Sammendrag

Ikke visste vel jeg da jeg begynte å skrive på denne oppgaven, at den skulle få en så uhyggelig aktualitet som den gjorde. Jeg ville se på informasjonssikkerheten i en tjeneste som var under utvikling, nemlig muligheten for videosamtale mellom AMK-operatør og innringer. Var det mulig å utvikle en slik tjeneste innenfor rammene av det eksisterende lovverket som ivaretar personvern og informasjonssikkerhet? Allerede i starten av mitt arbeid begynte det å ulme en global fare i Kina, en farlig pandemi var under rask utvikling. Og snart preget Corona-pandemien hele verdenssamfunnet, med nedstenging av hele samfunn som verden ikke har sett maken til i fredstid. Med denne isolasjonen tvang det seg frem nye måter å samarbeide på, for å holde samfunnet i gang.

De fleste av oss ble beordret til hjemmekontor over lang, lang tid. Vi ble nærmest over natten tvunget til å ta i bruk digitale kommunikasjonsplattformer, som kanskje ikke var dimensjonert for den omfattende bruken. Da vi stod i en situasjon som ikke var planlagt, bar kanskje innføring og bruk av nye samhandlingsplattformer preg også av dette. Etter kort tids bruk ble en klar over at disse nye samhandlingsplattformene kunne være en trussel for informasjonssikkerheten.

Så mens pandemien utfoldet seg der ute i den virkelige verden og kom stadig nærmere og nærmere, med alle de konsekvenser det hadde med seg, satt jeg og skrev om informasjonssikkerhet i en digital samhandlingstjeneste, videosamtale mellom AMK og innringer.

Mulighetene for og kravene om å ta i bruk ny teknologi i helsevesenet, har utfordret personvernet. I den perioden jeg har skrevet på denne oppgaven har der jevnlig vært rapportert om nye dataangrep, hvor uvedkommende har fått tilgang til eller prøvd å få tilgang til helsedataene våre.

Der er meldt om datainnbrudd og andre former for data-angrep både målrettet mot bl.a. sykehus og legekontor, men også angrep som treffer mer tilfeldig.

Helsevesenet skal fylle mange funksjoner og dekke mange behov. Jeg har i denne oppgaven sett nærmere på den prehospitale kjeden, som har ansvar for å bistå når akutte hendelser og kriser oppstår. Jeg har fordypet meg i informasjonssikkerheten i en tjeneste som muliggjør videosamtale mellom AMK-operatør og innringer.

For å få innsikt i hvordan AMK-tjenesten er bygget opp, hvilket ansvar og arbeidsoppgaver den enkelte AMK-operatør har, har jeg benyttet en ferdig utarbeidet behovsanalyse utført av Making Waves. Den har gitt meg verdifull innsikt i hvordan arbeidshverdagen til den som sitter og besvarer nødsamtaler kan arte seg.

Helsevesenet er underlagt mange lover og forskrifter. Den prehospitale kjeden har, i tillegg til ordinær helselovgivning egen forskrift som må overholdes. Dette er Akuttmedisinsk forskrift.

Også når det gjelder informasjonssikkerhet er der mange lover og regler som regulerer tilgang til helseopplysninger. Disse skal bidra til tilfredsstillende informasjonssikkerhet slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas. Det er viktig at vi som privatpersoner kan ha tillit til at våre personopplysninger blir behandlet på en forsvarlig måte.

Før en ny datatjeneste kan tas i bruk i helsevesenet, må den gjennomgå en vurdering i forhold til hvordan informasjonssikkerheten i den nye tjenesten er i varetatt. Dette for å ivareta risikostyringen hos databehandlere av sensitive personopplysninger.

Et viktig hjelpemiddel i arbeidet med risikovurdering for en tjeneste er verktøyet risiko- og sårbarhetsanalyse (ROS -analyse). Jeg har derfor foretatt en Ros-analyse av en tjeneste som gjør det mulig å etablere en videosamtale mellom AMK-operatør og innringer. ROS-analysen er basert på gjeldende lover og forskrifter, samt sikkerhetsprinsipper etablert for å oppnå tilfredsstillende informasjonssikkerhet i infrastruktur og applikasjoner.

På bakgrunn av den teorien jeg har benyttet, behovsanalysen, gjeldende lovverk og svar innkommet i spørreundersøkelse utført bland AMK-operatører, mener jeg denne oppgaven kan konklusjonen med at dette er et svært viktig verktøy for AMK-operatørene, som med gitte forutsetninger, er innenfor akseptable rammer for informasjonssikkerheten til enkeltmennesker i en sårbar situasjon.

AMK-operatørene rapporterer i sine svar fra spørreundersøkelsen at de har reddet mange liv allerede på den tiden de har hatt tilgang til video som verktøy. Den beskrives som «Et helt uvurderlig verktøy. En ny æra innen akuttmedisin»

Abstract

When I started writing this thesis, I did not know that it would have such an eerie topicality as it has. I wanted to look at information-security in a service that was under development, the possibility of video-calls between AMK-operators and callers. Was it possible to develop such a service within the framework of the existing legislation that safeguards privacy and information security? At the start of my work, a global danger began to simmer in China, a dangerous pandemic was developing rapidly. Soon the Corona pandemic affected the entire world, with closures of entire communities, closures on a scale the world had not before seen in modern time. With this isolation, we were forced to find new ways of working together, to keep society going.

The most of us were assigned to home-offices over a long period of time. Almost overnight, we were forced to use digital communication platforms, which may not have been dimensioned for this extensive use. Now we were in a situation that was not planned, perhaps the introduction and use of new interaction platforms was affected by this. After a short period of time, it became clear that these new collaboration platforms could be a threat to information security.

So while the pandemic unfolded out there in the real world and got closer and closer to home, with all the consequences it brought, I sat and wrote about information-security in a digital interaction-service, video-call between AMK and caller. The possibilities for, and requirements for using new technology in the healthcare system have challenged privacy. In the period I have worked on this thesis, new data-attacks have been regularly reported, where unauthorized people have gained access to or tried to gain access to our healthcare data.

There have been reports of data-burglary and other forms of data-attacks targeting both hospitals and doctors' offices, but also more random attacks. The health care must fulfill many functions and cover many needs. In this thesis, I have looked more closely at the prehospital chain, which is responsible for assisting when acute incidents and crises occur. I have immersed myself in information security in a service that enables video calling between AMK-operators and callers.

In order to gain insight into how the AMK-service is structured, and what responsibilities and expectations of the individual AMK-operator, I have used a completed needs analysis carried out by Making Waves. This provides valuable insight into how the working day of the person answering emergency calls can be.

Health care is subject to many laws and regulations. In addition to ordinary health legislation, the prehospital chain has its own regulations that must be complied to. This is the Emergency Medical Regulations.

When it comes to information security, there are many laws and regulations that regulate access to health information. They contribute to satisfactory information security so that health care can be offered in a responsible and effective manner, at the same time as privacy is safeguarded. It is important that we as private individuals can have confidence that our personal data is processed in a responsible manner.

Before a new data service can be used in the health care system, it must undergo an assessment in relation to how the information security in the new service is taken care of. This takes care of the risk management of data processors of sensitive personal data.

An important tool in the work with risk assessment for a service is the tool of risk and vulnerability analysis (ROS analysis). I have therefore carried out a praise analysis of a service that makes it possible to establish a video call between the AMK-operator and the caller. The ROS analysis is based on current laws and regulations, as well as security principles established to achieve satisfactory information security in infrastructure and applications.

Based on the theory I have used, the needs analysis, current legislation and answers received in a survey conducted among AMK-operators, I believe this thesis can conclude that this is a very important tool for AMK-operators, who with given assumptions, are within acceptable framework for the information security of individuals in a vulnerable situation.

The AMK-operators report that they have saved many lives already in the time they have had access to video as a tool. It is described as «A completely invaluable tool. A new era in emergency medicine. »

Forord

En utrolig kjekk og lærerik tid er over. Jeg har i tre og et halvt år vært student ved sagnomsuste og prestigefylte NTNU. Jeg har gått i gangene på Gløshaugen og på Øya helsehus. Det er nesten ikke til å tro og nå har jeg ferdigstilt min masteroppgave ved masterstudiet innen Helseinformatikk. Det har vært en av de mest lærerike periodene i mitt liv, takket være engasjerte foredragsholdere, flinke medstudenter og ikke minst utrolig interessante fag.

Jeg har alltid hatt stor fasinasjon for den «Den prehospitale kjeden» og den har gått som en rød tråd gjennom studiet mitt. Og nå avsluttes studiet med en masteroppgave som fordyper seg i akutt medisinsk kommunikasjonssentral (AMK) og informasjonssikkerhet knyttet til nye tjenester som blir tatt i bruk for å bedre tjenesten AMK yter til samfunnet og enkeltmennesker i en nødsituasjon.

Der er flere som fortjener en stor takk for at jeg er kommet så langt som jeg har.

Først vil jeg nevne at jeg er utrolig stolt over at jeg hadde så pass tro på meg selv at jeg turte å søke opptak til dette studiet og ikke minst at jeg har fullført på en ganske respektabel måte.

Jeg vil rette en stor takk til pre-hospital seksjon, Sykehuspartner HF. Uten rådene fra medarbeidere ved pre-hospital seksjon hadde ikke denne oppgaven blitt til. De pekte meg så velvillig i retning av et utrolig spennende tema for min masteroppgave. De gjorde meg oppmerksom på Vestre Viken sitt innovasjons-prosjekt, videosamtale mellom AMK-operatør og innringer, samt AMK OSLO sitt tilsvarende prosjekt. Også ansatte ved AMK OSLO ønsker jeg å rette en stor takk til, for sin svært imøtekommende holdning til meg og min masteroppgave. Det har gitt meg svært nyttig informasjon, som vært helt avgjørende for at jeg kunne ferdigstille denne masteroppgaven.

Jeg vil videre takke arbeidsgiver for å ha vært svært imøtekommende både når det gjelder å få anledning til å møte på samlingene i Trondheim, men også så velvillig har lagt til rette for at jeg har fått tid til å ferdigstille oppgaven. Videre vil jeg takke gode arbeidskollegaer for gjennomlesning og faglige råd og veiledning.

Familien min fortjener en stor takk for sin utstrakte tålmodighet med en voksen student i huset. Det har vært forventninger om både gjennomlesning av «en glimrende ide» både hverdag som helg, samt ønske om servering av måltider både i tide og utider.

Sist, men ikke minst vil jeg takke min veileder på NTNU, Pieter Jelle Toussaint for tålmodig å ha ledet meg gjennom oppgaven på en trygg og behagelig måte.

Innhold

1 Introduksjon

Jeg har privat, i mange år fått bidra til den frivillige redningstjenesten, ved at jeg har hatt godkjent redningshund og deltatt på utallige redningsaksjoner hvor liv og helse har stått på spill. I dette arbeidet har jeg blitt fasinert over det nære og gode samspillet de frivillige redningsorganisasjonene har med «blålys-etatene». Jeg har selv opplevd betydningen av god kommunikasjon og forståelse for situasjonen på ett skadested. Dette, samt generell interesse for akuttmedisin, har ført til at jeg har en særskilt fasinasjon for den prehospitale tjeneste.

I hele studieperioden ved HTNU har jeg hatt særskilt interesse for den rollen AMK spiller når en akuttsituasjon oppstår. Jeg har sett på informasjonsflyten i den prehospitale kjeden, fra innringer tar kontakt med AMK og varsler om en nødsituasjon, til pasient er trygt plassert på akutt mottak på et sykehus, ved hjelp av ambulansetjenesten.

Generelt i samfunnet blir der tatt i bruk ny teknologi. Internett, smarttelefoner og nettskyen har gitt oss nesten ubegrenset tilgang til informasjon. Også i helsesektoren har man tatt del i den teknologiske utviklingen. Regjeringen vil øke digitaliseringen i helsetjenesten. Det vil gjøre arbeidsdagen bedre for dem som jobber der, men enda viktigere er det at hverdagen blir bedre for pasientene. For at pasienten skal få god helsehjelp må vi sørge for at relevante opplysninger følger den enkelte. Gode digitale e-helseløsninger er en forutsetning for dette(Regjeringen, 2019) Et eksempel på det er at stiftelsen Norsk luftambulanse i samarbeid med AMK OUS, har utviklet en tjeneste hvor der kan etableres video-overføring fra innringer på et skadested, slik at AMK operatør kan få tilgang til kamera på innringers smarttelefonen.

Videosamtale kan potensielt være livreddende i situasjoner der innringer misforstår den muntlige veiledningen som gis, som for eksempel ved utføring av hjerte-lungeredning. Videosamtale vil også kunne bidra til økt pasienttilfredshet, tillit og opplevd trygghet for innringer. Men samtidig er det noen viktige forutsetninger som må tas hensyn til ved videosamtale med AMK, som personvern og informasjonssikkerhet. Det er viktig at innringer har tillit til at helseopplysninger gitt i en sårbar situasjon, blir behandlet på en trygg og sikker måte og at personvernet ivaretas.

Men der er en rekke eksempler på dataangrep rettet mot helsevesenet, hvor det antas at trussel-aktører kan ha fått tilgang til personsensitiv informasjon fra disse tjenestene.

Direktør ved ett av de berørte helseforetakene uttaler følgende «Vi opererer i en virkelighet med et trusselbilde i endring. Dataangrepet viser nødvendigheten av det kontinuerlige arbeidet med informasjonssikkerhet, både i det daglige og i den pågående moderniseringen av infrastrukturen i regionen » (Sykehuset Innlandet HF, 2020a)

Jeg vil derfor i denne oppgaven, se på videotjenesten utviklet for nødsamtaler mellom AMK og innringer, i et informasjonssikkerhetsperspektiv.

2 Forkortelser - Begrepsliste

Hvert fagfelt har sin fagterminologi. Fagterminologi er ord og uttrykk som brukes innenfor et avgrenset fagområde. Hensikten er å gjøre utveksling av fagkunnskap og kommunikasjon mellom dem som arbeider innenfor fagområdet, lettere og mer entydig. Alle bransjer og yrker har en egen fagterminologi, men det varierer hvor omfattende fagterminologien er. (Jansen, 2018)

Helsesektoren har sin fagterminologi, som består av et spesielt ordforråd som er knyttet til faget. Fagterminologier inneholder som regel mange fremmedord. (Det norske medicinske selskab, 2011) For å sikre en felles forståelse av sentrale begreper, vil dette kapittelet gi en kort forklaring på begreper og forkortelser brukt i denne studien.

2.1 Forkortelser

AMK	Akutt medisinsk kommunikasjonssentral
DPIA	Data Protection Impact Assessment
ECC	Emergency Communications Centre
Flight following	«Monitorering og oppfølging av helikopter på oppdrag for å ivareta sikkerhet ved uforventede hendelser» Innebærer å innhente flyrute og antatt landingstidspunkt, samt antall personer om bord ved alle forflytninger av helikopter. I tillegg iverksettelse av nødvendige tiltak hvis kontakt med helikopter blir brutt, dette innenfor beskrevne kriterier (tiltaksprosedyre).(Flight Following – Funksjon, 2020)
GPS	Global Positioning System
HEMS	Helicopter Emergency Medical Services.
HLR	Hjerte – lunge- redning
IKT	informasjons- og kommunikasjonsteknologi.(Store norske leksikon, 2019)
InfoSek	Informasjonssikkerhet (information security)
ISRM	Risikostyring for informasjonssikkerhet
LV	Legevakt

NTNU	Norges teknisk-naturvitenskapelige universitet
PCI	Perkutan koronar intervensjon, PCI er en metode hvor man blokker opp trange partier i hjertets kransårer ved hjelp av et kateter som føres gjennom huden.(NHI, 2019)
RHF	Regionalt helseforetak
RTC	Sanntidsdatasystemer er en klasse av tekniske datasystemer som vektlegger krav til responstid og ytelse. Sanntidsdatasystemer kalles på engelsk for Real Time Computer Systems. Et sanntidsdatasystem må overholde en bestemt tidsfrist fra hendelse inntil systemet reagerer. Et ikke sanntidsdatasystem derimot krever ingen tidsfrist for systemreaksjon, selv om så rask utføring som mulig er ønskelig. (Høyskolen i Østfold, 2012)

2.2 Begrepsavklaring

2.2.1 Personvern

Personvern handler i hovedsak om å beskytte og ivareta informasjon ut fra hensynet til den enkeltes privatliv og bestemmelsesrett over egne personopplysninger. Dette innebærer bl.a. å sørge for at det ikke lagres flere opplysninger enn nødvendig og at alle har rett til innsyn i sine opplysninger (e-helse, 2018). Begrepet innebærer i stor grad også vernet av enkeltpersoners rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv. Vi skal i størst mulig grad kunne bestemme over egne personopplysninger. (Datatilsynet, 2019b)

2.2.2 Personopplysninger

Definisjonene av personopplysninger er i Personvernforordningen artikkel 4 definert slik:

Personopplysninger er «enhver opplysning om en identifisert eller identifiserbar fysisk person. Personopplysninger er alle opplysninger og vurderinger som kan knyttes til deg som enkeltperson. Typiske personopplysninger er navn, adresse, telefonnummer, e-post og fødselsnummer. Biometri slik som fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) er også personopplysninger. Opplysninger om atferdsmønstre er også regnet som personopplysninger. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du fysisk beveger deg i løpet av en dag og hva du søker etter på nettet er alt sammen eksempler på dette. (Datatilsynet, 2019a)

2.2.3 Særlige kategorier av personopplysninger

Tidligere kjent som sensitive personopplysninger.

