616. Elsevier B.V. doi:10.1016/j.future.2008.12.001

Campbell, D.T., (1955). The Informant in Quantitative Research, American Journal of Sociology, 60, 339-342.

Cartwright, D., (1949). “Some principles of mass persuasion”. Human Relat., 2, 253-67. 6, 16f.,51.

Cheng, T.C.E., Lan,D.Y.C., Yeung,A.C.L., (2006). “Adoption of Internet Banking: An Empirical study in Hong Kong”, Elsevier.

Davis, Fred D. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly* 13(3), 319-340.

Dourish, P., Grinter, R.E, Delgado de la Flor, J., Joseph., (2004). ”Security in the wild: user strategies for managing security as an everyday, practical problem”, *Springer-Verlag London Limted.*

Durkee, Dave. (2010). ―Why cloud computing Will never Be free‖. Communication of the ACM. doi:10.1145/1735223.1735242

Dyer,W.,G.,Jr., Wilkins, A.,L., (1991). “Better stories, not better constructs, to generate better theory: a rejoinder to Eisenhardt”, Academy of Management Review, pp 613-619.

Eagly, Alice H. & Shelly Chaiken., (1993). *The psychology of attitudes*. Fort Worth, Texas:Harcourt Brace Jovanovich.

Eisenhardt, K., (1989). “Building Theories from case study Research”, Academy of Management Review, Vol 14, No 4, pp 532-550.

Gephart, R., (1999). “Paradigms and Research Metods”, Research Methods Forum Vol.4.

Glassberg, B.C, Grover, V., Teng, J.T.C., (2006). ”Information Systems Research with an Attitude”, The DATA BASE for Advances in Information Systems (Vol.37, Nos 2 & 3)

Green, B.F., (1954). Attitude measurement. In Handbook of social psychology, Vol.1, ed. G. Lindzey. Cambrigde Mass., Addison-Wesley, 335-69. 5

Harding, J., Kutner, B., Proshansky, H., og Chein,. I, (1954). Prejudice and ethnic relations. In Handbook of social psycology, Vol. 2, ed. G.Lindzey. Cambridge, Mass., Addison-Wesley, 1021-61. 4f., 23.

Hartley, E., (1946). “Problems in prejudice.” Oxford, England:Kings Crown Press

Henderson. R & Mitchell.W., (1997). The Interactions of Organizational and Competitive Influences on Strategy and Performance. *Strategic Management Journal*, Vol.**18** (Summer Special Issue), 5-14.

Hill, Charles W.L og Jones, Gareth R., (2004). Strategic Management Theory – An integrated approarch. Houghton Mifflin Company, Boston.

Hovland, C.I., (1954). Effects of the mass media of comunication. In handbook of social psychology, Vol.2, ed. G Lindzey. Cambridge, Mass., Addison-Wesley, 1062-103. 5, 23.

Jeyaraj, A., Rottman, J.W., Lacity, M.C., (2006). “A review of the predictors, linkages and biases in IT innovation adoption research”, Journal of Information Technology

John, G. og T. Reve., (1982). The Reliability and Validity of Key Informant Data from Dyadic Relationships in Marketing Channels, Journal of Marketing Research, Nov (19), 517-524.

Johnson, A.M., (2005). " The Technology Acceptance Model and the Decision to Invest in Information Security", *Proceedings of the 2005 Southern Association of Information Systems Conference.*

Kahle, Lynn. (1984). "*Attitudes and social adaptation. A person-situation interaction" approach*. University of Oregon, USA: Pergamon Press.

Katz, Daniel. (1960). "The Functional Approach to the Study of Attitudes". I: *The Public Opinion Quarterly*. (vol. XXIV) 2, s. 163-204.

Katz, D og Braly, K., (1933). "Racial stereotypes of one-hundred college students". K. Abnorm Soc.Psychol., 28, 280-90. 4

Ketokivi, M., R. G. Schroeder., (2004) "Perceptual measures of performance: fact or fiction?", Journal of Operations Management, 22, 247-264.

