Uppsala Universitet

Institutionen för informatik och media

Molntjänster för svenska sjukvårdsorganisationer

- *En guide för behandling av patientdata*

Siri Djurberg

Antonia Miocic

Kurs: Examensarbete

Nivå C

Kurskod: 2IS042

Termin: VT18

Handledare: Claes Thorén

Datum: 13 juni 2018

Förord

Först och främst vill vi rikta ett stort tack till vår handledare Claes Thorén, som varit en riktig idéspruta under arbetets gång. Vi vill även tacka våra respondenter som deltagit nämligen Per Foyer, Ralph Benton, Kim Hindart, Per-Olof Wadeborn och Hans Berglund som gjort arbetet möjligt då de bidragit med kunskaper och insikter som format uppsatsen.

Sammanfattning

Molntjänster har redan tagit över flera branscher och sjukvården står näst på tur. Molntjänsters effektiviseringar lockar sjukvården som är en hård pressad bransch både inom kompetens och tid. Samtidigt ansvarar sjukvården över patientdata vilket leder till att de har strikta lagar och regelverk att följa som innebär stora utmaningar. Det kan vara svårt att få en holistisk bild av vad molntjänster kan erbjuda sjukvårdsorganisationen och därför har vårdens syn på molntjänster undersökts och vilka faktorer som präglat deras hantering av patientdata i molnet. En kvalitativ studie har genomförts och där respondenter som är IT-ansvariga både på sjukvårdsorganisationer och molnleverantörer har intervjuats. Sammanfattningsvis dras slutsatsen att i IT-ansvariga på sjukvårdsorganisationer ser molntjänster som en möjlighet och en väg som de måste tas. För att kunna möta patienters behov är de överens om att sjukvården kommer behöva möta deras patienter på en digital plattform och att det krävs tydliga gemensamma riktlinjer för hur man som sjukhusorganisation bör agera vid beslutstagande av molntjänster från en molnleverantör. Det är av intresse att en myndighet upprättas för att ta fram dessa lagar och riktlinjer i syfte att vara rådgivare och inte granskande. Slutligen presenteras sex stycken punkter, som enligt respondenterna, präglar hantering av patientdata i molntjänster som är riktade till de beslutsfattande och IT-ansvariga som är involverade i de beslut som ska fattas kring användandet av molntjänster inom sjukvårdsorganisationer.

Nyckelord

Cloud computing, security, responsibility, risks, healthcare, McCumber

Innehållsförteckning

1. Inledning

Idag ställs sjukvården inför stora utmaningar och det finns många olika faktorer som kommer att påverka på hur hälso- och sjukvården kommer att se ut i framtiden. Sjukvårdsorganisationer måste leverera sjukvård av mycket hög kvalitet som kräver hög kunskap, samtidigt som det finns andra ansvar, såsom att hålla nere kostnader och arbeta förebyggande med patienter för att främja folkhälsan. (Microsoft Corporation, 2013, s.4) Sjukvårdsorganisationer innefattas i denna studie av primärvården, länssjukvården och regionsjukvården (Nationalencyklopedin, 2018). Samtidigt som sjukvården ställs inför dessa utmaningar har de också stora krav på att följa regelverket kring säkerhet och integritet, då de hanterar patientdata. Regelverk såsom patientdatalagen, patientsäkerhetslagen och personuppgiftslagen eller GDPR. (Microsoft Corporation, 2013, s.4) Enligt AbuKhousa, Mohamed och Al-Jaroodi (2012) är en viktig strategi för många vårdorganisationer att planera för att utnyttja den senaste tekniken inom vårdindustrin både för att förbättra vården men också minska driftkostnaderna. Det finns en stor ökning av efterfrågan på hälsovårdstjänster samtidigt som det finns en brist på kvalificerad vårdpersonal såsom läkare, sjuksköterskor och apotekare, vilket utgör en av de hårdaste prövningar för just sjukvårdsorganisationer. (AbuKhousa, Mohamed & Al-Jaroodi, 2012, s.622)

Det finns många chefer och experter som tror att molntjänster kan förbättra hälso- och sjukvården, vårdforskning och förändra hela tekniken då molntjänster är ett nytt sätt att leverera datorresurser och tjänster (Kuo, 2011, s.1). Likadant hävdar Zissis och Lekkas (2010, s.585) att så länge man använder betrodda tjänster inom molntjänster och det finns ett starkt förtroende för att bevara sekretess, integritet och äkthet av data kan molntjänstleverantörer erbjuda idealiska molnlösningar.

1.1 Bakgrund

Enligt Bushhouse (2011, s.388) finns det flera olika definitioner och förklaringar på vad molntjänster är då det representerar ett brett begrepp. Enligt författaren innebär användning av molnet för datatjänster att man förblir ägare till sin information, men att någon annan ansvarar för att lagra den och behålla säkerheten. Användning av molntjänster kan erbjudas som en fullständig tjänst alternativt flera tilläggstjänster beroende på valet av användaren. Det finns många leverantörer som levererar dessa molnbaserade tjänster som erbjuder varierade prissättningsmodeller för de kunder som vill använda vissa produkter som en “service”, antingen för ett specifikt projekt eller en längre tid. Detta handlar om att förlita sig på en tredje part, vilket kan väcka frågor om just säkerhetsaspekter som konfidentialitet, integritet, tillgänglighet och lagring. Man bör därför säkerställa en pålitlighet hos den tredje parten innan implementation av servicen. Dock är det inte nödvändigt att placera alla resurser i molnet. Utan det finns särskilda modeller som möter olika behov. (Bushhouse, 2011, s.389)

Kuo (2011, s.4) menar att precis som med vilken innovation som helst, så bör man noggrant utvärdera molntjänster innan en eventuell implementation kan ske samt ta ställning till vad man som organisation faktiskt behöver. Men att det finns flera skäl att tro att det skulle hjälpa sjukvården att skapa nytta genom att implementera just molntjänster.

1.2 Problembeskrivning

I en bransch där kvalité på arbete och kostnadseffektiviseringar kan vara livsavgörande förväntas sjukvårdsorganisationer utforska IT-system som möjliggör detta (Bushhouse, 2011, s.392). Men vem skyddar patientdata om leverantören för molntjänsten går i konkurs eller blir uppköpt? I en rapport *Vägledning – informationssäkerhet i upphandling* från myndigheten för samhällsskydd och beredskap(MSB) från 2013, belyses hur organisationer hamnar i direkt beroendeställning till leverantören av tjänsten molntjänster. MSB varnar för hur avtalet mellan leverantören och kunden förflyttas till annan part vid konkurs och därför ligger utanför kundens kontroll. Denna problematik har växt till en stor diskussionsfråga i debatten om vårdens införande av molntjänster. Det som oroar motståndarna är de förödande konsekvenser som skulle följa vid en säkerhetskris eftersom sjukvårdsorganisationer hanterar stora mängder patientdata och sekretessbelagda dokument. (MSB, 2013, s.19)

Det finns mycket tidigare forskning som konstaterar fördelar med molntjänster i sjukvården och de som driver implementeringen framåt bemöter ofta problematiken genom att förespråka en moln-modell anpassad efter organisationens behov, det styrker bland annat Kuo i en rapport från 2011 och MSB i sin rapport från 2013 (Kuo, 2011 ; MSB, 2013). Staten har uppmärksammat en brist av lagar för hantering av personuppgifter för myndigheter (Myndighetsdatalag, 2015). Det kan därför vara svårt vid beslutsfattande att få en holistisk bild av vad molntjänster kan och får erbjuda för sjukvårdsorganisationen och vilka risker varje tjänst innebär. Ett möjligt utfall blir då att hela molntjänsten förkastas trots att molntjänsten kunde vart en effektiv lösning för organisationen. (Gorelik, 2013, s.23)

1.3 Syfte

Uppsatsen har som syfte att öka förståelsen för om molntjänster bör användas av sjukvårdsorganisationer utifrån ett säkerhetsperspektiv. Att visa på dagens argumentation och förståelse för molntjänster i vården, samt se till vad för faktorer det finns som påverkar användandet vid hantering av patientdata. Den målgrupp uppsatsen vänder sig till är främst de beslutsfattande och IT-ansvariga som är involverade i de beslut som ska fattas kring användandet av molntjänster på sjukvårdsorganisationer.

1.3.1 Frågeställning/forskningsfrågor

Den frågeställningen som ligger till grund för uppsatsen är följande:

- *Hur förstår IT-ansvariga på sjukvårdsorganisationer i Sverige molntjänster och vilka faktorer är det som präglar användandet ur ett säkerhetsperspektiv för patientdata?*

En förklaring till ordet *faktorer* ses som relevant då det anses finnas en bred betydelse och vara ett svårtolkat ord, faktorer anses vara det uttalande som de IT-ansvariga på sjukvårdsorganisationer uppger utifrån de krav som ställs gällande säkerheten för patientdata vid användande av molntjänster.

1.4 Avgränsningar

Det övergripande ämnet "molntjänster inom organisationer" är i denna uppsats avgränsad till sjukvårdsorganisationer. Denna avgränsning har sin motivering i uppsatsens problemformulering då det observerades brister inom tidigare forskning i detta ämne. Resultatet baseras på data som är geografiskt avgränsat till sjukvårdsorganisationer inom Stockholm och Uppsala.

För att ytterligare avgränsa uppsatsen har resultatet inhämtats utifrån ett IT-säkerhetsperspektiv, med fokus på behandling av patientdata. Fokus på patientdata är valt då denna data är känslig och hanteras av sjukvården vilket innebär att de, utöver patientdatalagen (PUL) eller General Data Protection Regulation (GDPR), även behöver ta hänsyn till patientdatalagen.

1.5 Kunskapskaraktärisering

Uppsatsen resulterar i en kvalitativ rapport som kommer att vara vägledande inför beslutsfattande vid användandet av molntjänster i sjukvårdsorganisationer. Vägledande kunskap innebär att man talar om hur man bör gå tillväga i olika situationer, alltså en handlingsinriktad kunskap. Vilket stämmer överens med uppsatsen syfte, att öka förståelsen för om molntjänster bör användas av sjukvårdsorganisationer utifrån ett säkerhetsperspektiv och se vilka faktorer det är som präglar användandet. Målet med den vägledande kunskapen är att kunna använda sig av molntjänster utan att äventyra säkerheten för patientdata, vilket refererar till uppsatsens värdekunskap. Värdekunskap innebär det önskvärda värden som handlingen förväntas leda till, det vill säga, att skapa medvetenhet och ge goda kunskaper kring molntjänster ur ett säkerhetsperspektiv. (Goldkuhl, 2011, ss.12–14)

1.6 Disposition

Uppsatsen är uppdelad i 5 kapitel, I *kapitel 2* presenteras de vetenskapliga teorierna som ligger till grund för uppsatsen. Begreppet molntjänst förklaras mer ingående under rubriken 2.1 Kunskapsinventering, tillsammans med andra väsentliga begrepp samt den tidigare forskning som uppsatsen kommer beröra eller kräver förståelse kring. Slutligen presenteras även ramverket "The McCumber Cube" som används för att analysera datan.

I kapitel 3 redovisas det vetenskapliga tillvägagångssättet, där forskningsansats, datainsamling och en generalisering av resultatet presenteras.

Vidare i *kapitel 4* presenteras resultatet både från intervjuer, tidigare forskning och dokument som samlats in, diskussion och analys görs löpande av det resultatet.

Slutligen i *kapitel 5*, vilket är den avslutande delen presenteras slutsatser som tagits utifrån frågeställningen och en reflektion kring uppsatsens resultat görs som sedan avslutas med en diskussion om eventuell vidare forskning.

2 Teori

I följande avsnitt presenteras de vetenskapliga teorierna som ligger till grund för uppsatsen. Främst redogörs väsentliga begrepp och tidigare forskning för uppsatsen i en kunskapsinventering och slutligen presenteras ramverket som används för att analysera resultatet senare i uppsatsen.

2.1 Kunskapsinventering

Detta kapitel ges en förklaring på de centrala begreppen för uppsatsen samt så behandlas vad tidigare forskning säger angående molntjänster, dess för och nackdelar tas upp i form av en presentation kring säkerheten i förhållande till molntjänster, risker med leverantörsinlåsning och ansvaret för patientdata. Kapitlet berör slutligen de lagar som är aktuella och vad tidigare forskning säger om det i förhållande till molntjänst.