Dette er personopplysninger om «rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap. Det gjelder også behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. (De nasjonale forskningsetiske komiteene, 2020)

2.2.4 Helseopplysninger
Personopplysninger om en fysisk persons fysiske eller psykiske helse, medregnet ytelse av helsetjenester, som gir informasjon om vedkommende sin helsetilstand. (Helseregisterloven, 2014a)

2.2.5 Helseregister
Enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier, og som inneholder helseopplysninger. (Helseregisterloven, 2014)

2.2.6 Behandlingsrettede helseregister
Behandlingsrettede helseregistre har som formål å dokumentere helsehjelp som gis, og således gi grunnlag for videre helsehjelp eller administrasjon av helsetjenester til enkeltpersoner. Pasientjournalsystemet i et sykehus er et eksempel på et behandlingsrettet helseregister. Slike registre er regulert gjennom pasientjournalloven. (Store norske leksikon, 2019b)

2.2.7 Dataansvarlig
Ansvarlig for behandling av helseopplysninger. (Helseregisterloven, 2014b)

2.2.8 Autentisering
Autentisering benyttes både om prosessen med å bekrefte en påstått identitet, og om prosessen med å bekrefte om informasjon er ekte og uendret. (Store norske leksikon, 2019a)

Autentisering av en sluttbruker forutsetter at en tillitsmodell eksisterer med nødvendige avtaler mellom partene. Identiteter må være opprettet og forvaltet og det må være etablert tillit mellom autentiseringstjeneste og identitetsforvalter. (Direktoratet for e-helse, 2019)

2.2.9 Autorisering
Autorisering vil innenfor it-området si å gi en gitt bruker tilgang til et veldefinert sett med ressurser. Å autorisere vil si å definere en tilgangs-policy.

2.2.10 Sporbarhet
Beskriver metoder som skal knytte enhver endring av informasjon til en identitet.

2.2.11 Samtykke
Med samtykke menes tillatelse fra pasienten. Et samtykke må være frivillig, uttrykkelig og informert. Samtykket trenger ikke å være skriftlig, men for at samtykke skal være gyldig, forutsetter det at det foreligger et informert samtykke. Det betyr at vedkommende som samtykker, har fått uttømmende informasjon om hvilke opplysninger det gjelder, hvordan disse skal anvendes og eventuelle konsekvenser av dette. (Datatilsynet, 2019)

2.2.12 Implisitt samtykke/ stilltiende samtykke
Stilltiende samtykke vil i sammenheng med helserelatert juss si at en godtar noe uten at man blir forespurt i utgangspunktet. Et eksempel på dette er at avgjørelser blir tatt av

helsepersonell når pasienten ikke selv er i stand til å gi sitt samtykke. (Pasient og brukerrettighets loven, 2019)

2.2.13 HelseCERT

Norsk Helsenett SF har etablert HelseCERT (Computer Emergency Response Team). Dette skal være helse- og omsorgssektorens felles kompetansesenter for informasjonssikkerhet. Senteret skal spre kompetanse om IKT-trusler og beskyttelsesmekanismer, monitorere trafikken på helsenettet og bistå aktørene ved konkrete IKT-sikkerhetshendelser. Målet er å forebygge og avhjelpe uønskede IKT-sikkerhetshendelser og ondsinnede inntrengingsforsøk. HelseCERT skal spre kompetanse om IKT-trusler og beskyttelsesmekanismer, og kontinuerlig overvåke trafikken i helsenettet. Senteret skal samarbeide med Nasjonal sikkerhetsmyndighet NorCERT og andre nasjonale og internasjonale enheter.(Helse og omsorgsdepartementet, 2016)

3 Innledning

Den akuttmedisinske kjeden representerer en sammenhengende rekke av tiltak for å sikre akutt helsehjelp fra hendelsessted, inkludert publikums innsats, fram til endelig behandlingssted, ofte på akuttmottak på et sykehus. Den er et uttrykk for samfunnets samlede organisatoriske, personellmessige og materielle beredskap. Kjeden er et nettverk bestående av fastlege, kommunal legevakt og legevaktsentral. Den inkluderer også helseforetakets akuttmedisinske kommunikasjonssentral (AMK-sentral), bil-, båt- og luftambulanse, og akuttmottak i sykehus. Det er innringer eller kontaktperson som aktiverer kjeden (Terje Olav Øen et al., 2018).

AMK-sentralene er en akuttmedisinsk tjeneste for publikum, som har i oppgave å redde liv og begrense skade ved medisinske nødsituasjoner (Utredning AMK-sentralene, 2016). Hastegraden bestemmes av opplysninger om pasientens symptomer eller informasjon om ulykken fra den personen som ringer nødnummeret 1-1-3. God koordinering av ambulansene gir bedre utnyttelse av ressursene og derved bedre beredskap. Ambulansepersonellet er helt avhengig av AMK-sentralens faglige vurdering, koordinering og ressursdisponering. (Kvinge, 2013, s7)

Ved behov for akutt helsehjelp ringer publikum 1-1-3, og kommer i telefonisk kontakt med en operatør på AMK. Misforståelser kan oppstå på grunn av språklige utfordringer, tvetydighet, manglende beskrivelse om lokalisering og andre utfordringer med kommunikasjon. Noen ganger viser det seg at situasjonen som ambulansepersonellet møter er en annen enn det innringer-meldingen skulle tilsi. (Kvinge, 2013) Det eneste AMK-operatøren kan basere sin informasjon om hendelsen på, er en telefonsamtale. Innringer er ofte i en stresset situasjon og klarer kanskje ikke å formidle budskapet klart og tydelig. Det er heller ikke sikkert at innringer, som ved de fleste tilfellene er lekfolk, har medisinsk-faglig forståelse for situasjonen pasienten er i. Det sier seg da selv at hendelsen som blir meldt inn, ikke alltid samsvarer med den faktiske hendelsen. (Kvinge, 2013) AMK har en viktig rolle i forhold til å gjenkjenne hjertestans, og å gi publikum telefonveiledning i HLR. Flere studier viser at tiltak for å øke gjenkjenning og veiledning i telefonveiledet HLR øker overlevelses-raten hos hjertestans-pasientene. (Utredning AMK-sentralene, 2016) Dersom AMK-operatør kan se det samme som innringer, vil det kunne hindre misforståelser som kan føre til tap av liv og helse, og gi operatøren på AMK en riktigere forståelse av situasjon ("Innovasjonspartnerskap – Videosamtale med Akuttmedisinsk kommunikasjonssentral (AMK)," 2019). Så god overensstemmelse som mulig, er viktig for å oppnå rask respons ved alvorlige situasjoner, der pasienten er avhengig av å komme under rask medisinsk behandling. Samtidig kan en på den måten unngå unødig bruk av ressurser ved hendelser som viser seg å være mindre alvorlige. Man kan dermed sikre at god akuttmedisinsk beredskap opprettholdes med minst mulig ressursbruk for samfunnet. (Kvinge, 2013)

Vestre Viken regionale helseforetak, ved Klinikk for prehospitale tjenester, med støtte fra Innovasjon Norge, holder på å utvikle en løsning for videosamtale mellom AMK og innringer. Video, i tillegg til tale, vil gi operatørene på AMK-sentralen bedre mulighet til å bistå i nødsituasjoner og potensielt redde flere liv.

Utfordringen som Vestre Viken HF sammen med Innovasjon Norge, ville se på var:» Hvordan kan vi skape en best mulig tjeneste for videosamtaler for ansatte ved AMK, slik at de kan bistå folk i nødsituasjoner på en rask og sikker måte?» (Platou, 2019)

Det er behov for en brukervennlig, sikker og rask løsning for videosamtaler med AMK som ivaretar taushetsplikten og personvernet til pasient, innringer og helsepersonell. Samtidig må løsningen kunne ivareta krav til dokumentasjon som vil gjelde AMK. Det finnes ingen AMK-sentraler som har slike løsninger i drift i Norge i dag. (Platou, 2019)

Å innføre tekniske løsninger som gir mulighet for videosamtale mellom innringer og AMK -operatør reiser en del spørsmål rundt personvern og informasjonssikkerhet. Slike prosjekter møter ofte tøffe hindringer fra den sentrale styringen av informasjonssikkerhet og personvern, nedfelt i lovverket og strengt håndhevet. (Christie, Hoholm, & Mørk, 2018)

Vi har nå kommet til 2020. Mobil-teknologien har kommet langt på få år og oppdateres stadig og blir bedre for hver dag som går. (Vedlegg : Videooverføring fra Hjelp 113-appen til AMK) AMK Oslo har i et samarbeidet med Stiftelsen Norsk luftambulanse NLA nyttiggjort seg denne teknologien og utviklet en tjeneste som muliggjør videosamtale mellom AMK-operatør og innringer. Tjenesten har blitt prøvd ut i ulike pilotprosjekt ved flere av landets AMK-sentraler, både i bynære strøk, men også sentraler som ligger i mer grisgrendte strøk.

3.1 Sikkerhetshendelser

Helsesektoren produserer og lagrer store mengder sensitive personopplysninger på vegne av samfunnet og for den enkelte av oss. Det er derfor svært viktig at helsesektoren kjenner til hvilke trusler disse opplysningene er utsatt for, både fra nasjonal og internasjonale trussel-aktører. For å forvalte helseopplysningene på en forsvarlig måte, må helsesektoren vite noe om hvilke trusler opplysningene er sårbare for og hvem som kan tenke seg å urettmessig prøve å få tilgang til dem.

Folk flest har tillit til at helsevesenet tar vare på de opplysningen de får av oss. Vi har tillit til at både det vi forteller, de prøver vi avgir og diagnoser som blir stilt med tilhørende behandling, blir godt tatt vare på og sikret. Vi har tiltro til at taushetsplikten ivaretar dette og at sensitive personopplysninger blir behandlet på en forsvarlig måte.

Men ett kjapt søk på internett forteller oss en annen virkelighet. En virkelighet vi kanskje ikke vil vite om. Datasikkerhet er et økende problem i helsesektoren, hvor et økende antall brudd på datavernloven blir rapportert til datatilsynet. (3M, 2020)

Her er en liste med tilfeldig valgte hendelser hentet fra mediebilde de siste årene.

Dataangrep mot Sykehuset Innlandet HF

Sykehuspartner HF avdekket 22. august 2020 at en hittil ukjent trusselaktør har gjennomført et angrep mot enkelte tjenester på internett, som driftes av Sykehuset Innlandet HF. Foreløpige analyser gir så langt grunn til å tro at det er hentet ut data.(Sykehuset Innlandet HF, 2020b)

Datainnbrudd helse Sør Øst

Tidlig i januar i 2018 ble Sykehuspartner HF varslet av Norsk Helsenett om at det pågikk unormal aktivitet mot datasystemer i Helse Sør-Øst. Innbruddet ble kort tid etter politianmeldt og PST innledet etterforskning. .. Sykehuspartners egen undersøkelse, som er gjort i samarbeid med NSM NorCERT og Norsk Helsenett (HelseCERT), har

identifisert at dette har vært et målrettet angrep mot e-læringsprogramvaren. (Sør-Øst, 2018)

Det er flere aktører som har interesse av å kartlegge norske enkeltpersoners pasientjournaler. (Klungtveit, 2018)

WannaCrypt virusangrep

Viruset WannaCrypt skremte nylig en hel verden. 200 000 pc-er ble infisert, og det gikk særlig hardt ut over det britiske helsevesenet. Et skadevareangrep kalt WannaCrypt, som utnyttet et sikkerhetshull i Windows operativsystemet, skremte nylig hele verden ved blant annet å ta pasientjournalene fra det britiske helsevesenet som gisler. WannaCrypt infiserte pc-er i over 150 land. Samlet sett antar man at viruset rammet over 200 000 maskiner. (Lund Flinck 2017)

Legekontor utsatt for hackerangrep

Datainnbruddet ved et fastlege-kontor i Nord-Norge var rettet mot en maskin som henter ut data fra pasientjournaler til forskning. Det er vanskelig å se hva de har vært ute etter, men det er sannsynlig at det kan være snakk om så kalt «ransomware», der alt som er på disken krypteres og det bes om løsepenger for at du skal få tilgang til filene igjen. Det er ikke kjent hvem som står bak angrepet. (Kalveland, 2019)

Forbyr ansatte å bruke populær videokonferanse-tjeneste

I forbindelse med den verdens-omspennende Corona-pandemien i første halvdel av 2020 ble der innført mange strenge restriksjoner som førte til at de ansatte arbeidet fra hjemmekontor. Mange bedrifter tok i bruk videosamtale-tjenester, mer eller mindre over natten, som et verktøy for samarbeid mellom de ansatte. Men med digital kommunikasjon kommer også behovet for sikkerhet. Den amerikanske nettvideotjenesten Zoom har vokst voldsomt i popularitet siden årsskiftet, men der er også påpekt en rekke sikkerhetshull i tjenesten. Det er bla. avslørt at selskapets app for iPhone sendte informasjon om brukerne til Facebook, uten at dette er gjort oppmerksom på i bruksvilkårene. Videre er det avslørt at der ikke er ende-til-ende kryptering, slik selskapet selv hevder. Tjenesten har også en svakhet som kan utnyttes av personer med vonde hensikter kan stjele innloggingsinformasjonen til brukeren som klikket på en spesiell lenke. Der er også opplyst om en svakhet i funksjonen med møteinnkalling til medlemmene i nettverket. Det er rapportert om flere tilfeller av uvedkommende som har kommet seg inn i undervisning og andre videokonferanser, avholdt i denne tjenesten. (Carlsen, 2020)

Dette viser med all mulig tydelighet hvor viktig det er med en planmessig og helhetlig strategi for informasjonssikkerhet i virksomhetene, og å være tro mot de prosesser som er vedtatt, selv når man står oppi en til dels kaotisk situasjon som krever rask avklaring og handling.

3.2 Problemstilling

Den prehospitale kjeden er et stort medisinsk fagfelt med stor samfunnsmessig betydning. Der er mange interessante forskningstema og problemstillinger som det kan være nyttig å få belyst. Jeg har valgt å fokusere på AMK-sentralene sin funksjon i denne kjeden. Oppgaven er konsentrert rundt Vestre Viken sitt innovasjonsprosjekt som skal utvikle tjeneste for videosamtale mellom AMK-operatør og innringer, samt AMK Oslo og NLA sin videotjeneste knyttet til Mobil appen Hjelp 113. Denne oppgaven begrenser seg til videosamtale-tjenesten, AMK-operatørens arbeidsplass samt personvern og informasjonssikkerhet knyttet til en slik tjenesten.

Innføring av videosamtale vil påvirke AMK-operatørenes arbeidshverdag. Det vil påvirke kommunikasjonen mellom AMK-operatør og innringer. Innringer gis mulighet på en helt ny måte å formidle situasjonen pasienten befinner seg i, og på den måten gi AMK-operatøren bedre innsikt i bl.a skadested og skadeomfang. Dette vil trolig påvirke triagering av pasient, og dermed også ressursutnyttelse av ambulanse, helikopter, fly og lege. Jo mer informasjon som er tilgjengelig i tjenesten, jo mer hensyn må man ta til informasjonssikkerheten. «Helseopplysningene våre er sensitive. Med dem kan vi ikke ha noe slingringsmonn», kommenterer Direktør i Datatilsynet Bjørn Erik Thon i en reportasje om stadig økende bruk av helseapper». (Carlsen, 2013)

3.3 Forsknings-spørsmål

Informasjonssikkerhetsleder og personvernombud ved Vestre Viken HF har konkludert med at en videosamtale mellom AMK-operatør og innringer kan utvikles med dagens regelverk. (Waves, 2019) I denne oppgaven vil jeg se på hvilke lover og forskrifter som gjelder for personvern og informasjonssikkerheten i helsevesenet og hvordan disse er ivaretatt i en slik tjenesten. For å se hvilke personverns-utfordringer implementering av en slik tjeneste møter, vil jeg utføre en risikoanalyse av en tjeneste som har funksjonalitet for å tilby videosamtale mellom AMK-operatør og innringer.