Klein, H.J., Myers, M.D., (1999). " A set of principles for conducting and evaluating interpretive field studies in Information systems" , MIS Quarterly Vol 23 No, March, pp. 67-94.

Knapp, K.J., Marshall, T.E., Rainer, R.K, and Ford, F.N., (2005). "Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness" (ISC)2 inc., Palm Harbor, Florida, and Auburn University, Auburn , Alabama, October 25.

Kotulic A.G., Clark, J.G., (2004). "Why there aren`t more information security research studies." Information & Management, 41,5, May. 2004, pp. 597-607.

Kowalski, S., Goldstein,M., (2006). "Consumer`s awareness of Attitudes Towards and Adoption of Mobil Phone Security", http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.2865&rep=rep1&type=pdf

Kramer, B.M., (1949). Dimensions of prejudice. J.Psychol., 27, 389-451. 5

Krech, D. og Crutchfield, R., (1948). Theory and problems of social psychology. New York, McGraw-Hill. 5, 15f.,223.

LaPiere, R.T., (1934). Attitudes versus actions. Sc. Forc., 13, 230-7.6

Lee, G. K., & Lieberman, M.B., (2010). Acquisition vs. Internal Development as modes of market entry. *Strategic Management Journal*, **31**:140-158

Leonard-Barton D. (1995). Wellsprings of Knowledge. Harvard Business School Press:Cambridge, MA.

Mahoney JT, Pandian JR. (1992). The resource-based view within the conversation of strategic management. *Strategic Management Journal* **13**(5): 363–380.

Malhotra, Y., Galetta, D.F. (1991), "Extending the Technology Acceptance Model to Account for Social Influence: Theoretical Bases and Empirical Validation", Proceeding of the 32nd Hawaii Internatioal Conference on System Sciences.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A., (2011). ―Cloud Computing — The business perspective‖. *Decision Support Systems*, *51*(1), 176 - 189. Elsevier B.V. doi:10.1016/j.dss.2010.12.006

Mell, Peter and Grance, Tim., (2009) The NIST Definition of Cloud Computing. National Institute of Standards and Technology, Information Technology Laboratory, version 15. Available at: http://www.nist.gov/itl/Cloud Computing/upload/Cloud Computing-def-v15.pdf (Acc. 2011-9- 15)

Mishina Y, Pollock TG, Porac JF., (2004). Are more resources always better for growth? Resource stickiness in market and product expansion. Strategic Management Journal **25**. 1179-1197

Nelson RR, Winter SG. (1982). An Evolutionary Theory of Economic Change. Belknap Press: Cambridge, MA.

Newbert SL. (2007). Empirical research on the resource-based views of the firm: An assessment and suggestion for future research. *Strategic Management Journal,* **28:** 121-146.

Otey, M. (2008). ―Cloud Computing. *Communication of the ACM*, 69-73. Retrieved from'http://public.management.uottawa.ca/~benyoucef/public/MBA5670/3.Articles/Article 1/Article 1.pdf

Paquette, S., Jaeger, P. T., & Wilson, S. C., (2010). "Identifying the security risks associated with governmental use of Cloud Computing". *Government Information Quarterly*, *27*(3), 245-253. ElsevierInc.doi:10.1016/j.giq.2010.01.002

Pavlou, P.A., Fygenson, M., (2006). "Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior". MIS Quarterly Vol. 30 No 1, March. pp 115-143.

Penrose, E. (1959). *The Theory of the Growth of the Firm*. Oxford University Press: Oxford.

Peteraf, MA.(1993). The cornerstones of competitive advantage: a resource-based view. *Strategic Management Journal* **14**(3): 179–191.

Petty, R.E., Wegener, D.T., (1998). "Attitude change: multiple roles for persuasion variables". In: D.T.Gilbert, S.T.Fiske and G.Lindzey, Editors, " The Handbook of Social Psychology", McGraw-Hill, New York.

Phillips, L. W., (1980) The Study of Collective Behavior in Marketing: Methodological Issues in the Use of Key Informants, unpublished Ph.d. dissertation, Northwestern University.