2.1.1 Molntjänst

Som tidigare nämnt finns det otaliga definitioner och tolkningar av just molntjänster. Information Technology Laboratory of the National Institute for Standards and Technology (NIST) definierar begreppet "Cloud computing" genom följande (Mell & Grance, 2012, s. 2):

> "Cloud computing is a model for enabling ubiquitous, 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."

Anledningen till att just denna definition presenteras är på grund av att kunna referera till en definition som är vedertagen i betydelsen och är väl spridd. Swedish Standards Institute (SIS), har antagit en svensk standard som baseras på den internationella standarden av ISO-organisationen, för att bland annat kunna definiera begreppet molnbaserade datortjänster. SIS svenska översättning av ISO-standarden definierar begreppet som följande (Swedish Standards Institute, 2014):

> "Koncept för nätverksåtkomst till en skalbar och elastisk pool av delade fysiska eller virtuella resurser med automatisk åtkomst och administration på begäran"

ISO-standarden fastställdes år 2014 och tillsammans med NIST:s definition ovan ses detta vara en bra förutsättning för analyser och resonemang då dessa definitioner anses som allmänt accepterade inom ämnet och dessutom väl använda.

2.1.2 Tjänstemodeller

Som tidigare nämnt finns det särskilda modeller som möter olika behov. Molntjänster består i grunden av tre olika modeller, så kallade tjänstelager: Infrastruktur, plattform, och mjukvara som en tjänst. Dessa lager kommer nedan förklaras kort för att skapa förståelse kring begreppet molntjänster, men kommer inte hanteras med något större fokus i uppsatsen. (Halpert, 2011, ss.5–6)

- *Infrastructure as a Service (Iaas)* = Infrastruktur som tjänst innebär att man som slutanvändare får tillgång till IT-infrastruktur. Med andra ord får användaren tillgång till tekniker och funktioner som finns i ett traditionellt datacenter, utan att kontinuerligt behöva investera i hårdvara och underhåll. En förenklad förklaring, ett företag hyr in sig på servrar och annan utrustning som ägs och sköts av leverantören.

- *Software as a Service (SaaS)* = Innebär att användaren får tillgång till mjukvara eller ett program, som hyrs ut via internet. Kunden har alltid tillgång till programmen från sin webbläsare, men programmen körs på leverantörens servrar.

- *Platform as a Service (PaaS)* = Som Erbjuder kunden bland annat hårdvara, nätverk eller operativsystem som tjänst, vilket tillhandahålls över internet. Kunden kör sina egna program/applikationer, men hyr allt som behövs för att köra dem.

2.1.3 Olika typer av molninfrastrukturer

Det finns olika typer av molninfrastrukturer nämligen publika moln, privata moln, partnermoln och hybridmoln. Molntjänster som tillhandahålls av en molnleverantör är vad som kommer hanteras främst i denna uppsats. Vilket både kan vara publikt eller privat moln beroende på vem som tillhandahåller servrarna. För att skapa förståelse för hela begreppet "molntjänst", lyfts alla olika infrastrukturer kort nedan. (Gorelik, 2013, s.19)

- *Publikt moln* = Molnet är en uppsättning datorresurser som tillhandahålls av organisationer från tredje part.
- *Privata moln* = Molnet är byggt och förvaltat inom en enda organisation. Infrastrukturen är dedikerad till beställaren och att inga andra företag använder de servrarna.
- *Hybridmoln* = En blandning av dataresurser som tillhandahålls av både privata och publika moln.
- *Partnermoln* = En samarbetsaccepterad version av privata moln där man delar resurser i flera organisationer.

2.1.4 E-Hälsa och Distansvård

Informationsteknik har fått en större och mer grundläggande roll i hantering, distribution och lagring av information i vården. Tekniken och tillämpning av informationsteknologi utvecklas ständigt. Det finns många olika titlar för att namnge det, och enligt (Shih et al., 2012. s.836) är e-hälsa den mest acceptabla termen. Med den motiveringen har den termen använts vidare i uppsatsen.

Världshälsoorganisationen (WHO) definierar e-hälsa som följande:

> "*eHealth is the use, in the health sector, of digital data transmitted, stored and retrieved electronically in support of health care, both at the local site and at a distance.*" (Shih et al., 2012. s.836)

2.1.5 Säkerhet i förhållande till molntjänst

Som tidigare nämnt finns det många anledningar till att tro att molntjänster är lösningen på många problem och framtiden för att effektivisera vården (Kuo, 2011, s.1). Detta menar även Sultan (2014, s.179) som påpekar människans ökande nivå av förväntad livslängd, med en åldrande befolkning som behöver vård har efterfrågan för effektivisering av just vård stigit. Molntjänster skulle också kunna öppna upp för en möjlighet för vårdgivare att dela sina uppgifter med andra intressenter som regeringens myndigheter, hälsoforskningsinstitut, auktoriserade privata företag såsom försäkringsbolag och andra sjukhus. Att kunna dela patienters data kan tjäna olika syften som bidrar till att förbättra kvaliteten av vården. Svårigheten med detta är dock att denna delning måste följa strikta regler för vem som delar och hur väl patienternas integritet upprätthålls. (AbuKhousa, Mohamed & Al-Jaroodi, 2012, s.622)

Precis som att molntjänster kan utgöra många fördelar för vården, kan det också medföra risker. Vid hantering av patientdata är tillgången av obehörig data en oerhört känslig punkt. Även om många molntjänsteleverantörer kan erbjuda säkerhetsåtgärder, som till exempel loggning av vem som har tillgång till datan anser ändå AbuKhousa (2012, s.626) att det finns mycket arbete kvar att göra för att öka säkerheten gällande just detta.

Enligt Löhr, Sadeghi och Winandy (2010, s. 223) är lagring av sekretesskänsliga data i centrala datacenter en av de största riskerna för informationsläckage till obehöriga enheter. De menar på att all känsliga data som lagras alltid måste vara tillräckligt skyddad, t ex med hjälp av kryptering. Dessutom måste det vara möjligt att administrera datacentret utan att administratörer kan få tillgång till patientdata vilket är betydligt svårare att kontrollera.

Precis som tidigare nämnt, menar Löhr, Sadeghi och Winandy (2010, s. 223) att all känsliga data alltid måste vara tillräckligt skyddad som t ex stark kryptering. Detta tar även Gorelik (2013, s.24) i form av frågor som är viktigt att säkerställa innan man antar en implementation av en molntjänst.

- Vem har tillgång till uppgifterna? Vad är reglerna för åtkomstkontroll?
- Kan data krypteras när den lagras i molnet? Vem håller krypteringsnycklarna? (Om en molnleverantör inte ska ha tillgång till uppgifterna bör krypteringsnycklarna endast innehas av det företag som äger uppgifterna).
- Är datan krypterad under överföringen från det interna nätverket till det offentliga molnet?

2.1.6 Leverantörsinlåsning hos molnleverantör

Enligt Armbrust et al., (2010) är inlåsning ett stort riskområde eftersom det inte finns några utformade standarder för molnet. En leverantörsinlåsning inom molntjänster innebär den komplexitet av att förflytta en applikation eller data mellan molnleverantörer alternativt tillbaka till organisationen. Faktorer som prisökning, tid, grad av svårighet och portabilitet, tillförlitlighetsproblem är variabler som bestämmer storleken av den inlåsningseffekt som företagen måste vara medveten kan uppkomma eller redan existera. Således kan kunderna inte lika enkelt extrahera sin data och program från en plats till en annan. De svårigheterna med att extrahera data från molnet förhindrar vissa organisationer från att anta molntjänster vid datoranvändning. Kundlåsning kan vara attraktivt för leverantören men deras kunder och användare blir i sin tur väldigt sårbara. (Armbrust et al., 2010, ss.54–55)

Även MSB (2013) lyfter i sin rapport *Vägledning – informationssäkerhet i upphandling* att leverantörsinlåsning är en stor risk. MSB menar att migrering av system mellan molntjänstleverantörer kan vara svårt eftersom det dels inte finns några etablerade standarder eller verktyg för detta samt dels för att leverantören inte har intresse att underlätta för ett eventuellt leverantörsbyte. Leverantörinlåsning är därför en viktig aspekt att beakta då det ger molntjänstleverantören hög auktoritet som kan försvåra för kundens begäran på införande av nya säkerhetskrav.

2.1.7 Ansvaret av patientdata

Enligt Löhr, Sadeghi och Winandy (2010, s. 223) är säkerheten i slutanvändarsystemet ett problem som är väldigt viktigt, men som sällan behandlas. Många definierar problemet som "out of scope", alltså att det inte ligger i deras händer att lösa. Författarna anser dock att, till exempel en läkare, som vanligtvis inte har den sorts kompetens och tid till att professionellt kunna hantera sina IT-system ska vara tillräckligt skyddad för att kunna arbeta, utan att riskera läckage. Å andra sidan används datorsystemen inte bara för att få tillgång till hälsoinformation om patienter utan också för andra tillämpningar såsom fakturering och webbläsare vilket försvårar situationen. (Löhr, Sadeghi & Winandy, 2010, s. 223)

Molntjänst-användare står inför säkerhetshot både från utsidan och inuti molnet. Enligt Armbrust et al., (2010, s.55) är många av de säkerhetsproblem för att skydda datan från yttre hot liknande de hot som organisationen redan står inför i sitt datacenter. Dock kan detta ansvar vara uppdelat mellan flera parter, såsom molnanvändare, molnleverantör och möjligtvis en tredje part. (Armbrust et al., 2010, s.55) I motsats till konventionell visdom föreslår forskning att små lokala molnleverantörer uppfattas som mer tillförlitliga och mer betrodda än stora och väletablerade företag. Författarna ser en potentiell fördel att anta en molnlösning, men menar att det är valet av att välja rätt molnleverantör som är den verkliga utmaningen. (Sultan, 2014, s.183) Gorelik (2013, s.24) påstår att det inte finns belägg för att garantera att data skyddas bättre internt jämfört med ett publikt moln. Faktum är att det finns en möjlighet att data kan vara mer säkert i ett publikt moln, detta eftersom molnleverantörer kan utgöra en högre grad av kompetens när det kommer till säkerhet än sina kunder. (Gorelik, 2013, s.24)

En viktig aspekt av informationssäkerhet är integritet, vilket innebär att tillgångar endast kan ändras på auktoriserade sätt, vilket gäller både för data, programvara och hårdvara. Integritet avser att skydda data från obehörig radering, modifiering eller tillverkning. Tillstånd är den mekanism som bestämmer vilken nivå av tillgång en viss autentiserad användare bör ha. På grund av det ökade antalet enheter och åtkomstpunkter i en molntjänst är auktorisering, enligt författarna, avgörande för att kunna säkerställa att endast auktoriserade enheter kan interagera med datan. Detta är givetvis extra viktigt att kontrollera om man outsourcar, att ha ansvar över vem som egentligen har tillgång och kan se den data som lagras. Att använda kryptografi är ett sätt att underlätta säkra interaktioner mellan två parter som båda måste lita på en tredje part. (Zissis & Lekkas, 2010, s.588)

2.1.8 Lagar/regler

Allt efter att teknologin utvecklas så framställs nya lagar, policys och riktlinjer som anpassas därefter. Denna utveckling kommer fortlöpa och eftersom både molntjänst-leverantörer och dess klienter är beroende av lagar, riktlinjer och policys tvingas dem till ett samarbete för att klargöra vad som ska göras, av vem och hur (Gordon, 2016, s. 475). Det innebär att ett juridiskt avtal behöver formuleras baserat på de riktlinjer parterna behöver följa. Dessa kontrakt kan se olika ut men lagen gör att de innehåller tre grundläggande komponenter. Gordon (2016, s. 473) definierar dessa enligt följande:

1. Juridiska komponenter, som t.ex. tvistlösning.
2. Datakomponenter, för praxis kring molndatat (äganderätt, säkerhet).
3. Tjänstekomponenter, som omfattar aspekter av hur tjänsten tillhandahålls. T.ex. såsom drifttid.