3.4 Oppgavens oppbygning

Informasjonssikkerhet skal være den røde tråd i denne oppgaven. For å få innsikt i hva det egentlig innebærer, slik at jeg til slutt har nok grunnlag og innsikt til å vurdere informasjonssikkerheten i en tjeneste som muliggjør videosamtale mellom AMK-operatør og innringer, har jeg bygget opp oppgaven først med ett kapittel med en begrepsliste for å sikre en felles forståelse for ord og uttrykk brukt i denne oppgaven. For å synliggjøre hvor dagsaktuelt temaet informasjonssikkerhet er, trekker jeg i kapittel 3.1 frem eksempler på sikkerhetshendelser fra helsesektoren av nyere dato. For å sikre en solid forankring når det gjelder krav til informasjonssikkerhet i tjenester som behandler sensitive personopplysninger, har jeg i kapittel 4.1 sett på gjeldene helselovgivning som er relevant for både den pre-hospitale kjede, samt lover og forskrifter som stiller krav til databehandling av pasientdata.

Norm for informasjonssikkerhet, Normen, er et sentralt rammeverk og definert som bransjestandard innen helsesektoren. Der er også flere lover som har som målsetning å ivareta personvern og informasjonssikkerhet for pasientene. Prosjektet som utførte behovskartleggingen trekker frem følgende lover som er spesielt relevante for videotjenesten, akuttmedisinforskriften, helsepersonelloven, journalforskriften, pasient- og brukerrettighetsloven, personvernforordningen og spesialisthelsetjenesteloven.

I kapittel 4.2 ser jeg på hva som ligger i begrepet sikkerhet generelt og informasjonssikkerhet spesielt, før jeg i kapittel 4.4 fordyper meg i en behovskartlegging av en tjeneste som muliggjør videosamtale mellom AMK-operatør og innringer.

Før man skal utvikle en ny tjeneste, må man finne ut det faktiske behov, samt i hvilke situasjoner og eksisterende miljø, tjenesten skal fungere i. For å få innsikt i hvordan en videotjeneste best i varetar både innringer, AMK-operatøren, samt de tekniske løsningene tjenesten skal fungere i, er behovskartlegging et godt hjelpemiddel for å få belyst dette. Behovskartleggingen er i sin helhet utført av Making Waves, på oppdrag fra Vestre Viken RH. Utfordringen de fikk var hvordan man kan skape en best mulig tjeneste for videosamtale for operatører ved AMK, slik at de kan bistå mennesker i medisinsk nødsituasjoner på en rask og sikker måte.

I kapittel 4.4 vil jeg se på de krav som kom frem i behovskartleggingen til Making Waves. Jeg vil se på hvilke data som er kommet frem i denne behovskartleggingen og hvordan disse er fremkommet. Jeg vil videre se på hvilke metoder Making Waves har benyttet i sin kartlegging og hvilke utvalg av informanter de har benyttet.

Videre vil jeg se hvilke innsamlingsmetoder de har benyttet, samt hvordan de har analysert disse for å komme frem til de slutningene de har.

Det var meningen at jeg selv skulle hospitere både på AMK-sentraler som har deltatt i pilotprosjektet for utprøving av tjenesten til AMK Oslo og NLA og i ambulansetjenesten for å få innsikt og forståelse i arbeidsflyten til AMK-operatørene som har benyttet videosamtalen i sitt arbeid. Men pga. Coronapandemien og smitterestreksjoner som samfunnet har vært midt oppi har det ikke latt seg gjennomføre. Jeg har derfor utarbeidet en spørreundersøkelse som omhandler bruken av og informasjonssikkerhet i en slik videotjeneste. Spørreundersøkelsen er gjennomført blant AMK-operatører ansatt på AMK-sentraler som har deltatt i pilotprosjekter for uttesting av AMK Oslo og NLA sin videotjeneste.

Litteratur er en kilde til kunnskap. Jeg har derfor i kapittel 4.5 sett på hvilken forskning som allerede er gjort i forhold til personvern og informasjonssikkerhet innen IKT i helsetjenesten, både nasjonalt, men også internasjonalt. Så i kapittel 5.1 og 5.2 vil jeg fordype meg i den sammenhengen videosamtalen skal fungere i, den prehospitale kjede. Jeg vil se på de to hovedaktørene som vil bli nærmest berørt av en videosamtale-tjeneste, AMK-sentralene og ambulansetjenesten. Hvordan er disse bygget opp, hvem er aktørene og hva er ansvarsområdet deres? En god kilde til innsikt her har vært behovskartleggingen til Making Waves. Videre i kapittel 5.4 ,5.5 og 5.6 legger jeg det teoretiske grunnlaget for en risikovurderingen av tjenesten. Her fordyper jeg meg i begrepene risikostyring, sikkerhetskrav og sikkerhetsprinsipper. Så, i kapittel 6 vil jeg vurdere tjenesten i ett informasjonssikkerhetsperspektiv. Som grunnlag for denne analysen vil jeg benytte funksjonell beskrivelse, tjenestedesign og annen beskrivelse av tjenesten som AMK Oslo har utarbeidet i samarbeid med NLA, samt behovskartleggingen til Making Waves. Jeg vil gå inn på ulike prinsipper som kan legges til grunn for en konkret vurdering, samt gjøre en sikkerhets og sårbarhetsanalyse av tjenesten. Denne analysen vil danne grunnlag for den drøfting jeg til slutt vil foreta om hvordan informasjonssikkerheten og personvernet er ivaretatt i løsningen.

4 Teori

I dette kapittelet presenterer jeg det teoretiske fundamentet som ligger til grunn for den risikovurderingen denne oppgaven skal resultere i. Innledningsvis i dette kapittelet begynner jeg å presentere den helselovgivning som er relevant for informasjonssystemer i helsesektoren. Der er en rekke lover og forskrifter som regulerer hvordan personopplysninger skal behandles, og skal sikre at sensitive personopplysninger behandles på en forsvarlig måte. Her er bl.a. Normen, en bransjenorm for informasjonssikkerhet og personvern i helsesektoren, sentral. Normen har som formål å bidra til å sikre at en virksomhet som etterlever og innretter seg etter Normen har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

Videre fordyper jeg meg i sikkerhet generelt og informasjonssikkerhet spesielt. Dette vil gi meg verdifull innsikt i hvordan jeg skal identifisere sårbarheter, samt analysere og evaluere risiko, og identifisere tiltak som kan redusere risikoen.

Behovskartleggingen i kapittel 4.4 utgjør en stor og viktig del av teorien i denne oppgaven. Den har gitt meg verdifull innsikt i arbeidshverdagen til en AMK-operatør som sitter og tar imot nødsamtaler. Den har gitt meg innsikt i ansvarsområder og ikke minst hvilke behov en videotjeneste skal dekke.

Der foreligger både norsk og internasjonal forskning knyttet ta i bruk ny teknologi i helsesektoren. I kapittel 4.5 både nasjonal og internasjonal forskning, som fokuserer på de muligheter som ligger i den teknologiske utviklingen presentert.

Informasjonssikkerhet er en del av et stort og omfattende tema med mange aspekter, nemlig informasjonskvalitet. Det er vanlig å dele informasjonskvalitet opp i følgende fire perspektiv. Dette er iboende kvalitet, sikkerhetsbehov, brukskvalitet og presentasjonskvalitet. Iboende kvalitet stiller spørsmål ved om informasjonen som er gitt henger sammen og ikke er selvmotsigende eller om den er gyldig over tid. Brukskvalitet sier noe om at samme informasjon kan ha ulik kvalitet eller verdi i ulike sammenhenger. (Store norske leksikon, 2019)

Presentasjonskvaliteten sier noe om hvordan informasjonen er tilgjengelig og har stor betydning for verdien av informasjonen. (Store norske leksikon, 2019b)

I denne oppgaven er det begrenset til informasjonssikkerheten som blir vurdert. Graden av informasjonssikkerhets gjenspeiler hvilke sikkerhetskrav som må stilles til den aktuelle informasjonen.

Når det gjelder lover og forskrifter som er relevant for fagfeltet, vil det føre for langt å behandle dette komplett og utdypende. I denne oppgaven er derfor de viktigste og mest relevante lovene tatt med. Det er kun gitt en opplisting av de mest relevante lovene, samt en kort beskrivelse av hva formålet til loven er.

Risiko og sårbarhetsanalysen er kun vurdert ut ifra personvernperspektiv og informasjonssikkerhet. Andre perspektiv, så som bla. driftsmessig, økonomiske eller samfunnsmessige perspektiv er ikke vurdert i denne oppgaven.

Det vil fremkomme i metode-kapittelet mer konkret hvilke metodiske og teoretiske avgrensninger som er gjort.

4.1 Helselovgivning

Helselovgivning er en samlebetegnelse på lover og forskrifter som regulerer forhold vedrørende helsetjenester og helsepersonell, samt adgangen til å gripe inn overfor faktorer som kan påvirke folkehelsen eller virke sykdoms-skapene. (Store norske leksikon, 2019a)

All helselovgivningen har først og fremst et helseperspektiv. Men der stilles også ulike informasjonssikkerhetskrav i lover og regler som omhandler helseinformatikk. Der stilles offentlige informasjonssikkerhetskrav til tjenesten, offentlige informasjonssikkerhetskrav i helsesektoren og informasjonssikkerhetskrav til systemet. Regelverket om informasjonssikkerhet er i hovedsak risikobasert. Det overlater til virksomheten å velge et passende nivå for usikkerhet (risikoappetitt), samt å velge egnede sikkerhetstiltak. Det gir rom for tilpasninger til virksomhetens størrelse, egenart og risikobilde. Selv om regelverket er fleksibelt kreves god kunnskap, kompetanse og evne for å utnytte denne fleksibiliteten og for å kunne gjøre kloke vurderinger og valg. (Direktoratet for e-helse 2019)

Der finnes i dag ikke et regelverk som gir klare føringer for videosamtale mellom AMK-sentral og innringer. Der finnes kun lover for lydsamtale. En må derfor foreta fortolkning av eksisterende regelverket. Følgende regelverk er vurdert som relevant når en skal vurdere informasjonssikkerheten i tjenesten.

4.1.1 Akuttmedisinsk forskrift

De akuttmedisinske tjenestene er et område hvor myndighetene har sett behov for en tydeligere regulering. Akuttmedisinforskriften stiller spesifikke krav til innholdet i de akuttmedisinske tjenestene, og har til formål å sikre at befolkningen ved behov for øyeblikkelig hjelp mottar forsvarlige og koordinerte tjenester utenfor sykehus. For disse tjenestene er ofte tid, tilgjengelighet, koordinering og samhandling avgjørende faktorer, og forskriften utdyper spesialisthelsetjenestelovens generelle krav. (Helse- og omsorgsdepartementet, 2016)

I tillegg skal den sikre at kommunikasjonsutstyr som blir benyttet av tjenesten har prioritert informasjonsflyt mellom institusjonene i kjeden og andre nødetater. (Akuttmedisinforskriften, 2015)

Forskriften pålegger AMK-sentralene å besvare 90 prosent av henvendelsene fra publikum innen 10 sekunder. (Helse- og omsorgsdepartementet, 2016)

4.1.2 Helsepersonell-loven

Lovens formål er å bidra til sikkerhet for pasienter og kvalitet i helse- og omsorgstjenesten samt tillit til helsepersonell og helse- og omsorgstjenesten. (Helsepersonell-loven, 2000)

4.1.3 Journalforskriften

Forskriftens formål er å bidra til at

a) pasienter ved hjelp av relevant og nødvendig dokumentasjon kan gis helsehjelp av god kvalitet, inkludert effektive og gode pasientforløp

b) personvernet ivaretas, inkludert pasientens rett til informasjon og medvirkning

c) helsehjelpen kan kontrolleres i ettertid.(Pasientjournalforskriften, 2019)

4.1.4 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)

Formålet med loven er å legge til rette for innsamling og annen behandling av helseopplysninger, for å fremme helse, forebygge sykdom og skade og gi bedre helse- og omsorgstjenester. Loven skal sikre at behandlingen foretas på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste. (Helseregisterloven, 2014)

4.1.5 Pasient og brukerrettighetsloven

Pasient- og brukerrettighetsloven inneholder rettsregler om de rettigheter pasienter og brukere har overfor helse- og omsorgstjenesten.

Pasient- og brukerrettighetsloven gjelder for alle i riket. Pasienter og brukere har etter loven rett til øyeblikkelig og nødvendig helsehjelp fra kommunen.

Loven slår fast at helsehjelp som utgangspunkt bare kan gis med en pasients samtykke. Bare hvis det finnes grunnlag for det i lov, kan helsehjelp gis uten samtykke. (Pasient og brukerrettighets loven, 2019)

4.1.6 Personvernforordningen (GDPR)

Forordning om beskyttelse av individer ved behandling av personopplysninger og om fri flyt av slike opplysninger.

Forordningens formål er å sørge for en god beskyttelse av personopplysninger samtidig som personopplysninger skal kunne utveksles fritt innenfor EØS-området.

Forordningsformen innebærer full harmonisering av personvernreglene i EU/EØS. Dette innebærer at det i utgangspunktet ikke er adgang til å fravike reglene og heller ikke til å gi supplerende regler. Imidlertid åpner forordningen selv for at det kan gis nasjonale regler i enkelte tilfeller. (Personvernforordningen GDPR, 2018)

4.1.7 Helseinformasjonssikkerhetsforskriften

- Forskrift om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre (helseinformasjonssikkerhetsforskriften)

Formålet med forskriften er å regulere nødvendig tilgang til helseopplysninger og å bidra til tilfredsstillende informasjonssikkerhet slik at helsehjelp kan tilbys på en forsvarlig og effektiv måte samtidig som personvernet ivaretas.
(Helseinformasjonssikkerhetsforskriften, 2011)

4.1.8 Spesialisthelsetjenesteloven

Lovens formål er særlig å:

1. fremme folkehelsen og å motvirke sykdom, skade, lidelse og funksjonshemning,
2. bidra til å sikre tjenestetilbudets kvalitet,
3. bidra til et likeverdig tjenestetilbud,
4. bidra til at ressursene utnyttes best mulig,
5. bidra til at tjenestetilbudet blir tilpasset pasientenes behov, og

6. bidra til at tjenestetilbudet blir tilgjengelig for pasientene.

(Spesialisthelsetjenesteloven, 2001)

4.1.9 Nasjonal Sikkerhetsmyndighet grunnprinsipper for IKT-sikkerhet.

NSMs grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. De er relevante for alle norske virksomheter.

De fire kategoriene

- Identifisere og kartlegge – opparbeide og forvalte forståelse om virksomheten herunder styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere. Dette er grunnlaget for en effektiv implementering av de øvrige grunnprinsippene.
- Beskytte og opprettholde – ivareta en forsvarlig sikring av IKT-systemet og opprettholde den sikre tilstanden over tid og ved endringer.
- Oppdage – oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåking.
- Håndtere og gjenopprette – håndtere sikkerhetshendelser effektivt.
- (Nasjonal sikkerhetsmyndighet, 2020)

4.1.10 NORMEN – Norm for informasjonssikkerhet i helse- og omsorgstjenesten.

Normen er en bransjenorm for informasjonssikkerhet og personvern i helsesektoren. Normen er utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren.

(Normen, 2020)

Formålet med Normen er å bidra til å sikre at en virksomhet som etterlever og innretter seg etter Normen har egnede tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern for sin behandling av helse- og personopplysninger.