Phillips, L. W., (1981) Assessing Measurement Error in Key Informant Reports: A Methodological Note on Organizational analysis in Marketing, Journal of Marketing Research, 18 (November) 395- 415.

Plouffe, C.R., Hulland, J.S., Vandenbosch, M., (2001). "Parsimony in Modeling Technology Adaption Decisions – Understanding Merchant Adoption of a Smart Card-Based Payment System". Information System Research, Vol 12, No 2, pp 208-222.

Raymond, L. Rivard,S. And Verreault,D., (2006). Resource-based view and competitive strategy: An integrated model of the contribution of information technology to firm performance.*The journal of Strategic Information Systems, Volume 15, Issue 1.*

Rogerson, S., (2002)."IS Security needs ethics", IMIS Journal, Vol.12 No 4, August.

Saunders, M., Lewis, P & Thornhill, A., (2007). Research Methods for Business Students. (4.Utg) Essex: Prentice Hall.

Schanck, R.L., (1932). A study of community and its groups and institutions conceived of as behavior of individuals. Psychol. Monogr., 43, No.2 (Whole No. 195). 6

Scholl, R.W., (2002). "Attitudes and Attitude Change" University of Rhode Island http://www.uri.edu/research/lrc/scholl/webnotes/Dispositions_Attitudes.htm Hentet ut 04.12.13)

Schultz, E., (2005). "The Human Factor in Security", Computers and Security, 24/2005, pp 425-426.

Seidler, J., (1974) On Using Informants: A Technique for Collecting Quantitative Data and Controlling for Measurement Error in Organization Analysis, American Sociological Review, 39 (Desember), 816-831.

Sinclare, Jollean K.,(2005) "Current research in Information Security and Privacy", Unpublished paper, http://sais.aisnet.org/SAIS2005/Sinclaire.pdf (accessed 20.01.2014)

Spanos YE, Lioukas, S., (2001). An examination into the casual logic of rent generation: Contrasting Porter`s competitive strategy framework and the resource-based perspective. Strategic Management Journal, **22**:907-934.

Steele, S., Wargo, C., (2007). "An Introduction to Insider Threat management" Information Systems Security, pp 16:23.

Straub, D.W and Welke, R.J., (1998). "Coping with system risk: Security Planning Models for Management Decision-Making, *MIS Quarterly (22:4, December), pp 441-469*

Sultan, N., (2010). "Cloud Computing for education: A new dawn?" . *International Journal of Information Management*, *30*(2), 109-116. doi:10.1016/j.ijinfomgt.2009.09.004

Svantesson, D., & Clarke, R., (2010). ―Privacy and consumer risks in Cloud Computing. *Computer Law & Security Review*, *26*(4), 391-397. Elsevier Ltd.doi:10.1016/j.clsr.2010.05.005

Taylor, S., Todd, P.A., (1995). "Understanding Information Technology Usage: A Test of Competing Models", Information Systems Research, June, pp: 144-176

Wald, Hannah., (2010) "Cloud Computing for the Federal Community." IAnewsletter, 13 (2), 10-15. Available at: http://iac.dtic.mil/iatac (Acc. 2011-9-15)

Wang, Lizhe, Laszewski, Gregor Von, Younge, Andrew,He, Xi, Kunze, Marcel, Tao, Jie and Fu, Cheng.,(2010) "Cloud Computing: a Perspective Study." New Generation Computing, 28 (2), 137-146. Doi: 10.1007/s00354-008-0081-5

Winter SG, Szulanski G., (2002). "Replication of organizational routines: conceptualizing the exploitation of knowledge assets." In the Strategic Management of Intellectual Capital and Organizational Knowledge: A Collection of Readings, Bontis N, Choo CW (eds). Oxford Univerity Press: NewYork: 207-222.