Jurister har en stor inverkan vid utvecklingen av molntjänster. Det eftersom jurister både formulerar lagen på uppdrag av politiska chefer samt tolkar lagen och därigenom har befogenhet att bestämma vid uppkomsten av konflikter eller tvetydigheter i juridiska tolkningar. (Eriksson, 2013, s.174)

Det finns olika lagar som sjukvården behöver ta hänsyn till. Följande lagar som presenteras är några av dessa som lyfts vidare i uppsatsen.

Personuppgiftslag, PUL, (1998:204) & General Data Protection Regulation (GDPR)
Personuppgiftslagen upphävdes 25 maj 2018 men redovisas eftersom den gällde under tiden för datainsamlingen. 1§ Syftet med denna lag är att skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter. Lagen reglerar bland annat överföring av personuppgifter som är under behandling. Dessa får inte överföras till ett land som saknar adekvat nivå för skydd av uppgifterna. Detta förbud gäller även överföring av personuppgifter för behandling i tredje land.

Personuppgiftslagen kommer ersättas av europaparlamentets och rådets förordning 2016/679 kallad General Data Protection Regulation, förkortat GDPR. Denna lag är vidare benämnt med den svenska beteckningen dataskyddsförordningen eller dess förkortning GDPR. I lagen under skäl (6) anges följande som visar på behovet av bredare kommunikation:

- “Tekniken har omvandlat både ekonomin och det sociala livet, och bör ytterligare underlätta det fria flödet av personuppgifter inom unionen samt överföringar till tredjeländer och internationella organisationer, samtidigt som en hög skyddsnivå säkerställs för personuppgifter.”

Patientdatalag (2008:355)
Innefattar förordningar som tillämpas vid vårdgivares behandling av personuppgifter inom hälso- och sjukvården enligt 1 kap 1.om hur vårdgivaren ska behandla personuppgifter inom hälso- och sjukvården. Lagen reglerar bland annat:

- Sammanhållen journalföring, som via ett elektroniskt system, möjliggör för vårdgivare att ge eller få tillgång till personuppgifter lagrade hos andra vårdgivare enligt 6 kap 1§.
- Lagen ger även möjlighet för vårdgivare har att ge patienten direktåtkomst till dokumentation om patienten via medel för automatiserad behandling som exempelvis via internet enligt 5 kap 5§.

Dataskyddsförordningen i förhållande till Patientdatalagen (2008:355) och PUL
Dataskyddsförordningen (GDPR) infördes 25 maj 2018. Den innehåller generella förordningar och regler kring användandet av personuppgifter inom hälso- och sjukvården. I vilken som mån Patientdatalagen kommer behöva regleras efter GDPR utreds av en särskild utredning som fått i uppdrag att se över vilka anpassningar av regler som behövs inom Socialdepartementets verksamhetsområde. (Datainspektionen, 2018)

Cloud Act - H.R.1625 (2017–2018)
Amerikanska kongressen har tagit fram lagen H.R.1625 - 115th Congress (2017–2018) i vilken Cloud Act Eller "Clarifying Lawful Overseas Use of Data Act" är en aktion. Lagen innefattar enlig Congress.gov (2018) H.R.1625 Division V - Cloud Act Sec. 103 § 2713:

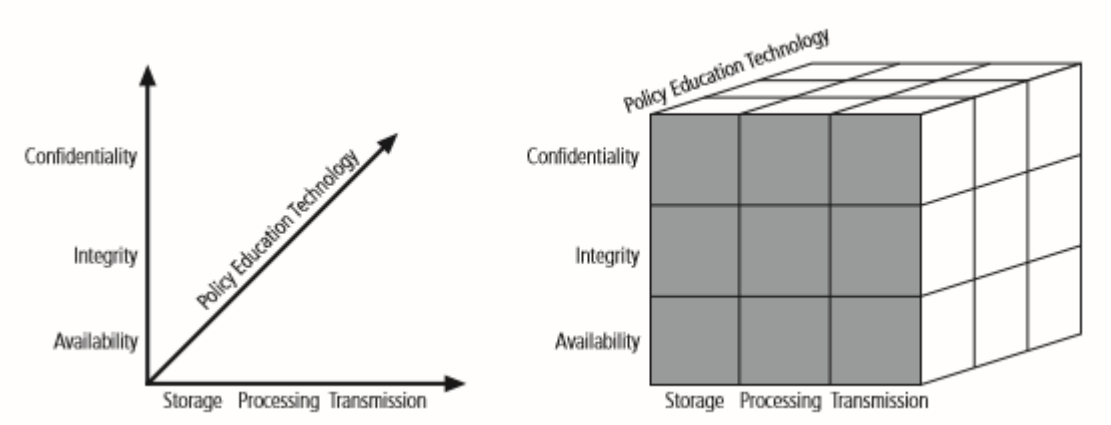
> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."

Sammanfattningsvis innebär lagen att en leverantör av en elektronisk kommunikationstjänst eller fjärrdatatjänst som är börsnoterade i USA ska bevara, säkerhetskopiera eller avslöja innehållet i en molntjänst som gäller en kund eller abonnent inom dennes tillhandahållare, vårdnad eller kontroll, oavsett om sådan kommunikation, post eller annan information finns inom eller utanför USA.

2.2 Ramverk

I detta avsnitt tas ramverket för uppsatsen upp som sedan används för att analysera resultatet.

2.2.1 The McCumber Cube



Figur 2. The McCumber Cube (Whitman, 2012, s.18)

Uppsatsen utgår från en modell, nämligen the McCumber Cube. Modellen skapades av John McCumber år 1991. Modellen har använts av the National Security Telecommunications and Information Systems Security Committee (NSTISSC) och är också publicerad i deras ordlista, National Information Systems Security (INFOSEXC). Modellen är utvecklad som ett svar på relationen mellan kommunikation och datasäkerhets riktlinjer. (McCumber, 2004, s.99)

The McCumber Cube har grundat sig i en annan modell vid namn C.I.A. triangeln som har varit standarden för datasäkerhet både inom industrin och regeringen. Denna standard är baserad på de tre egenskaperna hos information som ger ett värde för organisationer, nämligen: konfidentialitet, integritet och tillgänglighet. (Whitman, 2012, ss.10–11)

Det har varit mycket debatt kring om dessa tre aspekter är tillräcklig, ur ett säkerhetsperspektiv, eller om man borde lägga till en ytterligare aspekt som skulle komplettera för den ansvarsskyldighet man bör ha till informationen (Hafiz & Johnson, 2006, s.16). Triangeln är generellt sett inte längre tillräcklig för att hantera den ständigt föränderliga miljön och teknik. Utan de ständigt växande hoten har lett till utveckling av mer komplexa modeller, såsom The McCumber Cube (Whitman, 2012, ss.10–11). Enligt John McCumber (2004, s.99) själv var utvecklingen av modellen nödvändig för att definiera en modell som inte begränsas av organisatoriska eller tekniska förändringar.

Modellen ger en grafisk representation av tillvägagångssättet som används allmänt inom dator- och informationssäkerhet. The McCumber Cube är utformad med tre dimensioner, som visas i Figur 1. Varje dimension/axel består av tre celler, vilket i sin tur utgör kubens 27 celler (3 x 3 x 3 = 27). Varje cell representerar områden som måste adresseras korrekt för att säkra ett informationssystem. Med andra ord så hjälper modellen till att komma ihåg att överväga alla viktiga designaspekter utan att bli alltför fokuserad på en speciell. (Whitman, 2012, ss.18–19) Modellen är tredimensionell av den anledningen att kunna fånga upp den sanna naturen hos cellernas samspel vid säkerhet av informationssystem. Genom att kolla på fler

aspekter får modellen både djupare och ingående syn på IT-säkerhet, speciellt eftersom kuben just sätter cellerna i relation till varandra. Modellen har enligt (McCumber, 2004, ss.108–109) flera viktiga tillämpningar, då kuben både kan användas till att identifiera informationstillstånd och systemproblem, men också till att urskilja de säkerhetsåtgärder som kan användas för att minimera de sårbarheter som hittas med hjälp av modellen. En annan viktig tillämpning, är att modellen kan användas som ett utvärderingsverktyg, och på så sätt hjälpa till att analysera och evaluera ett redan existerande informationssystem. (McCumber, 2004, ss.108–109)

Kubens olika dimensioner består av följande:

1. Confidentiality (konfidentialitet), integrity (integritet) och availability (tillgänglighet) (C.I.A. triangle)
2. Policy (lagar/riktlinjer), education (utbildning) och technology (teknologi)
3. Storage (lagring), processing (bearbetning) och transmission (transmission)

Motivationen till valet av att använda the McCumber cub är för att modellen idag har blivit en allmänt accepterad utvärderingsstandard för informationssystems säkerhet. (Whitman, 2012, s.18) Den är applicerbar på uppsatsen eftersom den implicerar hur respondenterna ska ta ställning till vad säkerhet är och hur den uppnås. Enligt Whitman (2012, s. 25) krävs det tvärvetenskaplig kunskap, skicklighet och erfarenhet för att kunna behärska det skydd av informationssäkerhet som behövs. För att kunna bemöta denna komplexitet ses det som en möjlighet att använda the McCumber cube och på så sätt få en relevant och rättvis grund till uppsatsen och dess analys. Det värde som modellen också medför till vetenskapen om informationssystemsäkerhet är tillämpningen av ett informationsbaserat tillvägagångssätt som kan tillämpas oberoende hur själva genomförandet rent tekniskt utförs (McCumber, 2004, s.18). Fokus ligger på begreppen konfidentialitet, integritet, lagring, lagar och tillgänglighet. Skälet till detta är den information som hämtas in och vad respondenterna tagit upp under intervjun.

3 Forskningsansats och Metod

Under denna rubrik kommer processen för studiens genomförande att beskrivas.

3.1 Forskningsansats

En kvalitativ fallstudie har genomförts på sjukvårdsorganisationer samt leverantörer av molntjänster till vården baserade i Uppsala och Stockholms län. Det som kännetecknar en fallstudie är att studien fokuserar mer på djup än på bredd vilket krävs för att besvara uppsatsens frågeställning. Fallstudier kännetecknas även av att använda flera datainsamlingsmetoder och samla data från flera olika källor (Oates, 2005, s. 142). Med den motiveringen har denna studie insamlat data från aktörer i vården samt olika molntjänstleverantörer för att erhålla olika perspektiv.

Studien har ett kvalitativt forskningsperspektiv vilket innebär att det initialt insamlades empiri för att utifrån den sedan formulera begrepp och hypoteser. Det innebär att studien haft en övervägande induktiv forskningsansats, dock inte fullständigt då en viss strukturering av teman gjordes innan datainsamlingen, för att samla en övergripande bild av fenomenet molntjänster och därmed underlätta för analysarbetet vilket kan ses som ett deduktivt förarbete. (Backman, 2008, s.54–61)

Fallstudien faller under kategorin beskrivande som kännetecknas av en detaljerad analys av fenomenet molntjänst i kontext till sjukvårdsorganisationens behov av skydd av personuppgifter. Uppsatsen presenterar en diskussion om molntjänster möjlighet samt en undersökning om sjukvårdens medvetenhet. (Oates, 2005, s.143) Den tidsaspekt som uppsatsen inriktat sig på är främst en short-term, nutida studie som återspeglar respondenternas inställning till molntjänster just nu men hanterar också till viss del en framtida reflektion. Uppsatsen innehåller också ett historiskt tidsperspektiv då tidigare forskning granskas inom ämnet. (ibid, s.145)

Populationen för uppsatsens studie är IT-ansvariga inom sjukvården samt IT-ansvariga inom molntjänstleverantör. IT-ansvarig anses vara alla de som har ett åtagande inom IT, eftersom respondenten behöver vara medveten om organisationens IT-struktur för att kunna ta ställning till fenomenet molntjänster. Det specificerades avsiktligen inte vilken grad av åtagande respondenterna behövde ha inom IT, utan endast vilken medvetenhet som krävs. Det har sin motivering i uppsatsens syfte för att bättre kunde visa på dagens argumentation från alla respondenter i sjukvårdsorganisationer inom primärvården, länssjukvården och regionsjukvården samt molntjänstleverantörer som hanterar patientdata. En medveten kritisk aspekt till denna population var att IT-ansvariga inte alltid behöver vara registrerad som IT-ansvarig utan kan vara tilldelad det ansvaret bredvid sin huvudsakliga befattning vilket gör populationen svår att identifiera. (Oates, 2005, s.96)

Uppsatsen innefattar ett icke-slumpmässigt urval. Det valdes eftersom det inte fanns resurser eller tid för att genomföra ett slumpmässigt urval. För att ta fram urvalet ur populationen användes en subjektiv urvalsteknik då tekniken förlitar sig på forskarnas omdömesförmåga. Forskarna väljer ut studiens respondenter efter att hur väl de tror respondenterna kan besvara undersökningen ämne.