(Normen, 2020)

I kartleggingen direktoratet for e-helse utførte i helse og omsorgssektoren i 2019 kom det frem at Normen er et viktig utgangspunkt for virksomhetens arbeid med informasjonssikkerhet ….. Normen utgjør en tydelig del av RHFs krav og styringssystem for informasjonssikkerhet for sine regioner. Normen er godt kjent, utbredt og i stor grad implementert i aktuelle prosesser i helsesektoren. (Nasjonal e-helsemonitor, 2019)

Normen Faktaark 54 – Videokonsultasjon, gir en oversikt over hvilke krav som gjelder ved etablering og bruk av sanntidsløsninger med videokonsultasjon. Virksomhetens ledelse er ansvarlig for at bruk av videokonsultasjon ivaretar pasientrettigheter- og sikkerhet, taushetsplikt, personvern og gir nødvendig informasjonssikkerhet i hele løsningen.(Direktoratet for e-helse, 2020)

4.2 Sikkerhet

Sikkerhet betyr beskyttelse av verdier mot skade. Et underliggende begrep her er personvern, som innebærer beskyttelse av privatlivets fred og kontroller av innhenting og bruk av personinformasjon. (Jøsang, 2018)

Som privatpersoner har vi rett til å bestemme over egne personopplysninger. (Datatilsynet, 2019). Personvernet er grunnlovsfestet. Enhver har rett til respekt for sitt privatliv, og staten skal sikre et vern om den personlige integritet. (Kongeriket Noregs grunnlov, 1814)

For å kunne gi god helsehjelp må man ha tillit. Tillit gir trygghet. Som pasienter må vi kunne stole på helsevesenet. Vi må ha tillit til at de som skal behandle oss har den kunnskap og informasjonen de trenger, når de trenger det. Helseopplysninger er nødvendig for å kunne gi god helsehjelp. Men det er bare de som trenger det, som skal se og bruke opplysningene. (Direktoratet for e-helse 2018b) Innbyggerne må ha tillit til at helseopplysninger blir behandlet på en trygg og sikker måte og at personvernet ivaretas. Samtidig må informasjonsflyten mellom helsepersonell være god slik at oppdatert informasjon er tilgjengelig når det er nødvendig. (Helse og omsorgsdepartementet, 2016) Tillit er avgjørende for digitalisering av helsedata. Helsevesenet må stole på helsedata. De som skal behandle pasienter må ha tillit til at informasjonen de har tilgjengelig er rett, tilstrekkelig og oppdatert.

4.3 Informasjonssikkerhet

For å gi god helsehjelp er det nødvendig å håndtere store mengder opplysninger om enkeltindivider. Disse opplysningene omhandler ofte personlige og sensitive forhold og er avgjørende for helsehjelpens kvalitet. (Direktoratet for e-helse 2018a)

På den andre siden står samfunnets- og helsevesenets behov for vid tilgang til opplysninger, for eksempel hensynet til at helsepersonell raskt og enkelt bør finne nødvendige opplysninger for å yte forsvarlig helsehjelp. Helsevesenet har krav om kvalitetskontroll slik at tjenestene til enhver tid fyller kravene til "rett hjelp til rett tid."

Å behandle opplysninger om pasienter og brukere på en betryggende måte, er avgjørende for å sikre tillit. (Direktoratet for e-helse 2018a)

Som nevnt tidligere betyr sikkerhet beskyttelse av verdier mot skade. Informasjonssikkerhet betyr å beskytte informasjonsressurser mot skade. (Jøsang, 2018)

Personvern- og helselovgivningen stiller krav til informasjonssikkerhet og personvern. (Direktoratet for e-helse 2018a)

Informasjonssikkerhet handler om å beskytte informasjon ut fra prinsipper om konfidensialitet, integritet og tilgjengelighet. (Normen, 2020)

Konfidensialitet betyr å sikre at informasjon ikke blir kjent for uvedkommende, integritet betyr å sikre at informasjon ikke blir endret utilsiktet eller av uvedkommende, mens tilgjengelighet handler om at rett informasjon er tilgjengelig ved behov. (Nasjonal e-helsemonitor, 2019)

I tillegg kan andre egenskaper som f.eks. autentisitet, sporbarhet, uavviselighet og pålitelighet omfattes. (Jøsang, 2018) Etablering av tilstrekkelig teknisk og organisatorisk

informasjonssikkerhet er en av de største utfordringene helseforvaltningen og helse- og omsorgstjenesten står overfor ved utviklingen av en digitalisert helse- og omsorgstjeneste. (Normen, 2020)

Informasjonssikkerhet er en kontinuerlig prosess får å oppdage og hindre trusler og å fjerne sårbarheter. (Jøsang, 2018) Det er også et fagområde under stadig utvikling. (Nasjonal e-helsemonitor, 2019) Men i en innbyggerundersøkelse gjennomført ved årsskiftet 2018/2019 av Kantar TNS Norsk Gallup kom det frem at kun 55 % av innbyggerne har tillit til at helseopplysningene deres er lagret slik at utenforstående ikke har tilgang til dem. (Direktoratet for e-helse, 2019)

For å kartlegge informasjonssikkerheten i en tjeneste, benytter man gjerne en Risiko og sårbarhetsanalyse (ROS). ROS-analysen er i hovedsak en kvalitativ risikovurdering, bygget på faglig skjønn og erfaring. Det har vist seg å være et effektivt verktøy for å definere forbedringsområder. (Brudvik, 2010)

En risikoanalyse skal gi grunnleggende informasjon om hva som kan gå galt og hva sannsynligheten er for at disse uønskede hendelsene inntreffer. I Metodekapittelet 6.7 Risikostyring, vil jeg gå mer detaljert inn på Risikoanalysen og hvordan den utarbeides.

4.4 Behovskartlegging

Den store utfordringen som er motivasjon og bakgrunn for utvikling av videosamtale for AMK-operatør og innringer, er hvordan man kan best mulig skape en tjeneste for videosamtale som kan bistå folk på en rask og sikker måte.

For å få ett innblikk i hvilke sammenheng tjenesten skal fungere, hvilke bruksmessige og funksjonelle krav som vil bli stilt har Making Waves gjennomført flere aktiviteter for å komme frem til en behovskartlegging. Det er benyttet tjenestedesignmetodikk i dette arbeidet. (Making Waves, 2019) Det er denne behovskartleggingen og innsamling av data fra aktiviteter i denne kartleggingen jeg vil benytte i min oppgave, da arbeidet Making Waves har gjort er utført profesjonelt og dekker de aller fleste behov for data til den konkrete tjenesten, samt at en da reduserer belastningen for de AMK-ansatte med nye intervju og nye rollespill m.m. Den beste metoden for å få en forståelse for hvilken sammenheng videosamtalen skal fungere i, hadde vært å benytte medlytt både på AMK-sentralen og hospitering i ambulansetjenesten. Men som nevnt innledningsvis, begrenset smittetiltak knyttet til Coronapandemien muligheten for fysisk hospitering. Jeg har derfor hentet informasjon fra spørreundersøkelse blant AMK-operatører som har testet ut tjenesten til AMK Oslo og NLA.

Behovskartleggingen kartlegger bla. følgende:

- Hvilke faglige behov en slik tjeneste vil medføre hos AMK-operatøren.
- Hva AMK-operatør oppfatter som fremmende og hemmende i løsningen.
- Hvilke tekniske behov og rammevilkår trengs i forbindelse med utvikling og implementering av den nye løsningen.

Den ønskede læring fra behovskartleggingen oppgis fra oppdragsgiver å være hvordan tjenesten oppleves både for ansatte, men også for innringer. En ønsker å se på hvordan en kan legge godt til rette for en arbeidsmåte. I forhold til teknologi ønsker en å se på hva som er viktig for å utvikle og implementere en god tjeneste. Og til sist, men ikke minst, ønsket en å se på hvordan man kan ivareta informasjonssikkerhet og personvern på en god måte i tjenesten.

Det har vært benyttet fire ulike perspektiv for å kartlegge behovene Disse er operatørs behov, innringers behov, teknologiske rammer og muligheter og sist, men ikke minst, personvern og informasjonssikkerhet i tjenesten. Den primære målgruppen for behovskartleggingen har vært AMK-operatør. Sekundær målgruppe er innringer. Pasientens perspektiv har ikke vært i fokus i denne kartleggingen.

Målet med behovskartleggingen har vært å finne ut hvordan tjenesten skal fungere og oppleves for de ansatte og innringer. Videre har det vært et ønske om å finne ut hvordan det kan legges til rette for nye arbeidsmetoder basert på den nye tjenesten. Man ønsket også å se på hvilke momenter som er viktig for å utvikle og implementere en god tjeneste. Hvordan man ivaretar personvern og informasjonssikkerhet er også et viktig moment.

Behovskartleggingen har sett på fire ulike perspektiv for innføring av videosamtalen. Hovedfokus er på AMK-operatøren og dennes arbeidshverdag. Det er videre vurdert innringers behov, teknologiske rammer, samt reguleringer med tanke på personvern og informasjonssikkerhet. På bakgrunn av hovedfokus er det AMK-operatørene som er primærmålgruppe i behovskartleggingen. (Making Waves, 2019)

4.4.1 Metode for behovskartlegging

Datainnsamling som bakgrunn for å kunne utarbeide en kravspesifikasjon, utført av Making Waves, baserer seg hovedsakelig på innsiktsaktiviteter som dybdeintervjuer med operatører og medlytt på AMK-sentralen. Der har også har vært benyttet simulering med tilsvarende teknologi, FaceTime, for å teste ut video i «praksis». Der har også vært gjennomført brukertesting.

Rollespill

Hensikten med rollespillet var å lære hvordan AMK-operatør opplever å benytte video i samtale med innringer.

Følgende to situasjoner ble testet i ett rollespill:

Situasjon A: Innringer ringer på vegne av andre på en privat fest hvor situasjonen er småkaotisk.

Innringer klarer ikke å gi en god beskrivelse av tilstanden til pasienten, som er døddrukken, men ikke bevisstløs.

Situasjon B: Innringer ringer på vegne av seg selv. Har falt i stuen og innringer oppfatter situasjonen som mer alvorlig enn den er. Pasienten er redd og alene. Det som innringer beskriver som store hodeskader, er i realiteten ett lite kutt.

Det ble benyttet Facetime for å simulere situasjonen. Ingen av operatørene som var med i rollespillet viste noe om situasjonen som møtte dem hos innringer.

Rollespillet ble til sammen utført med fem ulike operatører ved AMK-sentralene i Oslo og Drammen. Innringerne var en kvinnelig og en mannlig ansatt ved Making Waves.

Målet med dette rollespillet var å se på hvordan AMK- operatøren brukte mulighet for å starte videosamtalen, og når de stoppet den. Videre ble det sett hvilke beslutninger som ble tatt, hvordan ble videosamtalen brukt i kombinasjon med Indexen (Norsk medisinsk index). Hvordan forholdt AMK-operatøren seg når innringer ikke fulgte instrukser som ble gitt. Hvordan håndterte operatør all den ulike informasjonen som kom frem i situasjonene. Kvaliteten på lyd og bilde, samt tidsbruk ble også vurdert. Og til slutt ble samarbeidet mellom AMK-operatør og innringer vurdert.

Simulering
Målet med denne simuleringen var å få ett innblikk i hvordan innringere opplever å bruke video-tjenesten. Hva opplever innringer som fungerer godt og hva er krevende.

Det ble simulert tre ulike situasjoner og benyttet fem testere, tre fra Making Waves og to studenter.

Innringer skulle i løpet av samtalen med AMK-operatør bli spurt om de ønsket å benytte videosamtale i samtalen.

Fire av testpersonene var under 30 år, mens en var 55 år. Alle er vurdert for å ha god teknologisk kompetanse. Det var et ønske å benytte en dame på 80 år også, men hun var dessverre forhindret fra å kommen. (Making Waves, 2019)

4.4.2 Krav til tjenesten.

De viktigste funnene i behovskartleggingen er at løsningen må gi raskere og riktigere hjelp, slik at AMK-operatørene kan redde flere liv. Dette krever at løsningen må være tidseffektiv, samt at den må føles trygg å bruke.

Ytterligere krav som ble avdekket i behovskartleggingen er at løsningen krever mye øving og testing for å finne beste måte å benytte denne i ulike situasjoner, både hos innringer og operatør. Operatør må kunne vurdere i hvert enkelt tilfelle om og når videosamtalen skal benyttes. Det må være en tydelig vilje-erklæring for å starte tjenesten. Det er viktig at innringer holder konsentrasjonen på situasjonen han befinner seg i, så videotjenesten må være veldig enkel å benytte, med svært enkle instrukser. Innringer må føle at de har kontroll over videotjenesten. Det er ikke ønskelig at innringer kan se AMK-operatøren, da dette kan oppleves som ett forstyrende element. Både lyd og billedkvaliteten må være god, dersom tjenesten skal tilføre AMK-operatøren mer innsikt i situasjonen. Videosamtalen skal ikke erstatte de systemene som benyttes i dag, så som triageringsverktøy, men være et støtteverktøy. Det må ikke være mulighet for å lagre opptaket på innringers enhet. Mulighet for at opptaket kan lagres av helseforetaket gir bedre dokumentasjon, med også større utfordringer med tanke på blant annet personvern. Basert på gjeldende regelverk stilles det også følgende krav til løsningen. Innringer må gi et aktivt samtykke både muntlig og ved klikk. Det skal ikke være mulig å lagre video på innringer sin enhet.

Det er også stilt krav til første versjon av tjenesten, at den skal kunne utvikles frittstående og kunne integreres med fremtidig kommunikasjonsplattform. På sikt skal det legges til rette for at tjenesten skal kunne bli «smartere» og videreutvikles med ny teknologi, som vil forbedre lyd og billedkvalitet. Det stilles også krav til at nyere versjoner av tjenesten skal kunne benyttes på ulike typer enheter, ikke bare mobiltelefoner, samt at det bør åpnes opp for mulighet for at videodialogen går begge veier. Det er også et ønske om å kunne dele videosamtale med legevakt, ambulanse og andre relevante aktører. (Making Waves, 2019)

4.4.3 Hjelp113 App.

Appen Hjelp113 er utviklet av Stiftelsen Norsk Luftambulanse. Den viser automatisk kartposisjonen din med nøyaktige tallkoordinater for bredde- og lengdegrad. Har du appen installert på mobilen, vil et bilde av din kartposisjon automatisk dukke opp på skjermen når du trykker på appen. Ved å klikke på ringeknappen 113 nederst i appen, ringer mobilen til AMK uten at posisjonen din forsvinner fra skjermen. Det gjør at du enkelt kan lese opp og gi posisjonen til akuttmedisinsk nød-sentral i en krisesituasjon. (Johnsen, 2018)

Hjelp113-appen er i dag et viktig verktøy for AMK ved at den sender mobilens GPS-posisjonen til AMK via mobildatanettverket. De fleste mobiler i dag har også mulighet for å sende video. Dette kan gjøres via en kryptert ende-til-ende-kobling mellom Hjelp113-appen og AMK-operatørens nettleser. Først må de to klientene "håndhilse" via en server. Når dette er gjort vil alt av video, lyd og data sendes mellom klientene gjennom denne ende-til-ende-koblingen. Den samme teknologien kan også brukes ved hjelp av en lenke i SMS siden den finnes i alle moderne nettlesere. Videooverføring-tjenesten fra innringer til AMK blir da en integrert del av Hjelp 1-1-3-appen (Se vedlegg 3, Videooverføring fra Hjelp 113-appen til AMK)

4.4.4 Funksjonell beskrivelse Hjelp113-app med integrert videosamtale

4.4.4.1 Hjelp113-appen

- AMK kan starte video-overføringen mens samtalen pågår

- Appen kan styre videokvalitet ved dårlig nett

- Appen vet på forhånd om videooverføring kan skje

- Godkjenning for å bruke kamera, mikrofon og GPS kan gis på forhånd (tidligst når man starter appen)

4.4.4.2 SMS-løsning for bruker

- AMK kan sende ut SMS til bruker med en lenke som vises i nettleseren på mobilen.

- Lenken er bare tilgjengelig i en kort tidsperiode.

- Ikke sikkert mobilen støtter videooverføring

- Godkjenning for å bruke kamera, mikrofon og GPS må gis underveis.

4.4.4.3 AMK-løsning på web

- AMK-operatør logger inn med mobilnummer og kode via SMS

- Viser mulighet klienter for videooverføring

- Mulighet for å sende SMS til mobilnummer

- Mulig å snu kamera til klient som er tilkoblet

- Mulig å få posisjon fra klient som er tilkoblet vist på et kart

- Mulig for AMK-operatør å dele video-feed med ressurskoordinator

4.4.5 Prosessbeskrivelse hjelp113 med Videoopptak integrert

1. Pasient/melder ringer AMK med Hjelp113-appen

2. Hjelp113-appen gjør et kall som forteller om videooverføringen er mulig i bakgrunnen. Hvis videooverføring er mulig, kommer det opp i webløsningen til AMK.