Wixom, B.H., Todd, P.A., (2005). “A Theoretical Integration of User Satisfaction and Technology Acceptance”. Information Systems Research, Vol.16, No 1, March, pp-85-102

Zheng, X., & Cai, Y. (2011). ―Energy-aware load dispatching in geographically located Internet data centers‖. Sustainable Computing: Informatics and Systems, 1(4), 275-285. Elsevier Inc. doi:10.1016/j.suscom.2011.06.002

Zhu, R., Sun, Z., & Hu, J. (2012). ―Special section: Green computing‖. Future Generation Computer Systems, 28(2), 368-370. doi:10.1016/j.future.2011.06.011

Zissis, D., & Lekkas, D., (2010). ―Addressing Cloud Computing security issues‖. *Future Generation Computer Systems*. Elsevier B.V.doi:10.1016/j.future.2010.12.006

8.2 Bøker

Ajzen, I., (1988). “Attitudes, Personality and Behavior”, Dorsey Press.

Ajzen, I., Fishbein,M., (1980). “Understanding Attitudes and Predicting Social Behavior”, Prentice Hall.

Blindheim, T., Sætrang, G., (1991). “På talefot med forbrukeren”, NKS-forlaget.

Bohner, G., Wänke,M., (2002). “Attitudes and Attitude Change”, Psychology Press.

Grønmo, S., (2007). *Samfunnsvitenskaplige metoder*(2.utg) Bergen: Fagbokforlaget

Hitchings, Jean., (1995).“Deficiencies of the traditional Approach to Information Security and the Requirements for New Methodology”., Computers and Security, (14), 377-383.

Høie, M., (2010). Historieforskning – et vell av mulige fortider. I:E. Arntzen & J.Tolsby (Red.) Studenten som forsker i utdanning og yrke: vitenskapelig tenkning og metodebruk (2.utg.) Læremiddel for profesjonsutdanning nr.10. Lillestrøm: Høgskolen i Akershus.

Jakobsen, E. W. and L. B. Lien., (2001). Ekspansjon; strategi for forretningsutvikling, Gyldendal fakta.

Jansen, A., Schartum, D.W., (2005). "Informasjonssikkerhet. Rettslige krav til bruk av IKT", Fagbokforlaget 2005.7

King, N. og C. Horrocks., (2010) Interviews in Qualitative Research Sage Publications, London.

Korb, M.P, Gorell J. & Van De Riet, V., (1989). Gestalt Therapy: Practice and Theory. Boston: Allyn and Bacon.

Kvale, S. & Brinkmann, S., (2009). *Det kvalitative forskningsintervju* (utg 2) (T.M. Anderssen & J. Rygge, overs.) (Orginaltittel: Interview: Learning the Craft of Qualitative Research Interviewing) Oslo: Gyldendal

Langdridge, D., (2004) Introduction to Research Methods and Data Analysis in Psychology, Harlow: Pearson Education

Mann, Leon., (1972). *Sosialpsykologi* (oversatt til norsk av Hedvig Wergeland). Oslo: Cappelen.

Marshall, C., Rossmann, G.B., (1999). "Designing qualitative research" Newbury Park: Sage Publications. 3rd ed., chapter 2, pp 21-54

McCracken, G., (1988). "The Long Interview", Newbury Park: A Sage Publication
Mehmetoglu, M., (2004) *"kvalitativ metode for merkantile fag "*, Fagbokforlaget.

Miles, M. B. og A. M. Huberman., (1994). An Expanded Sourcebook, Qualitative Data Analysis, Sage Publications, London

Panko, Raymond R., (2004). "Internet Security," In Hossein Bidgoli, *The Internet Encyclopedia*, John Wiley & Sons.

Ringdal, K., (2007) “Enhet og Mangfold”, Fagbokforlaget, 2.utgave.

Rosenberg, Milton & Carl I. Hovland., (1960). *Attitude Organizations and Change. An Analysis of Consistency among Attitude Components*. New Haven: Yale University Press.

Ryen, A., (2002) Det kvalitative intervjuet: fra vitenskapsteori til feltarbeid, Bergen: Fagbokforlaget.