Det gör att resultatet oftast inte kan generaliseras men tekniken som används i uppsatsen gör att man får ett kvalitativt resultat och bredd i de olika ställningstaganden som finns bland sjukvårdsorganisationerna samt molntjänst-leverantörerna. Urvalet togs även fram genom ett bekvämlighetsurval där respondenterna utsetts efter studiens geografiska avgränsning, alltså i Uppsala och Stockholmsområdet. (Oates, 2005, ss.96–98)

3.2 Datainsamling

För att bidra med en vägledande studie krävs en förståelse för hur inställningen kring molntjänster är idag och vilka faktorer som faktiskt präglar besluten kring just molntjänster. Därför gjordes valet av att ha semistrukturerade intervjuer som datainsamlingsmetod. Främst på grund av att få en grundlig bild över hur IT-ansvariga ställer sig till frågan om just molntjänster. Valet att genomföra just intervjuer av semistrukturerad karaktär stöds främst av intresset att låta de intervjuade svara fritt på de öppna frågorna inom ramen för ämnet samt möjligheten för intervjuaren att ställa följdfrågor. På så sätt bevarades kontrollen över ämnet samtidigt som möjligheten för respondenten att ge nya vinklar gavs. De enstaka teman som förbereddes innan intervjuerna utformades utifrån en medvetenhet hos intervjuerna baserad på tidigare teorier inom ämnet. (Alvehus, 2013, s.83)

Respondenternas bakgrund presenteras under rubriken 4.1 Introduktion till resultat, i syfte att ge läsaren en tydligare struktur inför analysen. Det har fokuserats på att presentera respondenten personligen och inte dess organisation vilket har sin motivering i uppsatsens frågeställning som undersöker just IT-ansvarigas förståelse. Tabellen nedan visar de genomförda intervjuernas egenskaper:

Respondent	**Anonymitet**	**Ljudinspelning/ Fältanteckning**	**Tidsåtgång**	**Tillvägagång**	**Transkriberade antal ord**
A Per Akademiska	Nej	Fältanteckningar	1h 10min	Personligt möte	1178
B Ralph Karolinska	Nej	Ljudinspelning	1h	Personligt möte	6804
C Kim **City Network**	Nej	Ljudinspelning	45 min	Personligt möte	5469
D Per-Olof Tieto	Nej	Ljudinspelning	20 min	Telefonintervju	1067
E Hans Tieto	Nej	Ljudinspelning	20 min	Telefonintervju	1144

Tabell 1. Intervjuer

Enligt Dalen (2008, s.120) är det viktigt att datamaterialet blir relevant och fylligt då de ska ligga till grund för tolkning; "Datamaterialets validitet stärks genom att intervjuaren ställer bra frågor och ger informanterna tillfälle att komma med innehållsrika och fylliga uttalanden". Därför spelades intervjun in då respondenten gav samtycke till ljudupptagning. Det innebar möjligheten att lyssna på intervjuerna en andra gång vid analys av informationen. Samtidigt som det gavs en bättre möjlighet till större fokus på själva intervjun istället för att behöva föra fältanteckningar och därmed störa konversationen. Det gäller bara fyra av fem intervjuer, då en av respondenterna inte godkände en ljudupptagning under intervjun. Detta påverkar även resultatet då exakta citat från respondenten saknas.

Eftersom respondenterna måste ta hänsyn till den sekretess som måste hållas och dessutom de regler och riktlinjer som finns för att bibehålla säkerheten kan svaren påverkas av detta genom att bli begränsade. En annan viktig aspekt som är viktig att ta i beaktning och som kan ha påverkat både respondenter och den data som utvunnits är att det i år 2018, är valår. Det finns anledningar att tro att detta både kan påverka respondenter och deras organisationer då ingen varken vill säga för mycket eller vågar säga någonting. Detta går givetvis inte att säga definitivt men finns en möjlighet att faktorer som den skulle kunna påverka resultatet.

3.3 Kodning och teman

För att analysera de resultat som inhämtats via den valda datainsamlingsmetoden, vilken presenteras ovan i 3.2, har en kvalitativ dataanalys gjorts. Det har sin motivering i studiens forskningsstrategi då det används en intervjustudie som genererar kvalitativa data. Vidare motiveras denna analys i det valet av insamlingsmetod som beskriver hur icke-numeriska data ska insamlas, d.v.s. ljudupptagningar från intervju-inspelningar. (Oates, 2005, s.267)

I studien analyserades endast textdata. En förutsättning för att kunna analysera data är att den i största möjliga mån har samma format, därför var första steget att *förbereda datan*. Inspelningarna transkriberades då från intervjuer till text. Fördelen med att transkribera all data på samma sätt var då att all data blev likgiltigt format och lätt att se över. (Oates, 2005, ss.267) För den intervju som inte spelades in, fördes istället fältanteckningar som sedan skrevs rent. Vid transkriberingen formaterades empirin genom att pauser, brus och utfyllnadsord avlägsnades för att efterlikna ett mer strukturerat skriftspråk. En medveten risk vid denna typ av transkribering är att ljudinspelningarna samt fältanteckningarna blir förändrade då det som intervjuaren hör inte alltid överensstämmer med vad respondenten sagt (Alvehus, 2013, s.85). Därefter gjordes en *dataanalys* då första steget var att dela in datan i olika segment beroende på hur relevant informationen var för uppsatsen, alltså beroende på hur hög validitet datan hade för studien. Slutligen gjordes en *temanalys*, där de segmenten som var relevant för uppsatsen delades upp i teman utifrån uppsatsens teoretiska ramverk the McCumber Cube. (Oates, 2005, ss.268–270) Segmenten styrde vilka faktorer i the McCumber Cube som fokuseras i denna studie som sedan utgjorde uppsatsens tema. Våra teman är därför ett resultat av både ett induktivt och deduktivt synsätt.

3.4 Generalisering av resultat

För att undersöka resultatets kvalité och möjlighet till generalisering undersöktes dess reliabilitet och validitet. Vad gäller studiens reliabilitet är intervjuer som datainsamlingsmetod svåra att reprisera. Det eftersom intervjuaren är en så pass stor del av forskningsprocessen och påverkar studiens objektivitet. (Oates, 2005, s.198) Denna aspekt visar på svag generalisering möjlighet för studien, därför argumenteras vidare för studiens validitet.

Vid intervjuer är en förutsättning att intervjuaren och respondenterna har en intersubjektivitetförståelse. Det innebär att de har en gemensam uppfattning och tolkning om situationen. Vilket också är fallet i denna uppsats, då olika IT-ansvariga på organisationerna uppfattar molntjänster i relation till säkerhet på olika sätt. Intersubjektivitet innebär att intervjuarens tolkningar av respondenternas svar har hög validitet. (Dalen, 2008, ss.117–118) Denna aspekt har varit en viktigt vid studiens intervjuer. Därför har intervjuerna genomförts med en öppenhet gentemot den kunskap som respondenten besitter och alla intervjuer utom en har genomförts via ett personligt möte. Intervjuerna med vårdgivarna skedde även i respondenternas kontext för att nå en djupare förståelse. Kritik kan riktas mot den telefonintervju som gjordes eftersom det är svårare att få en gemensam intersubjektivitet över telefon vilken kan påverkat tolkningarna som gjorts utifrån denna. Det handlar även om *forskarens reflexivitet*, att forskare inte är neutrala i sin forskning utan kan hela tiden påverkas av sina egna antaganden, vilket oundvikligen kommer att forma forskningsprocessen. (Oates, 2005, s.292) Detta gäller främst den intervju som inte fick spelas in, då endast ett fåtal exakta citat finns med.

Urvalet i studien behöver också valideras för att möjliggöra en generalisering. Arbetet började med sökning efter flera respondenter där man eftersökte IT-ansvariga på alla de större vårdorganisationer runt om Stockholm och Uppsala. Men på grund av tidsbrist och lågt intresse hos efterfrågade respondenter, då endast 2 respondenter var villiga att delta, gjordes en bedömning av att även ta in respondenter som levererar molntjänster för att få ett bredare perspektiv. Det hade sin motivering i Dalen (2008, ss.118–119) som menar att ett kvalitativt urval bör vara baserat på individuella variationer som är relevanta för forskningsfrågan. Dalen (2008) bemöter kritiken om att “kvalitativa urval endast studerar ett fall och vars resultat kritiseras för att endast producera vägledning för det specifika fallet” och menar att generaliseringsbarheten för denna typ av urval ligger i mottagarens bedömning. För att mottagaren ska kunna värdera om uppsatsens resultat är tillämpbart i dennes vårdorganisation har uppsatsen presenterat relevant empiri som både beskrivits och tolkats. Då hela sjukvården hanterar patientdata samt har lagar och regler som gäller för hela branschen borde denna fallstudie även vara intressant för andra vårdgivare vilket skapar stora möjligheter för generalisering.

4 Empiri och Analys

I detta avsnitt presenteras resultatet från intervjuerna och är uppdelat i olika kategorier utifrån de teman som fanns vid intervjutillfället. Avsnittet presenterar inledningsvis en bakgrund av respondenterna och organisationerna och därefter följer respondenternas åsikter om molnet, definitionen av molntjänster och hur deras arbete kring detta ser ut idag. Beslutsprocessen kring just dessa beslut angående molnet, lagar och slutligen framtiden. Avslutningsvis presenteras den dokumentation som tagits del av från respondenterna.

4.1 Introduktion till resultat

Följande avsnitt kommer inledningsvis presentera de respondenter som deltagit och deras arbetsplats, vidare presenteras och analyseras empirin utifrån ramverket som tidigare introducerats.

Respondent A: Per Foyer
Roll: Respondenten arbetar som IT Security Specialist/Analyst på Akademiska sjukhuset. Respondenten har arbetat på Akademiska sjukhuset i 7 år.

Akademiska sjukhuset är ett länssjukhus, specialistsjukhus, utbildningssjukhus och forskningssjukhus beläget i Uppsala. Sjukhuset är en del av Region Uppsala och har 8300 anställda och ca 700 000 människor vårdas här varje år. (Akademiska sjukhuset, 2018)

Respondent B: Ralph Benton
Roll: Respondenten arbetar som Chef för Information och IT Säkerhet på Karolinska universitetssjukhuset. Respondenten har arbetat inom vården i ca 1 år och har tidigare vart CISO (Chief Information Security Officer) inom den privata sektorn.

Karolinska universitetssjukhus har ca 15 800 anställda och har ca 1 580 000 patientbesök varje år (Karolinska Universitetssjukhuset, 2018).

Respondent C: Kim Hindart
Roll: Respondenten arbetar som Chief Security Officer / Data Protection Officer på City Network som är en global leverantör av molntjänster för IT-infrastruktur, genom deras tjänst City Cloud. City Cloud erbjuds som både publikt och privat moln (City Network, *Om företaget*, 2018). City Cloud för Hälso-och sjukvård möjliggör att efterleva de krav och direktiv som ställs på hantering och säkerhet av exempelvis patientdata (City Network, *Hälso- och Sjukvård*, 2018).

Respondent D: Per-Olof Wadeborn
Roll: Quality Partner Industry Delivery på Tieto. Tieto är idag leverantör till samtliga landsting i Sverige och outsourcing-partner till Region Skåne och en handfull andra regioner. Hälso- och sjukvård är ett utvalt satsningsområde på Tieto, de har i ett nära samarbete med Region Skåne anpassat en av deras molnlösningar till att uppfylla de krav i form av lagar och policys som finns inom svensk hälso- och sjukvård. (Tieto, 2008)

Respondent E: Hans Berglund
Roll: Information Security Manager på Tieto (se information om företaget ovan).

4.2 Molntjänst - definition

För att kunna presentera och analysera empirin utifrån The McCumber Cube, det valda ramverket, och i sin tur svara på den huvudsakliga frågeställningen kommer respondenternas definition av molntjänster redogöras nedan.