3. Webløsning hos AMK startet ende-til-ende koblingen til innringers mobil.

4. Innringer vil få spørsmål om bruk av kamera (eventuelt allerede gitt tilgang),RTC er klar mellom pasient og AMK. AMK kan nå se hva kameraet på mobilen til innringer viser.

5. AMK kan sende over kommandoer til appen som f.eks få GPS posisjon, bruk kameraet bak på mobiltelefonen, o.l. (Se vedlegg 3 , Videooverføring fra Hjelp 113-appen til AMK)

4.5 Litteratursøk og aktuell eksisterende forskning

Aktuell litteratur er viktig for å kunne orientere seg om hva som er gjort tidligere, samt å kunne tilegne seg den kunnskapen som er viktig for å få nok innsikt til å gjennomføre egen studie.

I dette kapittelet vil jeg kort beskrive litteraturen jeg har benyttet, samt hvilken aktuell forskning jeg har funnet, både norsk og internasjonal.

4.5.1 Litteratursøk

Det meste av litteraturen som er benyttet i denne oppgaven er hentet fra pensumlitteratur i faget, samt forelesningsnotater fra forelesninger i faget. Der er også foretatt tilfeldige søk både i NTNU sitt bibliotek Oria, og Google.schooler.com er benyttet. Videre har jeg benyttet Lovdata, som har en sentral rolle i forvaltningen av det rettslige informasjonssystemet, blant annet ved en kontinuerlig konsolidering av hele det norske regelverket. Jeg har også benyttet presentasjoner som er utarbeidet for selve utviklingsprosjektet, samt behovskartleggingen utført av Making Waves.

4.5.2 Eksisterende forskning

I 2019 utførte direktoratet for E-helse en undersøkelse i helsesektoren for å kartlegge status for informasjonssikkerheten blant norske helseforetak. Deltagerne i undersøkelsen var de fire regionale helseforetakene (RHF), Helse Nord, Helse Midt, Helse Vest og Helse Sør-Øst, noen helseforetak og deres IKT-tjenesteleverandør. Dette er Sykehuspartner, Helse Vest IKT, Hemit, Helse Nord IKT, samt Norsk Helsenett. Kartleggingen baserer seg på sammenlignbare indikatorer, så som styring og kontroll, risikostyring, beredskap og hendelseshåndtering, samt sikkerhetskultur og kompetanse.

Alle RHF oppgir at de gir føringer for informasjonssikkerhetsarbeidet til regionens felles IKT-tjenesteleverandør og HF. Informasjonssikkerheten oppfattes derfor som forankret og plassert på rett nivå.

Samtlige nivå, og regionsnivået spesielt svarer at de benytter Norm for informasjonssikkerhet og personvern i helse -og omsorgstjenesten som utgangspunkt for utforming til krav. Dette bekrefter dermed at Normen er godt innarbeidet som felles kravsett for sektoren.

Et av hovedfunnene var at de regionale ikt-leverandørene skåret gjennomsnittlig høyere enn sammenlignbare IKT-leverandører i helsesektoren globalt.

(Nasjonal e-helsemonitor, 2019)

Videokonferanse og mobiltelefoner: Nye muligheter for 113

Allerede i 2011 så forskere på effekten av å ta i bruk videosamtale mellom AMK-operatørene og innringer. I en doktorgrads-studie, utført av stipendiat Stein Roald Bolle ved Universitetet i Tromsø, har 180 gymnaselever og en akuttmedisinsk kommunikasjonssentral (AMK-sentral) deltatt i simulerte forsøk med hjerte-lungeredning.

Resultatene viser at ungdommene syntes det var tryggere å ha videosamtale med AMK-sentralen i stedet for vanlig telefonforbindelse. .. – Å vite at noen ser om det du gjør er riktig, og samtidig gir deg korrigerende instruksjoner, ga ungdommene trygghet, sier Bolle… Det var ikke bare ungdommene som foretrakk videosamtaler, men også sykepleierne som tok imot samtalene mente at levende bilder var bedre.

Sykepleierne fikk en bedre forståelse av ulykkessituasjonen når de hadde videosamtaler.

– De oppklarte misforståelser raskere og kommunikasjonen ble mer effektiv ved video, sier Bolle.

– Teknologien er jo der. Mange har videomuligheter på mobilene sine, men ingen AMK-sentraler har i dag mulighet til å ta imot videosamtaler, avslutter Bolle.

(Øvreberg, 2011)

Smarttelefonens muligheter i prehospital tjeneste En kvalitativ studie av AMK og ambulansetjenesten i Tromsø.

Denne studien, som ble gjennomført i 2013, handler om kombinasjonen av telemedisin og akuttmedisin. En har gjennom en eksperimentell studie, ønsket å undersøke om de siste års utvikling innen mobiltelefonteknologi har gitt muligheter som kan utnyttes av AMK. I studien ble det testet kvaliteten på videokonferanse mellom lekfolk og AMK-sentral. Det ble i denne studien konkludere med at videokonferanse kan gi god lydkvalitet både til og fra skadested, men at bildekvaliteten avhenger av lysforholdene. (Hotvedt & Melbye, 2013)

Operatørkrav til avstandsoppfølgingssystem i et kommunalt responssenter En brukersentrert tilnærming

I en studie utført av Brørs og Nordstrøm i 2017, har de forsøkt å identifisere krav operatører i et responssenter stiller til systemer for avstandsoppfølging. Gjennom

kvalitative, brukersentrerte metoder har de bygget forståelse for og identifisert 30 operatørkrav for systemer for avstandsoppfølging.

Hovedfunnene i studien er bla. knyttet til tilgjengelighet av informasjon for operatøren, behov for en digitalisert egenbehandlingsplan, at prosess- og beslutningsstøtte understøtter arbeidsflyten i responssenteret, hvor stor verdi prototyping har og at brukerinvolvering i designprosesser er en viktig faktor for å lykkes med utvikling og implementering av IKT-systemer i helsevesenet. (Brørs & Nordstrøm, 2017)

Personvern i elektronisk pasientjournal -Til hinder for forsvarlig helsehjelp?

Oppgavens tema er elektronisk pasientjournal og personvern. Dette er et tverrfaglig tema som berører både helseretten og personvernretten. Problemstillingen som reises er om reglene for personvern i elektroniske pasientjournaler er til hinder for forsvarlig helsehjelp.

I dette studie om personvernet er et hinder for forsvarlig helsehjelp konkluderes med at et godt personvern er avgjørende for at pasienten skal ha tillit til helsetjenestene. Denne tilliten er grunnlaget for at helsetjenesten skal fungere godt og at helsehjelpen som ytes er forsvarlig. Man kan derfor ikke risikere at pasienten frykter for at informasjon kommer på avveie, ei heller at helsepersonell unnlater å utveksle informasjon. Personvern er , etter forfatterens mening, ikke et problem som man skal forsøke å finne løsningen på, men en verdi som skal bevares og være et mål i seg selv.

(Kandidat 670 Det juridiske fakultet UIO, 2016)

Mobil App med helseopplysninger – en mulighetsstudie innenfor det norske lovverket

I en masteroppgave fra 2013 har Knut Henrik Andersen sett på hvordan handlingsrommet i norske lovbestemmelser er omkring personvern og informasjonssikkerhet for etablering av HelseApp-tjenester som baserer seg på mobil teknologi og nettsky-løsninger. Han konklusjon med at lovverket er komplekst og kan være vanskelig å tolke og anvende i lys av App-økologien. En av årsakene til dette kan være at lovverket er utviklet for 13-17 år siden. En raskt voksende App-økologi og nettsky-økologi som ikke kjenner landegrenser, slik vi er vant til, kan dette være problematisk. At handlingsrommet preges av mer usikkerhet. Det kan konkluderes med at det stilles store utfordringer til den som skal etablere HelseApp tjenester i samsvar med det norske lovverket. (Andersen, 2013)

Risikovurdering ved lovpålagte tilsyn med informasjonssikkerhet i helseforetak

Ali Muhammed Barsinje har i sin masteroppgave fra 2010 sett på hvilke forventninger man bør kunne stille til informasjonssikkerhet i større virksomheter og hvilke utfordringer det statlige tilsynet med informasjonssikkerheten stilles ovenfor. I oppgaven vektlegges det resultater fra forsknings og utviklingsarbeid knyttet til informasjonssikkerhet og risikoanalyser. Studien konkluderer med at Helsetilsynet har systematiske opplegg både for intern opplæring av tilsynsførere og gjennomføring av tilsyn. Men ingen av disse har et særlig fokus på informasjonssikkerhet. Dette avspeiles også i det faktum at

informasjonssikkerhet ikke har noen tydelig plass i tilsynsrapportene som skrives. (Barzinje, 2010)

4.5.3 Internasjonal forskning

An Analysis of Next Generation 9-1-1: Video Calling for Emergency Situations

I en studie fra 2017 utført i Kanada, har man sett på hvilke fordeler og ulemper innføringen av videosamtale kan gi. Studiet er utført i tre ulike «emergency communications centre" ECC. Det er gjennomført observasjoner og dybdeintervju i tre ulike ECC sentre for å undersøke disse punktene.

Resultatene viser det videosamtaler kan gi verdifull informasjon om en situasjon og bidra til å overvinne utfordringer for innringer. Dette kan være uklarhet i informasjon som er gitt, beliggenhet, og kommunikasjonsproblemer. Men en fant også at ved å innføre mulighet for videosamtale mellom operatør og innringer, kan det reises spørsmål rundt kontroll, overbelastning av informasjon, og personvern dersom systemer ikke er utformet robust og godt. Disse resultatene peker på behovet for å tenke på flere alternative tekniske løsninger ved innføring av nødvideo-anrop. Dette kan være alt fra lydanrop ledsaget av bilder eller videoklipp, til enveis video strømmer, til toveis videostrømmer der kamerakontroll og kameraarbeid må utformes nøye.

Live video footage from scene to aid helicopter emergency medical service dispatch: a feasibility study

I 2018 ble det gjennomført en studie utført i tre distrikt helsedistrikt i Sør-Øst England som ønsket å se på hvordan mulighet for å ta videosamtale i bruk i kommunikasjonen mellom innringer og nødkommunikasjonssentral. De ønsket å fokusere på i hvor stor grad innringer akseptere å benytte videosamtale, samt mulighet for å benytte videoopptaket som et hjelpemiddel i koordinering og utkalling av ambulansehelikopter til hendelsessted.

I studien ville de ha svar på følgende spørsmål: I hvilken grad aksepterer innringer bruke videooverføring fra skadested og gir HEMS-utsendelsessystemet mulighet for å bruke videoopptaket som et hjelpemiddel i HEMS utsendelse. Resultatene peker i retning av at sanntids videoopptak fra ulykkesstedet er et akseptabelt og gjennomførbart hjelpemiddel for HEMS-utsendelse, men ytterligere studier er nødvendig for å få enda større utbytte av tjenesten ved å forbedre nøyaktighet i HEMS-utsendelsen. Der er også et potensiale for at tjenesten kan forbedre samarbeid nødkommunikasjonssentralene i ulike distrikt og på tvers av ambulansetjenester.

Som vi ser av de eksempler på både nasjonal og internasjonal forskning, så er det fokusert på de muligheter som ligger i den teknologiske utviklingen.

Det er både beskrevet et ønske og et behov, men også en muligheter for å utvikle en slik tjeneste. Jeg vil derfor i denne oppgaven se på hvordan en slik tjeneste som muliggjør videosamtale mellom AMK og innringer utfordrer informasjonssikkerheten i tjenesten, ved å gjennomføre en risikoanalyse av en slik tjenesten

5 Metode og material

Formålet med dette metodekapitlet er å redegjøre for den vitenskapelige metoden som er benyttet for å belyse forskningsprosjektet mitt. Jeg vil redegjøre for min motivasjon for å velge AMK-sentralen som fokusområde for min oppgave, jeg vil se på hva som er viktig å passe på i forhold til forskningsetikk. For å ha forståelse for i hvilken sammenheng tjenesten skal fungere, vil jeg se på oppbygningen av AMK-sentralene, med roller, ansvar og hvilke eksisterende dataprogrammer AMK-operatøren benytter i sitt arbeid. Når det gjelder datainnsamling, så gjorde omstendighetene rundt koronapandemien det slik at jeg har benyttet bla. spørreundersøkelse for å få innsikt. Dette kapittelet beskriver derfor spørreundersøkelsen jeg utførte blant noen få AMK-operatører.

Forskningsspørsmålet mitt er hvordan informasjonssikkerheten er ivaretatt i en tjeneste som tilbyr videosamtale mellom AMK-operatør og innringer. Jeg har derfor sett på hvordan man kan sikre metodisk og systematisk risikostyring for en tjeneste som behandler sensitive persondata. Jeg har sett på hvilke sikkerhets-krav som må stilles til en slik tjeneste, og beskrevet hvordan man kan gjennomføre en sårbarhets og risikoanalyse for en tjeneste som behandler sensitive personopplysninger. I kapittel 5 vil jeg se på svarene fra spørreundersøkelsen, mens jeg i kapittel 6 vil utføre en risiko og sårbarhetsanalyse av tjenesten basert på metoden beskrevet i dette kapittelet.

I forskningsprosjekt mitt, som handler om hvordan informasjonssikkerhet er ivaretatt i tjenester som muliggjør videosamtale mellom AMK og innringer, trenger jeg innsikt fra fagfeltet. I dette kapittelet vil jeg derfor beskrive kort hvordan den akuttmedisinske kjeden fungerer i Norge. Jeg vil videre se på hvordan AMK er organisert, hvilke krav som stilles til operatøren, samt hvilke ansvars- og -arbeidsoppgaver en AMK-operatør har. Jeg vil se på hvilke verktøy de har tilgjengelig i sitt arbeid, både når det gjelder triagering av pasient, men også for kommunikasjon og samhandling med bl.a. ambulansetjenesten. Jeg går kort inn på hvordan en forventer at behovet for AMK vil utvikle seg i fremtiden, både med tanke på kapasitet, men ser også på hvordan en forventer at behovet for faglig spesialkompetanse vil endre seg.

For å få en bedre forståelse for i hvilken sammenheng videotjenesten skal benyttes, var det planlagt at jeg skulle hospitere både på AMK og ambulansetjenesten. Dette for å få førstehånds informasjon om bl.a. arbeidsflyt og samhandling mellom operatørene og innringer.

Dette utgår pga. Coronapandemien Det ble derfor foretatt en spørreundersøkelse blant AMK-operatører som har prøvd ut en videotjeneste til bruk mellom innringer og AMK-operatøren istedenfor.

For å få bedre innsikt i hvordan informasjonssikkerheten blir ivaretatt i det ønsket om å skape en best mulig tjeneste for videosamtaler for ansatte ved AMK, vil jeg utføre en risiko og sårbarhetsanalyse (ROS-analyse) av skissert tjeneste, basert på prinsipper for sikkerhetsstyring. En vurdering av personvernkonsekvenser, (DPIA) ved bruk av tjenesten, vil også være et viktig bidrag for å vurdere hvordan informasjonssikkerheten i tjenesten er i varetatt, men det vil føre for langt å gjennomføre innenfor rammene av denne oppgaven.

I denne oppgaven er deler av datainnsamlingen foretatt av andre. Jeg sikter her hovedsakelig til behovskartleggingen som Making Waves har utført for denne type

tjeneste. Denne kartleggingen er utarbeidet på bakgrunn av forskningsmetoder som simulering, dybdeintervju, medlytt og rollespill. Dataene fra disse aktivitetene er så bearbeidet og registrert systematisk.

Tema blir presisert i form av et forskningsspørsmål som skal ha basis i tidligere forskning og teori. Forsknings-spørsmålet skal være klart formulert og så presis som mulig. Definering og operasjonalisering av sentrale begreper, spørsmålet må gjøres før undersøkelsen starter. (Sigrunn Drageset, 2009)

For å få svar på de spørsmål man søker, er det viktig å ha en overordnet plan over hvordan man skal gå frem for å få svare på problemstillingene. Dette innebærer bl.a. valg av tema og formulering av problemstilling. Hvilke materiale og data trenger man for å få svar på det man søker å belyse. Hvilken metode for datainnsamling er mest velegnet og gir det mest korrekte bildet. Vil valg av tidsperiode og sted ha innvirkning på hvilke data som kommer frem? Videre vil de innsamlede data påvirke hvilken analysemetode man velger for å bearbeide disse.