Thagaard, T., (1998). ”Systematikk og innlevelse. En innføring i kvalitativ metode”. Fagbokforlaget.

Thagaard, T., (2002). ”Systematikk og innlevelse. En innføring i kvalitativ metode”. Fagbokforlaget.

Whitman E. M., and Herbert J. Mattord., (2011). ”Principles of Information Security”, Fourth edition,

Yin, R.K. (2003). “Case Study Research”, SAGE Publications

Yin, R.K. (2009). “Case Study Research”, SAGE Publications

8.3 Rapporter

Christensen, Kåre Gerhard., Kristensen, Terje., og Sætre, Per Jarle., (2000) Rapport nr.5 fra MUVIN 2 i Norge. ” Hør på oss!”- Elevenes syn på miljøundervisning og miljøspørsmål. Høgskulen i Sogn og Fjordane. http://www-bib.hive.no/tekster/muvin/rapport5/rapport5-07.html

Mona I. A. Engedal, Ekaterina Denisova, Kristine Langhoff, Kjell Lorentzen, Geir Martin Pilskog, Marina Rybalka og Knut Viken., (2009).”Nøkkeltall om informasjonssamfunnet”. Statistisk Sentralbyrå **http://www.ssb.no/a/publikasjoner/pdf/sa_118/sa_118.pdf** Hentet ut 19.02.14

Norden., (2012). ”Nordic Public Sector Cloud Computing - a discussion paper. 19.01.2012. ISBN: 978-92-893-2286-7 Publikasjonsnummer: TemaNord 2011:566 https://www.norden.org/sv/publikationer/publikationer/2011-566

NOU 2000:24, ”Et sårbart samfunn”, Justis og politidepartmentet.

NOU-2006-6 ”Når sikkerheten er det viktigste”, Justis politidepartementet, 2006 http://www.regjeringen.no/Rpub/NOU/20062006/006/PDFS/NOU200620060006000DDDPDFS.pdf

8.4 Nettsider

ENISA, “*Information Security awareness initiatives: Current practice and the measurement of success*, http://csrc.nist.gov/organizations/fissea/2009-conference/presentations/fissea09-mgupta-day3-panel_process-program-build-effective-training.pdf, (Accessed 27.01.2014).

Etableringer i Norge – IKEA http://www.ikea.com/ms/no_NO/about_ikea/facts_and_figures/ekspansjon_norge/ekspansjon.html (Hentet ut 28.05.13)

Forskningsetiske komiteer (2012) (hentet ut 6.11.2013). Av De nasjonale forskningsetiske komiteene. Publisert: 20. mai 2009. Sist oppdatert: 15. Oktober 2012. https://www.etikkom.no/no/Forskningsetikk/Etiske-retningslinjer/Samfunnsvitenskap-jus-og-humaniora/

Kunnskapsdepartmentet (2009) (Hentet ut 06.11.13) http://www.regjeringen.no/nb/dep/kd/dok/regpubl/stmeld/2008-2009/stmeld-nr-30-2008-2009-/9/2.html?id=556618

Myers, M.D., (2008).“Qualitative Research in information systems”, http://www.qual.auckland.ac.nz/, (accessed 13.01.2014).

Møller, Friis. Morten. (2013). ”Cloud Computing ger besparingar inom IT i offentlig sektor”. Hentet fra http://www.norden.org/no/aktuelt/nyheter/Cloud Computing-Computing-ger-besparingar-inom-it-i-offentlig-sektor 06.05.14. Utgitt 13.08.2013

Nilssen, D., (2012). “Hele journalsystemet til Vestre Viken brøt sammen”. Hentet 03.03.2014 http://www.vg.no/nyheter/innenriks/sykehus-norge/hele-journalsystemet-til-vestre-viken-broet-sammen/a/10057621/

North America`s Business Center- Missouri Development, hentet ut 04.05.2013 http://www.missouridevelopment.org/business%20solutions/Innovation%20and%20Business%20Development/Business%20Development.html

Reference, Security, hentet ut 15.11.2013. http://www.reference.com/browse/security