> Ralph (Karolinska): "En molntjänst i form av data ligger hos en leverantör och man kan inte säga exakt vart datan ligger, man kan kanske säga att den ligger inom EU eller ligger inom Sverige men man kan inte säga att den ligger på just den servern som står där, så ser jag det".
>
> Kim (City Network): "Molntjänster är en outsourcing med en viss prismodell. Där finns de olika moln-koncept av de olika varianterna av molntjänster. Den ska ha stor access till många nät, den ska vara konsumerbar över internet, den ska ha någon form av resursmätning och en betalmodell i relation till en förbrukad kapacitet. Det även finnas en nivå av self-service där man ska kunna justera det här från en tid till en annan."
>
> Hans (Tieto): "Det finns flera sorter av molntjänster. Det finns både det man kallar för private cloud och publika molntjänster och publika molntjänster är mer traditionella som levereras från exempelvis Microsoft, Amazon och Google. Private cloud är det vi levererar inom våra egna datacenter."

Per (Akademiska) definierar molntjänst som data som man kommer åt vart som helst. Per-Olof (Tieto) förklarar det som att "Vi tar betalt för den kapacitet man använder, och kan skala upp och ner." Här ser man tydligt på hur respondenterna definierar begreppet vilket bidrar till validitet i resultatet, att de begriper molntjänster ungefär på samma sätt även om förklaringarna skiljer sig en aning.

4.3 Integritet

Per (Akademiska) uppger att det inte hanteras någon patientdata i någon molntjänst idag. Medan Ralph (Karolinska) förklarar att om det lagras någon känsliga data i molnet så är den informationen krypterad både under transport och lagring. Detta görs för att skydda integriteten hos deras patienter. Som tidigare nämnt, så finns det mycket som pekar på att molntjänster skulle effektivisera och förbättra hälso-och sjukvården och vårdforskning men detta måste göras utan att riskera patienternas integritet, detta menar bland annat Kuo (2011, s.1) och AbuKhousa, Mohamed & Al-Jaroodi (2012, s.626). Kim (City Network) säger att "Som individ ska man kunna förvänta sig att ens personuppgifter inte blir spridda utan att du själv valt att sprida dem och till vem man väljer att göra det." Alltså att man som patient måste kunna förvänta sig att ens uppgifter blir hanterade på rätt sätt, och att man som individ äger beslutet om vem som ska ha tillgång till vad. Ralph (Karolinska) tar upp ett exempel angående integritet, ett specifikt fall som hade hjälpt patienter på Karolinska något otroligt, då patienter idag behöver befinna sig på sjukhuset varje dag i sju veckor för att lära sig göra sin egen dialys. För att sedan regelbundet leverera minneskortet med den informationen till mottagningen. Här finns det enligt respondenten många patienter som skulle vara beredda att eventuellt riskera sin patientinformation, i hopp om att få ett mer normalt liv och istället kunna arbeta eller iallafall ha valet till att kunna arbeta.

> Ralph (Karolinska): “Men det kan vi inte göra, för lagligt sett är det inte okej, men man måste ju ha med sig det här. Därför berättar jag det, det blir ju bokstavligen en livsförbättring för människor”.

Här kommer, precis som respondenten säger, problemet att bara för att patienten är villig och är beredd på detta, finns det lagar som styr om det är lagligt eller inte. Vad som är svårt att avgöra är om det borde vore möjligt för patienten att kunna ge sitt samtycke och därmed eventuellt kunna riskera den integritet som lagarna finns där för att skydda. Ett antagande som kan göras är att det hela tiden är en avvägning mellan just integritet och deras uppdrag, att leverera bra vård. Ralph (Karolinska) lyfter ett annat intressant exempel som gäller ett projekt med, bland annat Karolinska sjukhuset, som rör balansgången mellan integritet och konfidentialitet. Nämligen den molntjänst som EU tagit fram för att samla specialister runt om i Europa för att kunna samarbeta för att kunna hjälpa varandra i vården trots att det inte är deras patienter. Samarbetet möjliggörs genom att patienten anonymiseras.

> Ralph (Karolinska): “Då kan man sitta och diskutera! En expert i Holland med en i Frankrike diskuterar den här enskilda patientens fall. Dom kanske har någon historisk bakgrund som vi inte upplevt här i Sverige ännu osv.?”

Respondenten menar att så länge tjänsten kan garantera de 15 krav på säkerhet som finns skapade (Bilaga 3) är detta vara genomförbart. Här handlar det om konfidentialitet, att patienten kan ge sitt consent och medger sitt samtycke till tjänsten och på så sätt kan specialister från hela Europa hjälpas åt för att kunna ge den bästa tänkbara vård till patienten. Enligt AbuKhousa, Mohamed & Al-Jaroodi (2012, s.622) kan delning av patienters data nämligen tjäna många olika syften som bidrar till att förbättra kvaliteten av vården men påstår att svårigheten med detta är att man då måste följa strikta regler för vem som delar, och hur väl patienters integritet upprätthålls. Här kan man anta att Sveriges sjukvård skulle gynnas mycket i och med den kompetens andra vårdgivare kan sitta på, samtidigt som Sverige också kan bidra med givande kunskap. Ett viktigt och innovativt samarbete som både kan vara berikande för patient och vårdgivare. Ser man till att följa de reglerna och att integriteten hos patienten upprätthålls antas tjänsten vara möjlig, men återigen finns det en balansgång, i detta fall mellan att leverera kvalitativ vård, konfidentialitet och integritet.

4.4 Konfidentialitet

En sak som både forskning och respondenter verkar hålla med om är att alla som hanterar patientdata står inför utmaningar. Per (Akademiska) menar att “De som arbetar på sjukhuset är hårt pressade och kan rimligen inte hålla koll på alla lagar och regler”. För att göra det enklare för de som arbetar på sjukhuset, menar Per (Akademiska) att den bästa lösningen vore att göra systemen vattentäta och lätta att använda, och därmed ska det vara omöjligt att kunna ladda upp och göra information synlig som inte ska vara det. Helt enkelt att det varken ligger i deras utbildning, arbete eller behörighet. Ralph (Karolinska) förklarar att “mitt jobb är att ta fram verktyg och processer som stödjer vården att, trots att man är världens bästa kirurg, också kan ta bra informationssäkerhetsbeslut”. Ralph (Karolinska) ser därmed lösningen på ett annat sätt och vill istället att med hjälp av beslutsstöd ska den anställde trots att den inte har utbildning inom ämnet, kunna ta kloka och beslut inom ramen för säkerhet. “Om du har ansvar över en viss sjukvårdsinstans på sjukhuset så måste du också ta ansvar över informationen och hur den hanteras.”

Per-Olof (Tieto) förklarar och menar att "det är en allmän utbildning, om man jobbar som exempelvis läkare eller sjuksköterska, och jag tror att det flesta vet om detta." Hans (Tieto) förklarar följande.

> "Det är alltid svårt att bygga bort allt sånt här genom system och kontroller. Ofta hamnar man ju alltid nån stans på personligt ansvar och styrande policys som man tagit fram i en vårdorganisation. Tror det blir väldigt svårt att bygga bort det helt, misstag kan folk alltid göra."

Forskning säger istället att det är någonting många valt att inte hantera, att det ligger utanför deras händer. Medan författarna (Löhr, Sadeghi & Winandy, 2010, s. 223) själva menar på att den anställde, som vanligtvis inte har den sorts kompetens och tid att professionellt kunna hantera systemen, bör vara tillräckligt skyddad för att kunna arbeta utan att riskera att information hanteras fel. Här finns det tydligt delade meningar, detta gör att det är svårt att definitivt säga vems ansvar detta ligger på och vad som är lösningen på problemet, om det nu ens är ett problem, då Per-Olof (Tieto) istället tror att de flesta inom området redan är medvetna om detta och hanterar det på rätt sätt. Enligt tidigare forskning ligger det största problemet möjligen i att ingen egentligen vill ta ansvaret. Men precis som Hans (Tieto) påpekar, kan man anta att det kommer vara väldigt svårt att bygga ett system som helt ska förhindra att den anställde kan göra ett fel, det håller även Kim (City Network) med om som tror på ett delat ansvar:

> "Jag tror mer på ett system som stödjer ett processtänk än att systemet måste vara teknisk säkert i alla lägen. För i slutändan kommer du aldrig ifrån att ett processtänk krävs då det finns en mänsklig integration... "

Samtidigt som forskning verkar trycka på, med medhåll av Per (Akademiska), att det ändå bör vara möjligt. Man kan anta att respondenternas svar skiljer sig så pass mycket på grund av flera anledningar, såsom erfarenheter och verksamhetsinriktning.

Samtliga respondenter, tidigare forskning och dokumentation pekar på att det är viktigt att loggning sker regelbundet och att man endast ska ha tillgång till informationen som krävs för genomförandet av de anställdas arbetsuppgifter. Detta nämns bland annat väldigt tydligt Region Uppsalas "*Riktlinjer för IT-säkerhet inom Region Uppsala"* som ligger bifogad som Bilaga 2 (s.17–19).

> "Medarbetare och konsulter inom Region Uppsala ska endast ha tillgång till den information som krävs för genomförande av deras arbetsuppgifter. Obehöriga personer ska inte kunna få åtkomst till och kunna modifiera, eller använda, en informationstillgång, och obehöriga användaraktiviteter ska kunna upptäckas."

Se även, "Loggning ska ske på alla system och elektroniska lagringsplatser där verksamhetskritisk eller annan känslig information lagras." Här nämns också att tilldelningen av privilegierade behörigheter, såsom administrativ åtkomst, ska begränsas så långt som det är möjligt. (Bilaga 2, ss.17–19) Trots att många molntjänsteleverantörer kan erbjuda säkerhetsåtgärder, som till exempel loggning, anser ändå AbuKhousa (2012, s.626) att det finns mycket arbete kvar att göra för att öka säkerheten gällande just detta. Här kan man anta utifrån både respondenter och tidigare forskning att det är viktigt att fastställa loggning för att ha kontroll på vem och när någon kommer åt informationen.

Sultan (2014, s.183) påstår att mycket forskning menar att små lokala molnleverantörer uppfattas som mer tillförlitliga och mer betrodda än stora mer väletablerade företag. De menar att den största utmaningen inte är att anta en molnlösning, utan att välja rätt molnleverantör. Ralph (Karolinska) förklarar att "Vi använder oss av ett regelverk som ska gälla för alla system, sen är det upp till leverantören att leva upp till detta regelverk i molnet". Ralph (Karolinska) menar alltså på att det endast handlar om att leverantören kan uppfylla ramverket för den säkerhet som organisationen kräver och så länge dem gör det, så är molntjänster möjligt inom säkra gränser. Kim (City Network) menar att "Sjukvården kan absolut använda molntjänster, men kanske inte med de vanliga standardavtalen. Man måste skapa rätt förutsättningar och sätta bra avtal."

> Ralph (Karolinska): "Vad är det som säger, att bara för att det råkar stå i någon hall i Solna, Kista eller någon annanstans i Sverige, att det är säkrare än i molnet? Dock kan det vara andra sorters risker. Det handlar om att man måste göra en bedömning."

Ralph (Karolinska) menar på att det inte behöver betyda att det är mer säkert att själva sitta på servern än att man hyr ut den delen av arbetet och låter någon annan hantera servern i deras lokaler. Att det egentligen grundar i en bedömning som måste göras, frågan är vem som gör den. Kim (City Network) påpekar att så länge bra och grundliga avtal sätts är det fullt möjligt för sjukvårdsorganisationer att kunna lita på en tredje part. Gorelik (2013, s.24) påstår, precis som Ralph (Karolinska), att det inte finns belägg för att garantera att data skyddas bättre internt jämfört med ett publikt moln. Att det till och med kan vara mer säkert i ett publikt moln, detta eftersom molnleverantörer kan utgöra en högre grad av kompetens när det kommer till säkerhet än sina kunder.

Här kan man anta att det finns mycket delade meningar, i och med att respondenters åsikter och den tidigare forskning som inhämtats. Viss forskning pekar på valet av att välja molnleverantör är utmaningen, medan annan forskning menar att det finns möjlighet att det finns bättre kompetens hos leverantören. Ralph (Karolinska), som menar på att det viktiga är att kraven uppfylls och utförliga avtal sätts. Alltså kan man anta att just möjligheterna och risker med outsourcing till en tredje part uppfattas och hanteras på väldigt olika sätt, även om gruppen av respondenter är liten och inte kan styrka någonting definitivt.