I all forskning bør metodevalget bestemmes ut fra problemstilling. Hvilken fremgangsmåte kan gi svar på det som skal undersøkes? (Kaarbø, 2009 - 2019)

5.1 Akuttmedisinsk kjede i Norge

Den prehospitale akuttmedisinske kjeden har som samfunnsoppdrag først og fremst å være — Et helhetlig system for håndtering av akutte sykdommer og skader utenfor sykehus. (NOU 2015: 17 Først og fremst, 2015)

Den akuttmedisinske kjeden består av fastlege, legevakt, kommunal legevaktsentral, akuttmedisinsk kommunikasjonssentral (AMK-sentral), bil-, båt- og luftambulanse, samt akuttmottak i sykehus. Kjeden representerer en sammenhengende rekke av tiltak for å sikre akutt helsehjelp fra hendelsessted, inkludert publikums innsats, fram til definitiv behandling. (Meld. St. 16 Nasjonal helse- og omsorgsplan (2011–2015), 2011) For å kunne yte akutt helsehjelp til befolkningen er man avhengig av at alle ledd fungerer, og den akuttmedisinske kjeden er således et samlet mål på materiell beredskap, beredskap hos personell og overordnet organisering for Norsk helsetjeneste.

5.2 Akutt Medisinsk Kommunikasjonssentral - AMK

AMK-sentral er telefonsentralen som besvarer det medisinske nødnummeret 1-1-3 og overvåker ambulansetransporter. AMK-sentraler er bemannet av helsepersonell, vanligvis sykepleiere og ambulansearbeidere.

Norge har 19 AMK-sentraler som yter spesialisthelsetjenester til hele befolkningen. Geografisk utbredelse omfavner urbane byområder til rurale og store, lett befolkede områder. AMK-sentralene disponerer store ressurser, som yter akutt hjelp, der hvor behov oppstår, uavhengig av beliggenhet. (Helsedirektoratet, 2020)

Medisinsk nødmeldetjeneste er en nasjonal organisasjon som skal sette de hjelpesøkende i fokus og hvor grunnverdiene er nærhet, likhet, felleskap og trygghet. Befolkningen skal i akuttmedisinsk situasjoner møte helsepersonell (fagkyndighetsprinsippet) som disponerer helsetjenestens samlede prehospitale ressurser. (Utredning AMK-sentralene, 2016)

5.2.1 AMK operatøren

Utdanning

I en kartlegging av den akuttmedisinske kjeden, utført av NAKOS er det oppgitt at det i AMK er krav om at medisinsk operatør skal være sykepleier eller ambulansearbeider. For de fleste AMK-sentralene hadde de ansatte sykepleiergodkjenning som høyeste godkjenning. Ved en sentral var samtlige av de ansatte sykepleiere med videreutdanning. Noen sentraler oppga at ansatte med paramedic-utdanning utgjorde en del av staben deres. (Nakos - prehospital akuttmedisin, 2019)

Roller på AMK

Operasjonsleder: Leder og koordinerer virksomheten og er leder for mannskaper på vakt.

Medisinsk operatør: Mottar 1-1-3-samtaler, vurderer meldingen, veileder innringer og beslutter primærtiltak. Medisinsk operatør er autorisert sykepleier eller ambulansearbeider og har særskilt opplæring og godkjenning.

Ressurskoordinator: Håndterer operative oppgaver i AMK. Styrer pre-hospitalt senters operative enheter, prioriterer oppdrag med samme hastegrad og fordeler disse til operative enheter. Sekundært håndterer ressurskoordinator andre henvendelser.

Luftambulansekoordinator: er ressurskoordinator dedikert til koordinering av ambulansehelikoptre og ivareta "flight following" for operatøren.

(Oslo universitetssykehus OUS, 2020)

AMK i fremtiden

Visjon om fremtidig akuttmedisinsk kjede er i korthet redde liv, spare leveår, redusere risiko for varig men og lindre lidelse. Målet oppnås best med rasjonell og samordnet ressursbruk. Samtidig trengs det større grad av standardisering også av akutte eller uplanlagte pasientforløp, med felles forståelse av ansvar, roller og handlingsmønster. Nødmeldetjenesten, spesielt AMK-sentralene, skal støtte og koordinere pasientforløp til pasienten er ivaretatt på bestemmelsessted. Samtidig skal nødmeldetjenesten legge til rette for minst mulig risiko for personellet i felt. (Kokom, 2018)

I en utredning utført av helse og omsorgsdepartementet i 2016, ser en for seg en befolkning og et helsevesen i rask endring/utvikling. Det er betydelig usikkerhet knyttet til denne utviklingen, men utredningsgruppen mener at det er overveiende sannsynlig at belastningen på AMK-sentralene vil øke både i form av et raskt økende antall henvendelser, men også i form av mer komplekse oppgaver og vurderinger, samt mer krevende samarbeidsgrensesnitt mot interne og eksterne samarbeidspartnere.
(Utredning AMK-sentralene, 2016)

Frem mot 2030 vil befolkningen øke noe, men andelen eldre vil øke sterkt, med tilsvarende reduksjon i andelen yngre. Aldersgruppen over 67 år vil øke med 64 %, mens gruppen over 80 år vil øke med 56 %.

Uavhengig av andre faktorer, vil befolkningsøkningen og økt antall eldre innebære økt etterspørsel etter helsetjenester – også akuttmedisinske tjenester.
(Utredning AMK-sentralene, 2016)

En fortsatt antatt økning i forekomsten av hjerneslag vil øke behovet for kompetanse og akuttmedisinske ressurser for å sikre rask identifisering av symptomer på slag og rask transport til sykehus for kvalifisert diagnostikk og behandling.
(Utredning AMK-sentralene, 2016)

Det er knyttet betydelig usikkerhet til hvordan utvikling av nye metoder for medisinsk diagnostikk og behandling vil påvirke de prehospitale tjenestene.

En vet likevel noe om hvordan de senere års utvikling på enkelte områder har påvirket tjenestene. Innføring av akutt PCI til pasienter med hjerteinfarkt gir bedre overlevelse og funksjonsnivå sammenlignet med annen (trombolytisk) behandling. Behandlingen stiller nye krav til kompetanse både hos AMK- og LV- operatører og ambulansepersonell.

En tilsvarende utvikling har man sett for behandling av pasienter med mistanke om hjerneslag. Tidlig behandling av pasienter med hjerneinfarkt redder liv og begrenser helseskaden. Forutsetningen er rask identifisering av symptomer og transport til sykehus med utstyr og kompetanse for diagnostikk (CT) og behandling.
(Utredning AMK-sentralene, 2016)

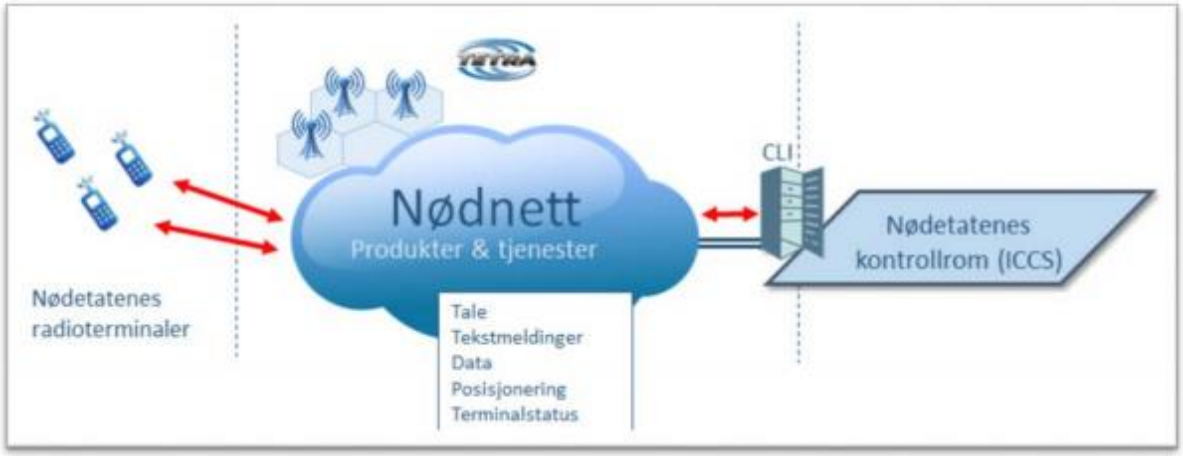
Flere og mer differensierte behandlingstilbud vil fordre bedre og sikrere prehospitale vurderinger, herunder 20 bedre metoder for prehospital diagnostikk hvor bl.a. ambulansepersonell og AMK-sentraler må forventes å ha en sentral funksjon.
(Utredning AMK-sentralene, 2016)

Ved siden av mottak av henvendelser til medisinsk nødnummer 1-1-3 og alarmering av helseressurser, har AMK-sentralene en viktig rolle i forhold til å gi innringer helsefaglige råd. Veiledning i livreddende førstehjelpstiltak som f.eks. hjerte- og lungeredning (HLR), etablering av frie luftveier, stansing av blødninger og forebygging av nedkjøling inngår i denne funksjonen. Nyere forskning viser at telefonveiledet HLR og bruk av hjertestarter har stor betydning for overlevelse ved hjertestans.
(Helse- og omsorgsdepartementet, 2016)

5.2.2 AMK sine IKT-systemer

5.2.2.1 ICCS nødnett

ICCS er en forkortelse for «Integrated Communication and Control System» og er kommunikasjonsentral-utstyret levert av Frequentis.



Abonnementet gir nødetatene tilgang til Nødnett funksjonalitet via ICCS og CLI. ICCSen er en server med betjeningsprogramvare og kommunikasjonsgrensesnitt både mot Nødnett og offentlig nett og utgjør kjernen i nødetatenes kommunikasjonssentralløsninger. ICCSen gir operatøren oversikt over blant annet radioterminalressurser, radioterminalanrop, talegrupper og innkomne telefonsamtaler. Abonnementet gir tilgang til tjenester i Nødnett som tale, SDS, data, posisjonering og terminalstatus Tale. Talefunksjonaliteten gir Kontrollrommet muligheten til å administrere og kommunisere i talegrupper og ringe en-til-en i Nødnett. Tekstmeldinger (SDS). Funksjonaliteten gir muligheten til å sende og motta tekstmeldinger i Nødnett som statusmeldinger, utalarmering og/eller sikkerhetsalarmer. Data Data-funksjonaliteten gir mulighet til å sende og motta datapakker i Nødnett. Posisjonering Radioterminaler med innebygd GPS funksjonalitet kan tilrettelegges for å sende posisjoneringsinformasjon via Nødnett til kontrollrommet. (https://www.nodnett.no/globalassets/dokumenter/bestillingsskjema-og-vilkar/produktvilkar---kontrollromstilknytning-for-nodetatene-1.3.pdf)

Grensesnittet gir også mulighet for å hente ut posisjonering og status for radioterminaler, samt andre nødvendige funksjoner man trenger i et kontrollrom.

(Nødnett, 2017)

5.2.2.2 TRANSmed

TRANSmed er et system som benyttes i AMK-sentraler og i ambulanser. Systemet benytter seg av kart og adresser for å identifisere innringers posisjon. I det samme kartet kan man på en enkel måte ha oversikt over hvor ambulansene befinner seg. Skriftlige meldinger kan sendes til og fra ambulansen.

I ambulansen kan man i eget kartverk se hvor man skal hente pasient, samtidig som man til enhver tid ser sin egen posisjon.

Det er viktig for operatør i en AMK-sentral raskt å identifisere innringers posisjon. Mange av innringerne er i en situasjon hvor man ikke kan redegjøre for seg. Med hjelp av TRANSmed kan man enkelt identifisere innringers posisjon. Når en nødmelding kommer inn, finner systemet automatisk eiendommens posisjon, og viser denne i kartet ved hjelp av symboler. Selv i områder uten gateadresse blir posisjonen vist. Dette sikrer en effektiv varsling til ambulanse. (Locus, 2020)

TransMobil er tilsvarende system ute i ambulansene.

- Viser detaljert oppdragsinformasjon
- Håndterer flere oppdrag samtidig
- Detaljerte kart for navigasjon

TransMobile har detaljerte kart med navigasjon som viser egen posisjon, og oppdragsposisjon. Inne på vaktsentralen viser TransMed alle mobile enheter med posisjon og status på oppdragene. (Locus, 2020)

5.2.2.3 AMIS (Akuttmedisinsk informasjonssystem)

AMIS er et IT-systemverktøy som benyttes ved alle AMK-sentraler i landet, samt legevaktsentraler og i ambulansetjenesten. Dette systemet benyttes til registrering og

dokumentering av opplysninger fra nødsamtaler og andre hendelser som operatørene håndterer. AMIS er et støttesystem for AMK-sentraler og brukes til å koordinere arbeidet i nødmeldetjenesten. Det brukes blant annet til å motta og registrere nødmeldinger og opprinnelsesmarkering, bestille ambulansetransport og sende henvendelser til legevakt. Videre kan en gruppere, sortere og prioritere oppdrag samt koordinere ventende oppdrag. Man kan også få tilbakemelding fra ambulansen om status og tidspunkter. Ved større ulykker registreres aksjonslogg og pasientoversikt. Hvis man i etterkant skulle ha behov for å se på tidligere data kan man enkelt, ved hjelp av AMIS, søke opp tidligere hendelser, oppdrag og pasienter. Samtidig kan man også bruke AMIS til å se på statistikk. AMIS er integrert med telefoni, radio, kart og flåtestyring. Dermed kan operatøren koordinere og betjene alt dette fra ett og samme tastatur. Videre fungerer AMIS også som journalsystem ved at alle hendelser arkiveres. Tidligere hendelser kan hentes frem på grunnlag av dato, tidspunkt, sted, adresse, ambulanse, innringer og/eller type hendelse. (Kvinge, 2013)

5.2.2.4 Kontorapplikasjoner

I tillegg har alle operatørene en skjerm med mer vanlige kontorapplikasjoner. Denne bruker til bla. oppslag på nettsider, så som Bliksund Web. (Making Waves, 2019)

5.2.2.5 NORSK INDEKS FOR MEDISINSK NØDHJELP

AMK bruker et verktøy kalt Norsk indeks for medisinsk nødhjelp når de vurderer hastegrad og responsmønster for hvert enkelt oppdrag. Norsk indeks er et hjelpemiddel for helsepersonell som besvarer medisinske nødmeldinger via 1-1-3, og har vært i bruk i Norge siden 1994. Norsk indeks for medisinsk nødhjelp er et verktøy utarbeidet av Den norske lægeforening. Det er et oppslagsverk som bidrar til at man bruker noenlunde like begreper og den er samtidig en norm for god faglig standard i nødmeldetjenesten. Indeks baserer seg på medisinsk kunnskap om sammenhengen mellom symptomer, problemer, hendelser, skademekanismer og medisinsk grad av hast og hjelpenivå. Den medisinske indeksen gir en standard metodikk for hvordan man kommuniserer og handler ved akutte medisinske tilstander og ulykker. Den er en mal for hvordan man innhenter informasjon og kommuniserer med innringer i ulike akuttmedisinske situasjoner. Samtidig inneholder den gode råd, instruksjon og veiledning. Utfra forskjellige kriterier er Norsk medisinsk indeks også en mal for bestemmelse av hastegrad og responsmønster ved de ulike tilstandene.

AMK fordeler oppdrag til ambulansene i tre hastekategorier:

- ”Akutt” – Rød respons: Øyeblikkelig hjelp. Utrykning med blålys og sirener.
- ”Haster” – Gul respons: Oppdrag som skal avvikles uten opphold, men uten bruk av blålys og sirener.
- ”Vanlig” – Grønn respons: Bestilte oppdrag og oppdrag uten særlig hast.

Det kan lages lokale tilpasninger til Norsk indeks, i forhold til spesiell tilgang på ressurser, geografiske og klimatiske forhold. Den medisinskfaglig ansvarlige lege ved den enkelte sentral eller legevakt avgjør hvorvidt retningslinjene skal gjelde på det aktuelle sted, eventuelt hvorvidt det skal fastsettes bestemte unntak fra disse. Norsk indeks er ikke noen fasit, men et hjelpemiddel for personellet som skal håndtere henvendelser om akuttmedisinsk bistand.