Sander, Kjetil, hentet ut 08.01.2013. Kunnskapssenteret – Holdninger http://kunnskapssenteret.com/holdninger/

Techtarget; (2011) Definition. Searchexchange.com. http://whatis.techtarget.com/ (Acc. 2011-9-15) http://searchcloudcomputing.techtarget.com/definition/cloud-computing (Hentet 08.02.14)

Wikipedia, Security awareness, hentet ut 15.11.2013 http://en.wikipedia.org/wiki/Security_awareness

8.5 Andre relevante kilder

Bakås, T.H., (2005). ”God praksis for å måle informasjonssikkerhetsnivå.” , *Masteroppgave Høgskolen i Gjøvik.*

Bjerkheim, Erna L E., (2008). *”Sikkerhet i forbindelse med informasjonssystemer. Har brukere, IT-ansatte og ledelse forskjellige holdninger til sikkerhet ved bruk av informasjonsteknologi?”* Et casestudie i Ringerike kommune. Masteroppgave; Høgskolen i Buskerud.

Christensen, Kenneth., (2013). Effektiv Ehelse i Helse Sør-Øst. Hentet fra http://www.idg.no/computerworld/article279836.ece 06.05.14. Utgitt: 06.12.2013

CSC: Company Profile., (2013) utgitt materiell fra CSC 28.05.13

CSC IaaS., (2013) Utgitt materiell fra CSC 24.05.2013

Eriksen, Henrik B., (2013). ”*Struktur og sikkerhet av nettverk ved integrerte operasjoner”* Masteroppgave, Teknisk Kybernetikk. NTNU – Det skapende universitet. Instituttet for teknisk kybernetikk fakultetet for informasjonsteknologi, matematikk og elektronikk. http://www.diva-portal.org/smash/get/diva2:644158/FULLTEXT01.pdf

Helse- og omsorgsdepartementet., (2011). De regionale helseforetakene, hentet fra http://www.regjeringen.no/nb/dep/hod/tema/sykehus/nokkeltall-og-fakta---ny/de-regionale-helseforetakene.html?id=528110

ISF., (2005). *“The standard of good practice for information security.”* Version 4.1. Information Security Forum.

Jakobsen, Erik W., (2012). Strategiforelesninger Masterstudiet i økonomi og administrasjon 25. Og 26. September 2012. ”Ressursbassert strategi, Ekspansjon og Innovasjon”. Av Dr Oecon Erik W. Jakobsen, Professor i strategi, HiBu.

Kaasbøll, Jens., (2009). ”Technology Acceptance Model”. 4. August, 2009. Universitetet i Oslo. http://www.uio.no/studier/emner/matnat/ifi/TOOL1100/h09/TAM.pdf

Mathisen, J., (2004).“Measuring information security awareness – A survey showing the Norwegian way to do it.”, Hovedfagsavhandling Høgskolen I Gjøvik.

Meese, Henning., (2007)“seks steg til IT-sikkerhet”, IDG Magazines Norge AS, pp 2-20.

Nordby, Y., (2005). Hansen, C.W., ”Informasjonssikkerhet – atferd holdninger, og kultur”., *i hovedfagsavhandling NTNU.*

Personopplysningsloven., (2000). Lov om behandling av personopplysninger, hefte 8. Sist endret LOV-2013-01.11.3 fra 01.06.2013. Hentet ut 14.02.14 http://lovdata.no/dokument/NL/lov/2000-04-14-31#KAPITTEL_2

Personvernloven., (2000). Lov om behandling av personopplysninger, hefte 8. Sist endret LOV-2013-01.11.3 fra 01.06.2013. Hentet ut 17.01.2014 fra http://lovdata.no/dokument/NL/lov/2000-04-14-31?q=person

Røyksund, Marie., (2011). “Informasjonssikkerhet i kraftforsyningen” Mastergradsstudium i samfunnssikkerhet. Universitetet i Stavanger http://brage.bibsys.no/uis/handle/URN:NBN:no-bibsys_brage_19637’

Sandvik, K., (2013) Forelesningsfoiler 03.11.2013 ”Forskningsetikk-Forskningsdesign og datastrategi 2.år”

Soo Hoo, Kevin J., (2000) ”How Much is enough? A risk-Management Approach to Computer Security”, Unpublished paper, June, http://iis-db.stanford.edu/pubs/11900/soohoo.pdf (Accessed 11.11.2013).