På grund av den sekretess som gäller då man hanterar känsliga data har inte de respondenter som representerar sjukhusen (Per, Akademiska & Ralph, Karolinska) möjlighet att svara på frågan om administratörer, hos exempelvis molnleverantörer, eller på själva vårdorganisationen har tillgång till informationen som lagras. Per-Olof (Tieto) menar att det inte är ett problem "då man kan ha verktyg som spelar in, vad du än gör så registreras det." Likadant påpekar Kim (City Network) och Hans (Tieto).

> Kim (City Network): "Man har en spårbarhet som motsvarar det man ska förvänta sig i sjukvården dvs. att man kan se vem som tittar och varför (motsvarande polisregistret) man får ju inte göra saker i nyfikenhet utan endast med ett giltigt skäl."

> Hans (Tieto): “I vissa fall behöver admin åtkomst till informationen för att kunna sköta sitt jobb, och det är egentligen det som är nyckeln. Behöver jag åtkomst till det här i mitt dagliga arbete eller inte? Inte, då ska man absolut inte ha den åtkomsten.”

Respondenterna som levererar molntjänster dvs. Per-Olof (Tieto), Kim (City Network) och Hans (Tieto) tog lättare fasta på frågan och diskussionen kring huruvida en administratör kan se datan eller inte. Per-Olof (Tieto) och Kim (City Network) hänvisar återigen till att det är därför loggningen är så pass viktigt. Här kan man göra antaganden om att inte all information idag är krypterad och att administratörer därmed kan se datan, men att de inte har rätt att tillgå informationen så länge inte de krävs för deras arbete.

4.5 Lagring

Det finns tydliga samband nämnt både av tidigare forskning och svar från respondenter gällande lagring, nämligen att om det är känsliga data som lagras måste datan alltid vara tillräckligt skyddad. Detta menar Löhr, Sadeghi och Winandy (2010, s. 223) och även både Per (Akademiska) och Ralph (Karolinska). Hur man skyddar data och vad som anses som tillräckligt skyddad är svårare att definiera utifrån datautvinningen. Enligt Löhr, Sadeghi och Winandy är ett sätt att skydda datan genom kryptering, det menar också Zissis & Lekkas (2010, s.588).

> Per (Akademiska): “Man kan se två typer av molnlagring som är möjliga i sjukvården, dels där datat i sig är oskyddat men anonymiserat genom till exempel personnummer lagrat som hash-värden och dels så kallad zero-knowledge-lagring där allt data krypteras hos den som ska lagra innan det åker upp i molnet, och dekrypteras efter att det hämtats.”

Detta styrker också Per (Akademiska) som argumenterar mycket för Zero-Knowledge i en molntjänst, som bygger på samma idé, att molnleverantören inte ska kunna ta del av informationen som lagras. Detta görs genom att all information krypteras och konceptet bygger på att datan krypteras redan innan den lämnar sjukvårdens servrar, och detta påstår Per (Akademiska) minskar riskerna både vid lagring och transport av data till molnet. Ralph (Karolinska) nämner också på att kryptering vid både transport och lagring är en förutsättning för att skydda informationen, detta med hänvisning till dokumentationen (bilaga 3) i form av de krav som satts upp av respondenten. En reflektion kring zero-knowledge är att data som lagras i molnet fortfarande är lika värdefull för sjukhuset oavsett om den är krypterad och oläslig för andra vilket fortfarande gör sjukvården känslig för utpressninngsprogram eller liknande. En ytterligare reflektion är att krypteringsnyckeln ger tillgång till livsnödvändig information och om den endast är i besittning en part ökar riskerna ifall att nyckeln förloras.

> Kim (City Network): “Enskild kryptering är jättesmidigt då man håller den enskilde administratören från att i klartext kunna se data. Men hur övervakar man då i sin tur att vårdpersonalen, och dem som har nyckeln i andra änden, inte gör någonting? Jag tror absolut på en krypterad lösning men jag tror också på det här med split responsibility. “

Även Kim (City Network) talar för kryptering, men påpekar tron för delat ansvar. Det man kan anta utifrån svaren är att det finns en gemensam mening om att kryptering är ett sätt att skydda data och som måste kunna säkerställas för att kunna lagra information i molnet. Men egentligen inte hur det bör ske, om det egentligen är det bästa sättet eller om det är tillräckligt för att helt eliminera risken att lagra känslig information i molnet.

Det finns flera möjligheter när det gäller kryptering men enligt Per (Akademiska) finns också risken och med en privat krypteringsnyckel. Nyckeln kan försvinna eller komma i orätta händer och den svåraste utmaningen att få tillbaka informationen utan att riskera dess riktighet. Enligt Gorelik (2013, s.24) är det inte en självklarhet vem som äger nyckeln utan om en molnleverantör inte ska ha tillgång till uppgifterna är det viktigt att säkerställa att nycklarna endast innehas av det företag som äger uppgifterna. Detta tar även Ralph (Karolinska) upp då det är viktigt att avgöra, vem som sitter på nyckeln.

> Ralph (Karolinska): "Vem sitter på nyckeln? Det är väldigt viktigt att avgöra. Om man då har en egen krypteringsnyckel så har man ju en helt annan möjlighet att kunna påverka skydd av din information i en molntjänst".

Ralph (Karolinska) menar att om man har en egen krypteringsnyckel så har man en helt annan möjlighet att kunna påverka skydd av informationen i en molntjänst. På samma sätt menar Hans (Tieto), att "Nyckel-ägarskapet ska tillfalla den som äger informationen, alltså i det här fallet, vårdgivaren." Utifrån både forskning och intervjuer kan man anta att om man väljer användning av en molntjänst där man krypterar datan så är det viktigt att sjukvården själva sitter på krypteringsnyckel och att leverantören därmed inte ska ha tillgång till datan.

Enligt Armbrust et al., (2010, s.55) är inlåsning ett stort riskområde då det inte finns några utformade standarder. Bilaga 2: "Det ska finnas export funktioner i tjänsten så att Region Uppsala vid avtalsslutet, eller i övrigt vid behov, lätt kan byta leverantör." Detta ser Per (Akademiska) på med stort allvar precis som nämndes ovan, att man måste ha en plan för att få tillbaka informationen. Det presenteras också tydligt i den dokumentation som mottagits från Per (Akademiska), "*Riktlinjer för IT-säkerhet inom Region Uppsala* " (bilaga 2, s.10), att det ska finnas export funktioner i tjänsten så att Region Uppsala vid avtalsslutet, eller i annat behov, lätt kan byta molnleverantör.

> Ralph (Karolinska): "Man måste våga ställa den frågan. Om vi inte är nöjda om ett halvår, hur gör vi då? Det kanske poppar upp en bättre molntjänst, har vi inte då tänkt hur vi backar ur den vi har då kan vi ju sitta där."

Likadant påpekar Ralph (Karolinska) som menar att det är viktigt att undersöka möjligheten för att backa från ett beslut med molnleverantören. Armbrust et al., (2010, ss.54–55) menar att de utmaningar och svårigheter med att extrahera data från molnet förhindrar vissa organisationer från att anta molntjänster. Det menar dock Ralph (Karolinska) inte heller kan hindra en, utan att ett avtal är ett avtal, och att det istället handlar om att ha en plan för att kunna backa och inte förkasta hela molntjänsten på grund av den rädslan. Utifrån både vad respondenter och forskning säger kan man anta att det är viktigt att ha en back-off plan. Även om respondenterna inte kan spegla andra organisationer, kan man ändå anta att organisationer såsom sjukhus verkligen skulle gynnas av att ha det, både för att bibehålla konfidentialitet och integritet, men också ur ett kostnadsmässigt perspektiv.

4.6 Lagar/ Riktlinjer

Per (Akademiska) säger att lagar och riktlinjer har stor inverkan på beslutsfattande vid hantering av patientdata i molntjänster. Även tidigare forskning styrker att jurister har stor inverkan vid utvecklandet av molntjänster. Eriksson och Goldkuhl (2013, s.174) lyfter att juristers tolkningar av lagen har stort inflytande vid utvecklingen inom den publika sektorn. Ett antagande är därför att lagar och riktlinjer präglar hanteringen i stor grad.

> Ralph (Karolinska): "Vart står det i lagen att man inte får använda sig av molntjänster?... Det är ju samma lag, hur kan det finnas så många olika tolkningar?"

Ralph (Karolinska) belyser också lagarnas inverkan och att de kan skiljas. Enligt Armbrust et al., (2010, s.55) finns inga utformade standarder för molnet. Det har även Kim (City Network) iakttagit och tycker att riskanalyser borde vara en enhetlig standard för alla sjukvårdsorganisationer, och att det idag saknas. Han menar också på att det borde finnas en rådgivande myndighet, istället för en granskande.

Ralphs (Karolinska) resonemang påvisar hur Skåne Regionen, Kry och doktor.se har haft jurister som tolkat lagen som främjande för molntjänster och Stockholms läns landsting har haft jurister som tolkat lagen till en mer restriktiv användning av molntjänster inom vården. En ytterligare tes är därför att dessa tolkningar både kan begränsa och främja sjukhusens implementation av molntjänster. Kim (City Network) talar om bristen på vägledande kunskap och att myndigheterna endast granskar vårdorganisationen. En analys är därför att det borde finnas gemensamma riktlinjer för sjukvården för hur patientdata bör hanteras i molntjänster vilka borde framtagna från en svensk myndighet som har syfte att endast rådgiva sjukvårdsorganisationerna. Kim (City Network) berättar att Patientdatalagen inte omfattar outsourcade It-tekniker vilket patientdatalagen styrker i första kapitlet första paragrafen där det specificeras att lagen endast gäller för vårdgivare. Det kan därför antas att lagarna behöver korrigeras så att alla med tillgång till patientdata ska stå under samma straffrätt.

Enligt definitionen av Cloud Act är leverantörer av molntjänster skyldiga att bibehålla, säkerhetskopiera och tillhandahålla information till den amerikanska staten som gäller en patient, oavsett om informationen finns inom eller utanför USA (H.R.1625, 2017–2018). Per (Akademiska) uppger att lagen gjort så att sjukhuset var tvunget till att punktera några av dess pågående projekt. Ralph(Karolinska) ställer sig istället avvaktande till effekterna av lagen och valde endast att fördröja de berörda projekten tills vidare. Det som behöver tas i beaktning är att vid tiden för intervjun så nämner båda respondenterna att de precis blivit informerade om den nya lagen, vilket antas haft påverkan på respondenternas svar och deras agerande. Då lagen precis införts finns ingen tidigare forskning om hur den kommer påverka de svenska myndigheterna. Per (Akademiska) antar att flera av de befintliga systemen som organisationen använder kan komma att behöva undersökas i en grundläggande riskanalys. Ralph (Karolinska) reflekterar istället om hur lagar som denna kan få slagkraft och spridning till andra ledande stater. Något som respondenterna båda uppmärksammar är att de upplever en generell naivitet i förhållande till Cloud Act. Därför kan en tes vara, i förhållande till respondenternas antaganden, att lagen behöver utredas i enlighet med deras framtagna säkerhetsriktlinjer se Bilaga 1 samt Bilaga 2 sättas i förhållande till PUL och GDPR som reglerar överföring av uppgifter till Tredje land.

Ralph (Karolinska) menar att ledande stater kan ta beslut om lagar som får effekt för sjukvårdens molntjänst då molntjänstleverantörer kan lyda under globala lagar vilket han menar är molntjänsters akilleshäl. Ett antagande är därför att Cloud Act kan få spridande effekt och att det eventuellt kan förväntas liknande lagar från andra stormakter som Ryssland och Kina. Det antagandet har även stöd i GDPR som har som skäl att underlätta för överföringar till tredjeland (europaparlamentets och rådets förordning, 2016/679, skäl 6) vilket innebär att den kommer kunna bana väg och förenkla vid införandet av lagar i samma slag som Cloud Act.