5.3 Datainnsamling

Datainnsamling er en sentral fase i undersøkelsesprosessen. En skiller mellom primærdata, som innebærer at forskeren samler inn opplysninger for første gang og sekundærdata, som er allerede eksisterende data som blir analysert. (Ellingsen, 2009)

I denne studien var den opprinnelige planen å selv samle inn primærdata fra både dybdeintervju og hospitering, mens jeg skulle hente sekundærdata fra bl.a. behovskartlegging utarbeidet utført av Making Vawes. Men corona-pandemien satte en stopper for muligheten for å hospitere. Jeg har derfor benyttet spørreundersøkelse for deler av datainnhentingen. Dette er en effektiv og effektiv form for datainnsamling, når smittevernhensyn fører til at personlig oppmøte ikke er anbefalt.

5.3.1 Spørreundersøkelse

Intervjuene foregå i et spørreskjema sendt på mail til seksjonsleder på utvalgte AMK-sentraler, hvor utvalgskriteriet var at sentralen hadde deltatt i pilotprosjekt for innføring av Videotjenesten.

Man tilstreber ofte å ha et strategisk utvalg informanter, bestående av et rikt og variert utvalg av personer, for å få dekket alle sider ved problemstillingen. En forutsetning er at deltakerne har det som studeres til felles. (Svensberg & Kristine Heitmann, 2014). Informantene vil bidra med størsteparten av datainnsamlingen, så det blir derfor viktig å få ett representativt utvalg. Utvalgskriterier var AMK-operatør som har deltatt i utprøving av den nye tjenesten.

Det ble viktig innledningsvis i spørreskjemaet informert om at det er frivillig å delta og at det er operatørens oppfatning som er viktig at kommer frem. Det ble også innledningsvis informert om at det vil ikke bli spurt om sensitive opplysninger i undersøkelsen, men all informasjon vil allikevel bli anonymisert.

5.3.1.1 Spørreskjema

Formålet med undersøkelsen er å få litt innsikt i hvordan AMK-operatørene opplever at videotjenesten fungerer i sitt med å besvare nødmeldinger. Det er videre vektlagt hvordan operatøren vurderer informasjonssikkerheten i tjenesten. Besvarelsene skal brukes får å få ett rikere bilde av hvordan tjenesten fungerer, samt om der er åpenbare sårbarheter i tjenesten.

Spørreundersøkelsen ble sendt til prosjektleder for utvikling av videotjenesten som er knyttet til Hjelp113-appen. Han distribuerte spørreundersøkelsen videre til AMK-sentraler som har deltatt i pilotperiode for utprøving av tjenesten

Det var ønskelig med et stort antall respondere, men det viste seg vanskelig å få operatørene til å delta i undersøkelsen. Årsaken til dette vet vi ikke sikkert, men stort arbeidspress og manglende informasjon før undersøkelsen ble sendt ut kan være noe av forklaringen. Deltagernes anonymitet ble godt ivaretatt ved at prosjektleder stå for all utsendelse og innsamling av spørreundersøkelsene. Det var bare selve skjemaet som ble sendt videre til meg. På den måten fikk jeg ikke tilgang til mailadressen til deltagerne heller.

Det har vært viktig for meg å lage en kort og presis spørreundersøkelse, som ikke oppholder AMK-operatørene unødig. Spørreundersøkelsen består av 18 spørsmål, med en

kombinasjon av avkrysningsbokser og kommentarfelt. Det vil normalt ta 5- 10 minutter å fylle ut skjemaet.

Spørreundersøkelsen har ett enkelt og lettfattelig språk, og det er lagt vekt på å være så nøytralt som mulig. Det vil si at det er ikke brukt ord som kan oppfattes som spesielt positive eller spesielt negative.

Der kom dessverre inn alt for få svar til at denne spørreundersøkelsen kan vektlegges i noen særlig grad og har derfor ingen stor vitenskapelig tyngde, men er med på å bekrefte de vurderinger som jeg kommer frem til i risiko-vurderingen. Svarene er gjengitt som en oppsummering av spørreundersøkelsen, hvor den enkeltes kommentar er tatt med.

Årsaken til den svake responsen for undersøkelsen kan være flere. Det kan være for dårlig informasjon om spørreundersøkelsen, stort arbeidspress blant AMK-operatørene eller manglende engasjement og eierskap til utprøving av tjenesten.

Det er en ganske enkelt utformet undersøkelse, så det skulle ikke være hverken krevende eller tidskrevende å svare på den.

Der var også satt ganske god tidsfrist for å svare, slik at selv om de ansatte går turnus og ikke er regelmessig på jobb, skulle det være god anledning til å rekke å besvare innen fristen

5.4 Risikostyring

Hovedmålet med selve risikostyringen er å oppnå akseptabel risiko. Derfor skal hovedproduktet fra hver gjennomført risikovurdering være en oversikt over uakseptable risiko og en liste med risikoadresserende tiltak utarbeidet i den hensikt å gjøre risiko akseptabel. (Mathiesen Slyngstadli, 2017) Risikostyring vil si å identifisere, vurdere, håndtere og følge opp hendelser som kan påvirke måloppnåelsen negativt. Risikostyring henviser til de systematiske aktivitetene for å vurdere og håndtere risiko som en del av styring og kontroll av informasjonssikkerhet. (Nasjonal e-helsemonitor, 2019)

Risikostyring øker sannsynligheten for måloppnåelse. Den gir bedre grunnlag for fastsettelse av realistiske mål og ambisjonsnivå. Videre blir sammenhengen mellom mål, risiko og kontrollaktiviteter/tiltak tydelig gjort. Den gir bedre grunnlag for prioritering og ressursstyring og bedre beslutningsgrunnlag. Risikostyring gir også en mer proaktiv og forutsigbar styring. (Direktoratet for økonomistyring, 2016)

Risikovurdering er en samlet prosess som består av planlegging, risikoanalyse og risikoevaluering. Dette handler om å identifisere farer og uønskede hendelser, analysere og evaluere risiko, og identifisere tiltak som kan redusere risikoen. (Standard Norge, 2020)

5.4.1 Verdi

Primærverdier for risikovurderingen av informasjonssikkerhet er informasjon og arbeidsprosesser. (Mathiesen Slyngstadli, 2017)

5.4.2 Usikkerhet

Usikkerhet er en tilstand der det er mangel på informasjon, manglende forståelse av, eller kunnskap om en hendelse, dens konsekvens eller muligheten for at den skal forekomme. (Direktoratet for økonomistyring, 2016)

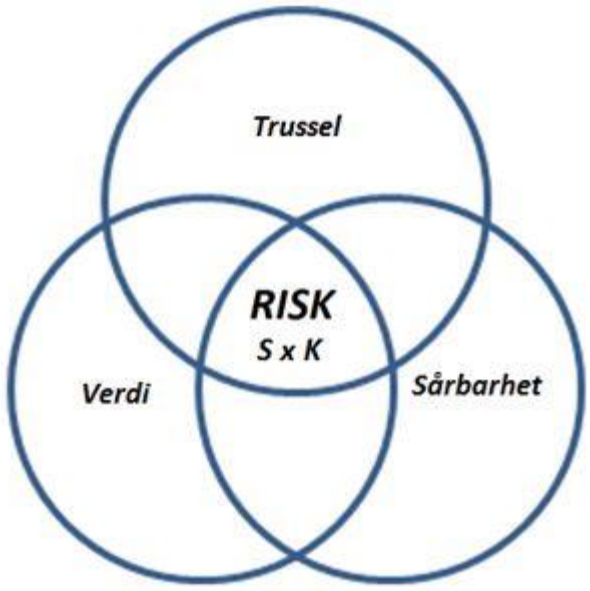
5.4.3 Risiko

Risiko er et begrep som gjerne har litt forskjellig betydning avhengig av situasjonen hvor det benyttes. All bruk av begrepet har stort sett det til felles at vi setter noe på spill (risikerer) for å få en gevinst. Det vi setter på spill refereres til som en verdi. Når risiko skal vurderes så blir det gjerne angitt med 3 hovedkomponenter:

- En hendelse som eksponerer en verdi for et tap
- Konsekvenser av tapet
- Sannsynligheten for at tapet forekommer.

  (Mathiesen Slyngstadli, 2017)

En spesifikt risikodefinisjon for Infosek er: "Potensialet for at en gitt trussel vil utnytte sårbarheter for å få urettmessig tilgang til en verdi eller gruppe av verdier og dermed forårsake skade på organisasjonen." (Mathiesen Slyngstadli, 2017)



Kombinasjonen av verdi, trussel og sårbarhet kalles gjerne trefaktormodellen og er en nyttig tommelfingerregel for å kunne overordnet vurdere risiko: En verdi kan være sårbar uten å ha en reell trussel. En kritisk verdi kan stå overfor en alvorlig trussel uten å være sårbar. Et system kan være sårbart med en alvorlig trussel uten å håndtere noen verdier med beskyttelsesbehov. I trefaktormodellen så oppstår risiko i skjæringspunktet mellom disse tre og er et nyttig verktøy for å prioritere risiko for videre analyse.

Figur 1 Trefaktormodellen for Informasjonssikkerhetsrisiko (Mathiesen Slyngstadli, 2017)

5.4.4 Sårbarhet

En sårbarhet er en svakhet i systemet som kan utnyttes av en angriper for å få tilgang til en verdi. (Mathiesen Slyngstadli, 2017)

5.4.5 Trussel

En trussel er en potensiell årsak til en utilsiktet hendelse som kan forårsake skade på en av organisasjonens verdier. Når vi gjør trusselvurdering så snakker vi alltid om menneskelige aktører som trusselen, eneste unntaket er trusler som kommer fra Moder jord. En trusselaktør har en motivasjon for å angripe som det er viktig å forstå for å sikre seg. For eksempel så er en skadevare en metode for å realisere intensjonen med angrepet. (Mathiesen Slyngstadli, 2017)

5.4.6 Penetrasjonstest

Penetrasjonstesting er betegnelsen på inntrengnings-forsøk en etisk hacker, ansatt i et IT-sikkerhetsfirma, gjør på oppdrag for eieren av et datasystem, nettverk og/eller applikasjoner.

Formålet med penetrasjonstesting er å identifisere sikkerhetshull og systemsvakheter, og peke på hvor en bedrift eller organisasjon trenger å iverksette kortsiktige og langsiktige tiltak for å styrke forsvaret mot angrep.

Ved å forsøke å bryte seg inn i aktuelle datasystemer simulerer penetrasjonstesterne hvordan en målrettet angriper vil angripe systemer og dermed foretak.(DALE, 2018)

5.4.7 Sannsynlighetsskala

For å kunne sette en sannsynlighetsverdi i en risikovurdering, må vurderingene knyttes til en skala som både angir hvilke sannsynlighetsverdier en risiko kan tillegges, og som spesifiserer betingelsene for å kunne tilordne risikoen en bestemt sannsynlighetsverdi.

Sannsynlighetsverdi	**Vurderingsgrunnlag**		
Skala	**Erfaringsunderlag**	Tiltaksstatus	Trusselbilde
5 - Svært høy **(Veiledende: 90 - 100%)**	Hendelsen har inntruffet mer enn 5 ganger i året	- Sikkerhetstiltak er ikke etablert - Etablerte tiltak kan enkelt omgås av uautorisert personell - Etablerte tiltak er lite robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell	–Foreligger aktører med høy evne og høy vilje til å begå uønskede handlinger
4 - Høy **(Veiledende: 65 - 90%)**	Hendelsen har inntruffet 1 - 5 ganger i året	- Sikkerhetstiltak er ikke implementert i henhold til krav og kun få kompenserende tiltak er etablert - Etablerte tiltak kan med begrenset verktøystøtte og begrenset kunnskap omgås av uautorisert personell - Etablerte tiltak er mindre robuste overfor tekniske endringer og/	–Foreligger aktører med moderat evne og høy vilje til å begå uønskede handlinger
3 - Moderat **(Veiledende: 35 - 65%)**	Hendelsen har inntruffet 1 gang i løpet av 1 til 2 år	- Sikkerhetstiltak er ikke implementert i henhold til krav og kompenserende tiltak er etablert - Omgåelse av etablerte tiltak krever verktøystøtte og kunnskap av uautorisert personell - Etablerte tiltak er nokså robuste overfor tekniske	–Foreligger aktører med moderat evne og moderat vilje til å begå uønskede handlinger

		endringer og/eller utilsiktede handlinger av autorisert personell	
2 - Lav **(Veiledende: 10 - 35%)**	Hendelsen har inntruffet 1 gang i løpet av 2 til 5 år	- Sikkerhetstiltak er etablert og kun mindre mangler i henhold til krav - Omgåelse av etablerte tiltak krever betydelig verktøystøtte og betydelig kunnskap - Etablerte tiltak er meget robuste overfor tekniske endringer og/eller utilsiktede handlinger av autorisert personell	–Foreligger kun aktører med lav evne og lav vilje til å begå uønskede handlinger
1 - Svært lav **(Veiledende: 0 - 10%)**	Hendelsen har inntruffet sjeldnere enn hvert 5 år	- Sikkerhetstiltak er fullt ut etablert i henhold til krav - Omgåelse av etablerte tiltak krever nyeste teknologi og inngående forkunnskap	–Foreligger ingen identifiserte aktører med evne og vilje til å begå uønskede handlinger

(Helse Sør Øst RHF, 2020a)

5.4.8 Konsekvensskala

Konsekvensskala kan dels inn i flere kategorier konsekvens, som konfidensialitet, integritet og tilgjengelighet. I denne oppgaven vil jeg vektlegge konsekvensskala for konfidensialitet.

Konsekvensskala for konfidensialitet beskriver hvilke betingelser som må være oppfylt for å kunne tilordne risikoen en bestemt konsekvensverdi ut fra mulige brudd på konfidensialitet.

Konsekvensverdi	
Skala	*Konfidensialitet*
5 - Svært alvorlig	- Særlige kategorier av personopplysninger blir eksponert ut mot Internett eller andre eksterne, slik at de ikke kan sikres fjerning/sletting. - Særlige kategorier av personopplysninger blir eksponert slik at pasienter motsetter seg fremover å dele slike opplysninger i kritisk behandlingsøyemed - Mer enn 500 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer enn 30 minutter –Særlige kategorier av personopplysninger til mer enn 1 % av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter –Stor andel virksomhetskritisk informasjon er tilgjengelig for uautorisert innsyn i mer enn 30 minutter
4 - Alvorlig	- Manglende systemmulighet til å etterkomme personvernrettigheter som sperring og sletting - Særlige kategorier av personopplysninger blir eksponert slik at pasienter motsetter seg fremover å dele slike opplysninger i behandlingsøyemed –Mellom 200-500 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer 30 minutter –Særlige kategorier av personopplysninger til mellom 0,5 - 1 % av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter –Mindre andel virksomhetskritisk informasjon er tilgjengelig for uautorisert innsyn i mer 30 minutter
3 - Moderat	–Inntil 200 individers særlige kategorier av personopplysninger er tilgjengelig for uautorisert innsyn i mer 30 minutter –Særlige kategorier av personopplysninger inntil 0,5% av individene er tilgjengelig for uautorisert innsyn i mer enn 30 minutter –Stor andel virksomhetssensitiv informasjon
2 - Liten	–Data og informasjon som ikke kan knyttes til enkeltindivid er tilgjengelig for uautorisert innsyn i mer 30 minutter–Mindre andel virksomhetssensitiv interninformasjon er tilgjengelig for uautorisert innsyn i mer enn 30 minutter
1 - Marginal	–Interninformasjon er tilgjengelig for uautorisert innsyn i inntil 30 minutter

(Helse Sør Øst RHF, 2020a)

5.5 Sikkerhetskrav – behandling av personopplysninger

I en tjeneste som behandler personopplysningen må det stilles strenge krav til håndtering av data. Det må utarbeides prinsipper og krav for å oppnå tilfredsstillende vern av informasjonen om personer i en sårbar situasjon.

Kravene under er en sammenstilling av noen av de mest sentrale kravene lover og Normen setter til tjenester som behandler sensitive personopplysninger.

5.5.1 Sikkerhetskrav – autentisering

Ifølge Pasientjournalloven § 22 skal det være tilgangsstyring, logging og etterfølgende kontroll.