Stølen, Kjetil., (2006). “En oversikt over forskjellige aspekter ved sikkerhetspolicyer”, http://www.sintef.no/upload/IKT/9012/KST/Seminarer/mars-2006/1.stoelen.pdf

Søiland, A.,b., (2007) “seks steg til IT-sikkerhet”, IDG Magazines Norge AS,

Sørum, Helene., (2012). *”Økologisk mat i Forsvaret - holdninger til økologisk mat og landbruk blant brukerne av Forsvarets messer”.* Masteroppgave; Mat ernæring og helse. Fakultetet for helsefag. Instituttet for helse, ernæring og ledelse. Høgskolen i Oslo og Akershus

Tronvold, Bård og Stålsett, Kenneth., (2012). *"Hvordan påvirker opportunisme kontraktuelle forretningsrelasjoner?"* Masteravhandling i markedsføring ved Høgskolen i Buskerud.

Ås, Berit., (1992). "*Usikkerhet om framtid og våre handlingsvalg".* s.103-115 i ; Stenseth, Nils Chr, og Hertzberg; Katrine. *Ikke bare si det men gjør det.* Universitetsforlaget.

9. Vedlegg

Vedlegg 1: Intervjuguide

Presenterer oss selv, takker for at de kunne stille opp.

Bakgrunnsinformasjon

- Hva slags jobberfaring har du?
- Stilling?

Generelt/startfasen

- Har dere tatt i bruk Cloud Computing løsninger? Eventuelt hvilke former for Cloud Computing løsninger snakker vi om?
- Har vi en felles forståelse av hva Cloud Computing løsninger er? Og hvordan definerer dere Cloud Computing?
- Hva slags holdninger har dere til Cloud Computing? (Eks. Sikkerhet, nytte, kostnad, implementering, oppstarts investering, skalerbarhet, global tilgjengelighet, integrering, mobil app, forhold til leverandøren, avtaler mellom leverandører, sentralisert plassering, flaskehalser ved dataoverføring/responstid, tap av fysisk kontroll, osv) Hvorfor?
- Hva mener dere Cloud Computing kan bidra med i norske sykehus? (f.eks gevinster og eventuelle risikomomenter?)
- Hvilke utfordringer ser dere for dere med tanke Cloud Computing innenfor offentlig sektor?

Sikkerhet

- Opplever dere sikkerhetsmessige utfordringer med Cloud Computing
- Hva tenker dere om Cloud Computing sikkerhet vs det nåværende datasystemet dere har?

Holdninger

- Anta at Cloud Computing data og eventuell programvare er lagret på en server i Norge – hvilken holdning har dere til dette? Endrer det noe av sikkerhetsproblematikken?

- Hvordan oppfatter du dine kollegaers holdninger til bruk av Cloud Computing?
- Hvilke kostnadseffektiviseringer ser du ved bruk av Cloud Computing?
- Hva er din holdning til brukervennlighet innenfor Cloud Computing?
- Hva er din holdning til Cloud Computings brukerstøtte?
- Hva er din holdning til effektivisering av deres IKT-systemer ved hjelp av Cloud Computing?
- Har dere noen videre planer for bruk av Cloud Computing?

Helt til slutt

- Hva tenker du når du hører CSC(computer Sciences cooperation)?
- Hva vet du om CSCs Cloud Computing produkt?

Ha i bakhodet

- Hva hindrer deg i å bytte ut ditt nåværende IKT-system mot Cloud Computing?
- Hvordan er sykehusenes nåværende systemer ift effektivisering, kostnad og brukervennlighet?