4.7 Tillgänglighet

Utifrån datautvinningen ser man tydliga påståenden från både Per (Akademiska) och Ralph (Karolinska) att e-hälsa och en digital mötesplats för att leverera vård är en nödvändighet. Per (Akademiska) menar att anledningen till detta är främst för att patienter ska slippa väntetid och att man då kan optimera tiden mellan patienterna vilket i sin tur då effektiviserar arbetet.

> Ralph (Karolinska): “Om vi då kan göra sjukvården digital och kunna träffa patienten hemma hos dem så kan man bättre uppfylla det uppdrag som karolinska har, nämligen att vara ett specialistsjukhus. Jag är helt övertygad att vi måste ha en digital mötesplats för att vården ska mäkta med... vi måste gå åt det hållet. För det är inte längre en fråga OM.”

> Kim (City Network): “Det kan centralisera kompetensen mycket mer, även på ett globalt perspektiv. Har man en ganska ovanlig sjukdom så är det klart att det är jättebra om du snabbt kan kommunicera med specialisterna.”

Ralph (Karolinska) trycker också på samma punkter, att e-hälsa möjliggör stora bekvämligheter för användarna då de slipper sitta och vänta på exempelvis akuten, och därmed effektivisera vården. Även Kim (City Network) menar att e-hälsa antagligen kommer öka betydligt eftersom människor bara blir mer digitala i vår vardag, och att detta är en möjlighet främst inom forskning. Respondenten ser också potential i att genom e-hälsa, kunna leverera bättre vård då man lättare kan ta del av andras kunskap. Respondenten tror dock att det kommer dröja innan sjukvården hittar lösningar och att det istället kommer vara andra branscher som hinner först.

> Per-Olof (Tieto): “Utmaningen är att man mer tillhandahåller den här typen av digitala tjänster med ett integritetsskydd för den enskilde. Det är en väldig utmaning och viktigt att man kan leva upp till det och att människor kan känna sig trygga.”

Det som måste tas i beaktning här är säkerhetsaspekter, precis som Per (Akademiska) menar är det viktigt både för patient och vårdgivare att kunna validera sin identitet. Detta handlar både om integritet och konfidentialitet, att man som patient och vårdgivare kan vara säker på vem man faktiskt pratar med. Detta menar även Per-Olof (Tieto). En annan aspekt som Per (Akademiska) tar upp är den kontroll som behövs göras på datatrafiken, om leverantören kan garantera att data endast trafikeras inom EU? Utifrån forskning som ändå pekar på att någon sorts e-hälsa som exempelvis e-hälsa är ett steg som behöver och kan tas, samt det som sagts från respondenterna kan man anta att detta är framtiden, att inom en snar framtid kommer sjukhusen behöva möta sina patienter även på en digital plattform. I och med att antalet

respondenter är få och endast representerar respektive sjukhus och två olika molnleverantörer är detta antagande inte definitivt, men å andra sidan kan man säga att det finns tydliga stöd för att säga att just Karolinska sjukhuset och Akademiska sjukhuset kommer att ta initiativ för en digital mötesplats för att möta deras patienter, om detta steg ännu inte redan kan ses som taget.

4.8 Utbildning/Transmission/ Bearbetning/Teknologi

Det teoretiska ramverket som empirin analyserats utifrån lyfter även aspekter inom utbildning, transmission, bearbetning och teknologi. Dessa värdeord har inte funnits i fokus vid tidigare forskning eller vid respondenternas svar. De uppkom i viss mån vid datainsamlingen men blev då framförda som bakomliggande faktorer som styrkt de tidigare nämnda fokusområden integritet, konfidentialitet, lagring, lagar och riktlinjer samt tillgänglighet. Det har sin motivering i följande exempel:

Kim (City Network) anser att vårdgivare behöver utbildning för att öka medvetenhet kring hanteringen av patientdata i systemet men syftar på att skydda konfidentialitet hos patientdata. Fortsatt hänvisas till Per (Akademiska) och Ralph (Karolinska) som diskuterar behandling av data i Cloud Act. Per (Akademiska) berättar att all data som är lagrad i molnet hos börsnoterade amerikanska företag kan komma att behandlas av de amerikanska myndigheterna “Kan det kanske till och med påverka sjukhusets Office-lösning?” Ralph (Karolinska) fortsätter: “...Cloud ACT, den har ju ställt allting på sin spets, men än så länge vet vi inte riktigt vad den kommer innebära för oss, gäller den bara för amerikanska medborgare?” Respondenternas syfte är dock inte hur data behandlas utan de vill istället uppmärksamma problematiken kring hur integriteten av patientdata påverkas.

Ovanstående exempel påvisar ett antagande om att de värdeord som fokuseras mest, integritet, konfidentialitet, lagring, lagar och riktlinjer samt tillgänglighet, även är de som främst präglar respondenternas hantering av patientdata i molntjänster. Att dessa ord främst stod i fokus och inte de andra är inte överraskande i och med det valda ämnet, att vad som är speciellt är att det rör patientdata, som räknas som känslig data. Därför är det väldigt naturligt att det läggs mycket vikt kring just integritet och konfidentialitet.

Anledningen till att teknologi inte fått större fokus i uppsatsen antas vara av två anledningar. Främst att respondenterna på grund av sekretess inte kunnat delge sig av specifik information kring detta. Därför har frågor som rör t.ex. hur sjukvården hanterar deras servrar, istället fått tillhöra avsnittet som rör lagring. Även om detta även hade kunnat lyftas som mer tekniskt. Den andra anledningen för att detta inte ansågs stå i fokus för att kunna besvara frågeställningen.

5 Avslutande del

I detta avslutande kapitel presenteras de slutsatser som tagits och den vägledande kunskap som tagits fram. Slutligen görs en reflektion av arbetet och förslag på vidare forskning presenteras.

5.1 Slutsats

Kapitlet redovisar resultatet och besvarar den frågeställning som ställts.

Hur förstår IT-ansvariga på sjukvårdsorganisationer i Sverige molntjänster och vilka faktorer är det som präglar användandet ur ett säkerhetsperspektiv för patientdata?

5.1.1 Hur förstår IT-ansvariga på sjukvårdsorganisationer molntjänster

Utifrån den fallstudie som gjorts kan det konstateras att IT-ansvariga inom sjukvårdsorganisationen samt IT-ansvariga inom molntjänstleverantörer gemensamt ser en ökad användning av molntjänster i vården framöver. Användandet kommer både vara i ett forskningssyfte och för att möta patienters behov. Alltså kan man dra slutsatsen att IT-ansvariga på sjukvårdsorganisationer ser positivt på molntjänster även om de fortfarande finns ett kritiskt tänk för att vara säkra på att de bibehåller säkerheten. För att kunna möta respondentpatienters behov verkar också IT-ansvariga både inom sjukvården och som molntjänstleverantörer överens om att sjukvården kommer behöva möta deras patienter på en digital plattform. De ställer sig positiva till tanken och ser både att detta är en möjlighet för dem själva och patienten. Trots att de också ser utmaningar i att kunna validera vårdgivaren och patienten, samt att lyckas hålla den kontroll över vart deras datatrafik befinner sig i samband med just digital vård.

Molntjänster blir allt vanligare och samtidigt som detta intresse och förståelse hela tiden ökar verkar de IT-ansvariga vara överens om att det krävs tydliga gemensamma riktlinjer för hur man ska sjukhusorganisation ska tänka vid beslutstagande om molntjänst, vilket idag saknas. Det är av intresse att en myndighet upprättas för att ta fram dessa lagar och riktlinjer i syfte att vara rådgivare och inte granskande. Sammanfattningsvis dras slutsatsen att i de stora hela ser IT-ansvariga på sjukvårdsorganisationer molntjänster som en möjlighet och en väg som de måste tas. Men att det gäller att göra det på rätt sätt, samtidigt som det råder brist på nationella standarder, lagar och riktlinjer om hur man som vårdorganisation ska göra användandet av molntjänster möjligt utan att riskera säkerheten.

5.1.2 Vilka faktorer präglar användandet ur ett säkerhetsperspektiv för patientdata

För att besvara andra delen av frågeställningen resulterar uppsatsen i sex punkter som präglar hantering av patientdata i molntjänster som presenteras nedan. Dessa punkter har analyserats fram genom ramverket The McCumber Cube och är en sammanställning av de aspekter som iakttagit vara gemensamt viktiga hos respondenterna och tidigare forskning. Det är därför en slutsats att dessa punkter är av stor vikt för målgruppen att överväga vid beslutstagande.

1. **Loggning**

För att se till att patientens integritet och att reglerna kring konfidentialitet bibehålls krävs det att loggning sker. På så sätt håller man kontroll över hur datan hanteras och kan på så sätt spåra om hanteringen inte sker på ett korrekt sätt. Loggning bör göras på alla system och elektroniska lagringsplatser där patientdata lagras.

2. **Kryptering**

För en säker användning av molntjänst vid ett publikt moln krävs det att man krypterar informationen både under transport och lagring. Nycklarna ska endast tillgå de som äger informationen, vilket i detta fallet är sjukvårdsorganisationen. För att garantera säkerhet när man dekrypterar är den ultimata lösningen att det ska krävas två nycklar. Det kan leda till ytterligare säkerhet om dessa nycklar dessutom ligger hos olika organisationer.

3. **Vattentäta system**

I den mån som det går borde det inte vara möjligt för de anställda att hantera datan på ett icke-korrekt sätt. Därför bör man utforma och skapa system som är vattentäta och väldigt enkla att använda. En anställds, t ex läkare/sjuksköterskors uppdrag handlar om att ta hand om patienten, inte säkerheten av IT. Alltså kan man inte räkna med att de anställda sitter på en sådan kompetens. Detta är en stor utmaning att lösa, men att detta hanteras i mån som är möjligt bör vara givet för att underlätta för anställda och minimera de risker som finns.

4. **Lagar**

Alla som behandlar patientdata i molnet bör svara till samma lag för att patientdata ska hanteras i molntjänster. Lagar har stor inverkan i beslutstagande och därför är det viktigt att vara medveten om dessa. Cloud Act kommer påverka möjligheten för molntjänst i vården och bör påverka valet av molntjänstleverantör. Då både Cloud Act och GDPR möjliggör för utbyte av patientdata mellan länder kan det förväntas fler lagar som dessa vilket kräver en konstant kritisk inställning till dessa.

5. **Tillgänglighet**

Det måste sättas upp tydliga krav på vad som krävs av vårdorganisationen när det gäller tillgänglighet, som leverantören dessutom måste kunna garantera under hela avtalets tid.

6. **Leverantörsinlåsning (back-off plan)**

När man ingår i ett avtal med en molnleverantör måste man se till att det avtalet täcker vad som händer då tjänsten avslutas. Detta för att förhindra leverantörsinlåsningar och att man säkerställer att ingen data sparas hos leverantören.

5.2 Diskussion

I följande kapitel presenterar en reflektion kring uppsatsens resultat, och avslutas med en diskussion om eventuell vidare forskning.

5.2.1 Reflektion

En diskussion kring mängden respondenter har tidigare redogjorts i metodavsnittet men för att ge en rättvis bild även till resultatet, påpekas detta ytterligare då det finns det nackdelar i att respondenterna är relativt få och inte representerar ett större omfång. Detta på grund av att deras svar också stundom var spridda, vilket kan ha sin förklaring i respondenternas arbetsplats och arbetsuppgift. Ämnesområdet är dessutom väldigt brett och komplext, därför har det varit svårt att under en kortare tidsperiod, motsvarande som en C-uppsats innefattar, granska området med ett sådant djup som skulle behövas för att med säkerhet kunna dra mer exakta slutsatser kring ämnet. Uppsatsens resultat kan därför av många anledningar inte presenteras som generellt med tanke på den kritik som lyfts angående både genomförande och resultat utifrån de intervjuer som gjorts.

Som forskare av denna uppsats kan man se fördelar med valet att använda både en deduktiv och induktiv ansats även i resultatet. Anledningen till detta är de följdfrågor som kunde ställas då det är ett väldigt brett ämne, med teman som var väldigt öppet för respondenten att tala fritt. Samtidigt som inverkan på svaren från respondenterna kunde göras så lite som möjligt för att på så vis verkligen se till respondenterna gav svar på hur de ser på molntjänster.

Generaliseringsbarheten anses vara begränsad till sjukvården eftersom uppsatsen fokuserar på hantering av patientdata och inte av personuppgifter generellt. En fokusering på patientdata utmärker sig bland annat eftersom det finns ytterligare lagar att följa utöver PUL och GDPR dvs. Patientdatalagen. Denna fokusering är även en motivering till uppsatsens unikhet och dess bidragande till dagens forskning.

5.2.2 Vidare forskning

Då denna kvalitativa fallstudie medfört ett resultat som anses vara begränsat för studiens respondenter bör vidare forskning undersöka större generaliseringsmöjligheter, som att generalisera över den hela svenska vården, genom att utvidga denna fallstudie till större områden och fler aktörer.

En möjlighet som sjukvårdsorganisationer idag är i behov av är, som tidigare nämnt, enhetliga standarder och riktlinjer att följa, att en myndighet finns till för hjälpande och rådgivande syfte istället för granskande. Detta leder in på förslag på vidare forskning i ämnet, att utöka bredden och djupet vidare från denna uppsats och göra en inriktning mer på hur vårdorganisationer bör agera gentemot molnleverantörer ses både som en eftertraktad och välbehövd undersökning. Vidare skulle en undersökning som tar upp ett "före och efter"-perspektiv hos sjukvårdsorganisationer, både vara intressant och givande. Då med en frågeställning som syftar till att besvara om organisationen upplevs som bättre efter införandet av molntjänst i förhållande till säkerhet.

Referenser

AbuKhousa, E. Mohamed, N. & Al-Jaroodi, J. (2012) *E-Health Cloud: Opportunities and Challenges.* Faculty of Information Technology, United Arab Emirates University (UAEU)

http://www.mdpi.com/1999-5903/4/3/621

Akademiska sjukhuset. (2018). *Om Akademiska*. Hämtad 21 maj 2018 från http://www.akademiska.se/sv/Om-Akademiska/

Alvehus, J. (2013). *Skriva uppsats med kvalitativ metod: en handbok*. Stockholm, Sverige: Liber.

Armbrust, M., Fox, A., Griffith, R., D. Joseph, A., H. Katz, R., Konwinski, A., Lee, G., A. Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A View of Cloud Computing. *Communications of the ACM*, 53(4), 50 - 58.

Backman, J. (2008) *Rapporter och uppsatser.* 2nd ed. Lund, Sverige: Studentlitteratur.

Bushhouse, E. (2011). Cloud Computing. *Journal of Hospital Librarianship*, 11(4), 388-392. https://doi.org/10.1080/15323269.2011.611112

City Network. (2018). *Våra tjänster.* Hämtad 21 maj 2018 från https://www.citynetwork.se/

Congress.gov. (2018). *H.R.1625. (2017-2018) - Consolidated Appropriations Act 115th Congress.* Official website for U.S. federal legislative information. https://www.congress.gov/bill/115th-congress/house-bill/1625/text

Dalén, M. (2008) *Intervju som metod.* 1 ed. Malmö, Sverige: Gleerups utbildning.

Datainspektionen. (2018). *Patientdatalagen*. Hämtat 24 april 2018 från: https://www.datainspektionen.se/lagar-och-regler/patientdatalagen/

Europeiska unionens officiella tidning (27.4.2016) *Europaparlamentets och rådets förordning (eu) 2016/679*. Hämtat 06 maj 2018 från:

http://eur-lex.europa.eu/legal-content/SV/TXT/PDF/?uri=CELEX%3A32016R0679

Eriksson, O., Goldkuhl, G. (2013). Preconditions for public sector e-infrastructure development. *Information and Organization*, 23(3), 149–176.

Goldkuhl, G. (2011). *Kunskapande*. Institutionen för ekonomisk och industriell utveckling: Linköpings universitet. Institutionen för Data- och Systemvetenskap (DSV): Stockholms universitet. http://www.vits.org/publikationer/dokument/409.pdf

Gordon, D. (2016). Legal Aspects of Cloud Computing. i S. Murugesan, & I. Bojanova, *Encyclopedia on Cloud Computing* (ss. 462-475). John Wiley & Sons, Ltd.

Gorelik, E. (2013). *Cloud Computing Models - Comparison of Cloud Computing Service and Deployment Models.* Massachusetts Institute of Technology.

Hafiz. M, Johnson. R.E. (2006). *Security Patterns and Their Classification Schemes*. Illinois, USA: University of Illinois.

Halpert. B. (2011). *Auditing Cloud Computing: A Security and Privacy Guide*. New Jersey: John Wiley & Sons.

Hedin, A. (1996). *En liten lathund om kvalitativ metod: Med tonvikt på intervju*. (red.) Martin, C, (2011).

Karolinska Universitetssjukhuset. (2018). *Om oss*. Hämtad 21 maj 2018 från https://www.karolinska.se/om-oss/

Kuo, A. M.-H. (2011). *Opportunities and challenges of cloud computing to improve health care service*s. Journal of Medical Internet Research, 13(3).

Löhr. H, Sadeghi. A-R, Winandy. M. (2010). Securing the e-health cloud. *ACM International Health Informatics Symposium*, 220-229. Arlington, Virginia, USA. https://dl.acm.org/citation.cfm?id=1883024

McCumber, J. (2004). *Assessing and managing security risk in IT systems*. A Structured Methodology. CRC Press. https://ebookcentral.proquest.com/lib/uu/detail.action?docID=2010330.

Mell P; Grance T. (2009). *The NIST definition of cloud computing*. National Institute of Standards and Technology: Information Technology Laboratory. Version 15.

Microsoft Corporation. (2013). *Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet.* Remissvar SOU 2016:41. Hämtad 2 februari 2018 från http://www.regeringen.se/48f9c0/contentassets/a415dda1610244df9e94d58148c012fe/159microsoftbilaga3.pdf

MSB. (2013). *Vägledning – informationssäkerhet i upphandling*. Myndigheten för samhällsskydd och beredskap. https://www.msb.se/RibData/Filer/pdf/26589.pdf

Myndighetsdatalag. (2015). *Slutbetänkande av Informationshanteringsutredningen - SOU 2015:39.* Stockholm, Sverige: Statens offentliga utredningar.

Nationalencyklopedin. (u.å.). *Hälso- och sjukvård*. Hämtad 02 februari 2018 från: http://www.ne.se/uppslagsverk/encyklopedi/lång/hälso-och-sjukvård

Oates, BJ. (2005). *Researching Information Systems and Computing*, London: SAGE Publications Ltd.

Patientdatalagen. (2008). Svensk författningssamling (2008:355).

Shih. F.-J., Y-W. Fan, C.-M. Chiu, F.Ji. Shish, S.-S. Wang. (2012) The Dilemma of “To Be or Not to Be”: Developing Electronically e-Health & Cloud Computing Documents for Overseas Transplant Patients from Taiwan Organ Transplant Health Professionals' Perspective. *Transplantation Proceedings*, 44(4), 835-838. https://doi.org/10.1016/j.transproceed.2012.02.001

Sultan, N. (2014). Making use of cloud computing for healthcare provision: Opportunities and challenges. *International Journal of Information's Management*, 34(2), 177-184. United Kingdom: University Campus Suffolk. https://doi.org/10.1016/j.ijinfomgt.2013.12.011

Swedish Standards Institute. (2014). *Informationsteknik – Molnbaserade datortjänster – Översikt och terminologi (ISO/IEC17788:2014, IDT).* https://www.sis.se/api/document/preview/104900/

Tieto. (2008). *Trendbrott inom vården mot fler molntjänster*. Hämtat 24 maj 2018 från: https://www.tieto.se/trender-och-insikter/trendbrott-inom-varden-mot-fler-molntjanster

Whitman. M., Mattord H.J. (2012). *Principles of information security*. 5:th edt. Boston, USA: Cengage Learning.

Zissis. D, Lekkas. D. (2010). Addressing cloud Computing security issues. *Future Generation Computer Systems*, 28(3), 583 - 592. Aegean, Greece: Elsevier science bv. https://doi.org/10.1016/j.future.2010.12.006

Bilaga 1 - Intervjuguide

Uppsatsen har som syfte att öka förståelsen för om molntjänster bör användas av sjukvårdsorganisationer utifrån ett säkerhetsperspektiv och visa på dagens argumentation om fördelar respektive nackdelar.

Den frågeställningen som ligger till grund för uppsatsen är följande:

- *Hur förstår IT-ansvariga på sjukvårdsorganisationer i Sverige molntjänster och vilka faktorer är det som präglar användandet ur ett säkerhetsperspektiv för patientdata?*

Respondentens Namn:	Respondentens roll i organisationen:	Ljudinspelning:	Anonymitet:

Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet:
"*Organisationer inom sjukvårdssektorn pressas ständigt till att använda sina resurser så effektivt som möjligt. En lösning är ofta att använda mer IT och teknik för att effektivisera sin verksamhet. Samtidigt måste organisationer inom sjukvårdssektorn följa alla svenska bestämmelser kring integritet och säkerhet för hälsoinformation.*"
Teman:

Patientdata	Beslut om implementation	Ansvar
Sjukvårdssektorn pressas ständigt till att använda sina resurser mer effektivt. En lösning är molntjänster.	*För beslutsfattare inom sjukvården väcker molntjänster frågor om säkerhet.*	*Vissa menar att ansvaret för patientdata är "out of scope" för de som levererar slutanvändarsystemet.*
• Vad finns det för utmaningar/riskerna kring patientdata i molntjänster? Skiljer patientdata sig från andra data? • Går det att hantera patientdata i molntjänster idag? Hur? Kryptering? • Hur hanteras konfidentialitet i molntjänsten, hur ser behörighetsnivåerna ut med tillgången till patientdata? Vem har tillgång till krypteringsnycklarna?	• Vad ligger till grund för beslutsfattning? dvs. grundläggande krav från kunden? Loggning, spårning, garantier om datahantering inom gränserna? • Vad sätter gränsen för vad som är möjligt? Lagar/regler? Statliga/ privata vårdgivare? • Hur tror du att Cloud Act kommer påverka lagring av patientdata i moln? • Hur ser du på att patientdata kan komma att ligga hos tredje part i en molntjänst?	• Hur ser du på ert ansvar för patientdatasäkerhet som leverantör av molntjänster? • Ska ansvaret för patientdatasäkerhet ligga hos användaren eller systemet? • Hur kommer det framtida arbetet med implementationer av molntjänster i vården att se ut? • Hur ser ni på KRY, doktor.se osv? Varför har inte alla inom sjukvården en skype-tjänst eller liknande?

Microsoft Corporation. (2013). *Microsofts molntjänster & svenska krav på integritet och patientdatasäkerhet.* Remissvar SOU 2016:41. (hämtad 2018-02-02) http://www.regeringen.se/48f9c0/contentassets/a415dda1610244df9e94d58148c012fe/159microsoftbilaga3.pdf

Bilaga 2 - Dokumentation Region Uppsala

Riktlinjer för
it-säkerhet inom Reg

Bilaga 3 - Dokumentation Karolinska Sjukhuset

Minimum Security Requirements

1. **Authentication**
   - ☐ Multi factor authentication?
   - ☐ Unique and individual user accounts?
   - ☐ Password only known by user?
   - ☐ Authentication information stored encrypted?

2. **Access Management**
   - ☐ Routines for assignment, change and deletion of user access?
   - ☐ Regular reviews of accesses in the system?
   - ☐ Ensuring Need-to-know access?
   - ☐ Access to information only by EU citizen?
   - ☐ Automated log out from the system after certain time?
   - ☐ Access log report for each individual account?
   - ☐ System and service accounts blocked for interactive log on?

3. **Encryption**
   - ☐ Information encryption in transport to and from the system?
   - ☐ Information encrypted in rest (storage)?
   - ☐ TLS (Transport Layer Security)?

4. **Pseudonymisation**
   - ☐ Routines for ensuring pseudonymisation of information and data?

5. **Intrusion detection**
   - ☐ Regular checks of the security log?

6. **Traceability (logging)**
   - ☐ User identity stored in security log?
   - ☐ Read access is stored in security log?
   - ☐ Time for event is stored in security log?

7. **Security tests**
   - ☐ System is tested for vulnerabilities (OWASP Top 10/CWE/SANS Top25)?
   - ☐ Threat and vulnerability scans are regularly performed?

8. **Storage and Deletion of information**
   - ☐ Information and data stored within EU?
   - ☐ Ensuring that deleted data is completely removed and can't be restored?