Sikkerhetskrav Autentisering

Krav til brukerkontoer.
- Løsningens brukerkontoer bør ikke være lokale, det bør benyttes domenebrukere eller servicebrukere.
- Løsningens brukerkontoer bør ikke kreve mer enn normal brukertilgang på servere og klienter.
- Løsningens brukerkontoer bør være unike per bruker (ikke bruk av felles brukerkonto)
- Løsningens brukerkontoer bør ikke ha løsningsspesifikke brukernavn.
- Løsningens brukerkontoer bør ikke ha løsningsspesifikke passord.
- Løsningens brukerkontoer bør støtte periodisk bytte av passord.

5.5.2 Sikkerhetskrav – Autorisasjon

Med autorisering menes å gi korrekte tilganger til en autentisert identitet.

Det settes en rekke krav til tilgangskontroll for journalsystemer og registre. Pasientjournalloven § 22 sier at "det skal gjennom planlagte og systematiske tiltak sørges for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet". "Dette omfatter blant annet å sørge for tilgangsstyring, logging og etterfølgende kontroll".

Sikkerhetskrav - Autorisasjon – Roller:

Tilganger skal være basert på rollestyring.

Vennligst bekreft at og beskriv hvordan kravet oppfylles, herunder støtte for systemets bruk av roller for autorisasjon.

Sikkerhetskrav - Autorisasjon - Attributtbasert tilgangskontroll:

Rollen og attributtene brukeren har i AMK-løsningen bør kunne avgjøre hvilken tilgang brukeren får til informasjon og funksjonalitet. Det kan også være andre tilleggsopplysninger om bruker eller kontekst som avgjør tilgang. Attributtbasert tilgangskontroll benytter kontekst i tillegg til statiske roller for beslutning om tilgang.

Sikkerhetskrav – Autorisasjon – Rettigheter:

Rettigheter i systemet bør være konfigurerbare og kunne knyttes til roller.

Beskriv systemets støtte for konfigurasjon av rettigheter.

Sikkerhetskrav – Autorisasjon – Beslutningsstyrt tilgangskontroll:

Rollen den ansatte innehar i AMK-løsningen bør gi mulighet for den ansatte selv til å beslutte tilgang til ikke-aktive pasienter/hendelser.
Beskriv systemets støtte for beslutningsstyrt tilgang.

Sikkerhetskrav - Autorisasjon - ekstern tilgangskontroll:

Beskriv støtte for ekstern tjeneste for tilgangskontroll. Beskriv også hvilke standarder som er i bruk (f.eks. XACML)

5.5.3 Sikkerhetskrav – Sporbarhet

Med sporbarhet menes å kunne bevare nødvendige detaljer knyttet til en handling. Under begrepet sporbarhet ligger også begrepet uavviselighet, som er å bekrefte at en handling eller et informasjonselement er uendret, og at det entydig kan knyttes til en bestemt digital identitet. Uavviselighet er i mange sammenhenger også omtalt som ikke-benekting. Uavviselighet benyttes også i sammenheng med autorisering og autentisering.

Behandlingsrettede helseregistre må derfor understøtte krav om sporbarhet på hvem som har fått tilgang til eller utlevert helseopplysninger.

Det følger at Pasientjournalloven § 22 jf. personopplysningsforskriften § 2-8 og § 2-14 at det skal være tilgangsstyring, logging og etterfølgende kontroll og at bruk av informasjonssystem skal dokumenteres.

Sikkerhetskrav – Logging – Generelt:

Alle relevante handlinger skal logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges:

- Alle typer innlogginger, inkl. forsøk på innlogginger
- Oppretting, endring og sletting av informasjonsobjekter
- Innsyn eller endring i helseopplysninger
- Endringer, eller forsøk på endringer, i systemkonfigurasjonen

Sikkerhetskrav – Logging – Tilgangsstyring:

Logger skal tilgangsstyres slik at de beskyttes mot manipulering/endring. Beskriv systemets støtte for tilgangsstyring av logger.

Sikkerhetskrav – Logging – Aktiviteter:

All definert aktivitet i behandlingsrettede helseregistre skal loggføres, men ikke være begrenset til følgende funksjoner/aktiviteter:

Pålogging, utlogging, åpning av journal, lesing i journal, skriving i journal, «sletting» av journal, sperring av journal, fletting, utskrift, oppretting og endring av tilganger og rettigheter, kopiering og sletting av brukerroller, eksport av datasett, samt søk som er gjort.

Sikkerhetskrav – Logging – Kommunikasjon:

All kommunikasjon mellom brukere/kontaktpersoner uavhengig av kommunikasjonsmedium bør lagres og tidspunkt for kommunikasjonen bør kunne logges.

Beskrivelse av systemets støtte for lagring og logging av kommunikasjon må etableres.

5.5.4 Sikkerhetskrav – Sperring (pasientens konfidensialitetsrettigheter)

Den enkelte pasient skal kunne motsette seg at helseopplysninger blir brukt i den videre behandling av pasienten. Dette refereres oftest til som "rett til sperring". Behandlingsrettede helseregistre må dermed ha støtte for å sperre tilgang til helseopplysninger for en valgt pasient.

Pasientjournalloven § 7 litra c angir at" Behandlingsrettede helseregistre skal være utformet og organisert slik at krav fastsatt i eller i medhold av lov kan oppfylles. Dette gjelder blant annet regler om» «c) retten til å motsette seg behandling av helseopplysninger, jf. § 17"

Pasientjournalloven § 17 angir "Pasienten eller brukeren kan motsette seg at a) helseopplysninger i et behandlingsrettet helseregister med hjemmel i §§ 8 til 10 gjøres tilgjengelig for helsepersonell etter § 19, jfr. helsepersonelloven §§ 25 og 45 og pasient- og brukerrettighets-loven § 5-3."

Manuell støtte i forkant for sperring:

a) Journalansvarlig skal forklare pasienten konsekvensen ved sperring, og at det eventuelt kan ha betydning for videre helsehjelp. Dersom pasienten er samtykkekompetent, og har fått forklart konsekvensene, skal pasientens krav om sperring etterkommes

b) Dersom ikke kravet etterkommes, skal det sendes informasjon til pasienten om retten til å klage til helsetilsynet i fylket

Behandlingsrettede helseregistre må derfor understøtte at pasienten kan detaljere hvem som ikke skal kunne ha tilgang i sin journal og hva det /hvilken informasjon det skal begrenses innsyn i.

Tabellen under angir kravene til slik sperring. Kravene gjelder både internt i et helseforetak og mellom helseforetak. Kravene skal anvendes både på eksisterende informasjon og dokumenter og framtidig informasjon og dokumenter som skal etableres.

(Journalansvarlig: person som omtalt i helsepersonelloven § 39 andre ledd. Journalansvarlig skal være oppnevnt, og har ansvar for innhold av journal, og vil normalt være den som må vurdere krav om retting, sletting og sperring.)

Sikkerhetskrav – Sperring – Sperre enkeltbrukere:

Det skal være mulig i AMK-løsningen og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at en navngitt person, eksempelvis nabo eller nær slektning eller andre entydige identifiserbare personer, ikke skal ha tilgang til hele eller utvalgte deler av journalen til pasienten.

Beskriv systemets håndtering av sperre for enkeltbrukere.

Sikkerhetskrav – Sperring – Sperre alle unntatt enkeltpersoner/roller:

Det skal være mulig i AMK-løsningen og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen, slik at utelukkende (alle) enkeltpersoner eller enkeltpersoner i en gitt rolle, eksempelvis alle leger, skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for alle andre.

Sikkerhetskrav – Sperring – Organisatorisk sperre:

Det skal være mulig i AMK-løsningen og etter forespørsel fra en pasient, å kunne begrense tilgangen til journalen til en pasient, slik at kun ansatte som tilhører en eller flere organisasjonsenheter, eksempelvis avdeling på et lokalsykehus, skal ha tilgang til journalen til pasienten, og dermed sperre tilgangen for alle andre brukerne.

5.5.5 Risiko og sårbarhetsanalyse (ROS analyse)

Enhver risikobeskrivelse avhenger av den tilgjengelige kunnskapen og de forutsetningene som gjøres, og det er derfor behov for å se utover de beregnede sannsynlighetene og forventningsverdiene når man skal vurdere risiko. (Aven, 2011)

En risikoanalyse skal gi grunnleggende informasjon om hva som kan gå galt og hva sannsynligheten er for at disse uønskede hendelsene inntreffer. Det siste kan i denne sammenhengen også beskrives som "faren". Hvordan sannsynligheten, eller "faren", beskrives er viktig for hvordan denne kan benyttes i risikovurderingen. I tillegg vurderes sårbarheten til utsatte objekt og konsekvensen dersom hendelsen inntreffer. (Kristensen, 2015)

Det er en forutsetning for fremstilling av risikovurderinger at der er et metodisk rammeverk som beskriver hva som skal vurderes, samt hvordan og hvorfor. Et metodisk rammeverk tjener både til å fremme kvalitet og transparens i vurdering av risiko og tydelighet i kommunikasjon av risiko. (SP) Det blir vurdert tjenestens evne til å innfri kravene til hver av de tre informasjonssikkerhetsområdene konfidensialitet, integritet og tilgjengelighet.(SP)

Utarbeidelse av risikovurdering med henblikk på informasjonssikkerhet kan brytes ned i seks distinkte trinn

5.5.5.1 Identifisering av risiko

identifisere potensielle uønskede hendelser og informasjonssikkerhetsbrudd

Formulere risikobeskrivelser med beskrivelse av hendelse, hvilke sikkerhetsbrudd samt hvilke uønskede konsekvenser som dette kan oppstå.

5.5.5.2 Verdivurdering

Verdiene det er ønske om å beskytte i en vurdering av personvernkonsekvenser, er de registrertes rettigheter og friheter. Det vil både si de registrertes rettigheter etter personvernforordningen. (Datatilsynet, 2019a)

5.5.5.3 Sannsynlighetsvurdering

Vurdering av sannsynlighet for at en hendelse inntreffer har som mål å finne svar på spørsmålet ”hvor ofte ...?” .. For å avdekke forventet hyppighet er det aktuelt å ta utgangspunkt i historiske data om identiske eller tilsvarende hendelser. Forutsatt at historiske data eksisterer vil sannsynlighetsvurderingen i så fall kunne baseres på statistiske metoder. I mangel av historiske data kan avdekking av forutsetninger for at en hendelse kan inntreffe være et alternativ. En slik letthetsvurdering skal gi svar på spørsmålet : ”Hva skal til for at ...?” Den må omfatte vurdering av behovet for resurser i form av utstyr og programvare, og i form av kompetanse og evner.

Sannsynlighetsvurderingen må avdekke om noen kan ha nytte av å påvirke behandlingen av personopplysninger. Nytte i denne sammenheng kan eksempelvis være betaling for utlevering av opplysninger eller etter trusler om å påvirke behandlingen ved å hindre tilgang til, eller skade/endre opplysninger.(Datatilsynet, 2019b)

5.5.5.4 Konsekvensvurdering

På samme måte som når årsaker vurderes, skal konsekvensvurderingen ta utgangspunkt i de uønskede hendelsene som er identifiserte. Konsekvensvurdering er vurdering av hvilke følger en hendelse kan få – det vil si å gi svar på spørsmålet av typen "hva medfører ..."? Konsekvens kan uttrykkes som økonomisk tap, men også forhold til virksomhetens anseelse og som eventuelt straffeansvar for virksomhet og ledelse. Ved vurdering av personvernrisiko er målet med konsekvensvurderingen å avdekke de følger en hendelse kan få for enkeltmenneskers personvern. Formålet er altså forskjellig fra arbeid med å avdekke annen risiko for virksomheten – eksempelvis forretningsmessig risiko (Datatilsynet, 2019c)

5.5.5.5 Risikoverdi

Risikoverdi (R) er resultatet av multiplikasjon av sannsynlighet (S) og konsekvens (K). (S * K) = R.

Risikoverdien blir ofte visualisert i en risikomatrise. Ved en risikovurdering ønsker man å redusere risikoverdien. Det gjør man ved å vise til sannsynlighets og konsekvens-reduserende tiltak.(QmPlus, 2010)

5.5.5.6 Visualisering av risiko - Risikomatrise

4	Moderat	Høy	Høy	Høy
3	Lav	Moderat	Høy	Høy
2	Lav	Lav	Moderat	Høy
1	Lav	Lav	Lav	Moderat
	1	2	3	4

Der opprettes en risikomatrise for hver identifisert risiko

5.5.5.7 Tiltaksoppfølging.

(Referanse: Sykehuspartner)

De risikovurderinger som blir gjort har betydning både for det styrende, det gjennomførende og det kontrollerende informasjonssikkerhetsarbeidet i en virksomhet. (Normen v. 5.3, 2020)

5.5.6 Data Protection Impact Assessment (DPIA)

En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas. En vurdering av personvernkonsekvenser er en prosess som skal beskrive behandlingen av personopplysninger, og vurdere om den er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak. (Datatilsynet, 2020)

5.6 Sikkerhetsprinsippene

Sikkerhetsprinsipper og –krav for IKT -infrastruktur og applikasjoner, inkludert behandlingsrettede helseregistre, er en sammenstilling av nødvendige prinsipper og krav for å oppnå tilfredsstillende informasjonssikkerhet i infrastruktur og porteføljen av applikasjoner. (Helse Sør Øst RHF, 2020b)

Databehandling	
3.1.1.1	Det skal være besluttet og godkjent et formål med databehandlingen
3.1.1.2	Det skal være opprettet og godkjent en tjenesteavtale og tjenestespesifikk databehandleravtale mellom Sykehuspartner og databehandlingsansvarlig
3.1.1.3	Det skal være etablert en oversikt over alle informasjonselementer som inngår i tjenesten
3.1.1.4	Alle avvik fra regionale sikkerhetskrav skal godkjennes av alle foretakene i regionen som blir berørt av avviket
3.1.1.5	Det skal dokumenteres hvorvidt en personvernkonsekvensvurdering er nødvendig, og hvor dette er nødvendig, skal personvernkonsekvensvurdering utarbeides
3.1.1.6	Det skal dokumenteres behandlingens art, mengde, omfang, lagringstid og tilgjengelighet knyttet til personopplysninger, samt sletterutiner for disse
3.1.1.7	Det skal uttømmende fremkomme fra hvilke land databehandlingen utføres fra, herunder bruk av tredjeland, og bruken skal være vurdert opp mot personvernet

3.1.1.8	Ved bruk av databehandling fra tredjeland, skal EUs standardpersonvernbestemmelser benyttes
3.1.1.9	Det skal være definert en systemeier og tjenesteansvarlig for behandlingen

Leverandørstyring	
3.1.2.1	Alt innleid personell, samt ansatte hos leverandører som utfører tidsbegrenset arbeid på vegne av virksomheten skal signere sikkerhetsinstruks
3.1.2.2	Alle leverandører og underleverandører som utfører databehandling på vegne av helseforetakene i Helse Sør-Øst, eller arbeid hvor innsyn i helse- og personopplysninger er jevnlig forventet å forekomme, skal signere databehandleravtale
3.1.2.3	Alle leverandører og underleverandører som skal behandle helseog personopplysninger skal kunne dokumentere egen informasjonssikkerhet iht. ISO 27001
3.1.2.4	Alle leverandører og underleverandører som skal behandle helseog personopplysninger skal ha opprettet personvernombud jfr GDPR artikkel 37 og personopplysningsloven § 19
3.1.2.5	All leverandørtilgang skal gjøres gjennom Virksomhetens leverandørportal
3.1.2.6	For at en leverandør og underleverandør skal kunne gis utvidede behovsbaserte rettigheter må det foreligge en godkjent risikovurdering
3.1.2.7	Leverandører kan ikke flytte eller kopiere data ut eller inn fra IKTutstyr i Virksomhetens nettverk, uten at det foreligger en godkjent risikovurdering
3.1.2.8	Når leverandører gis tilgang skal det etableres tekniske barrierer som hindrer leverandøren i å få tilgang til annet enn hva som er formålet med tilgangen.
3.1.2.9	Ved opphør av kontrakt plikter leverandør å følge instruks for terminering som beskrevet i databehandleravtale

Anskaffelser	
3.1.3.1	Leverandør og underleverandør skal bekrefte at de er kjent med kravene i personopplysningsloven/GDPR og etterlever Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten (Normen)
3.1.3.2	Anskaffelser fra tredjeland som innebærer behandling av personopplysninger må særskilt prøves, før databehandlingen kan godkjennes
3.1.3.3	Anskaffelsen er i tråd med HSØ sine sikkerhetsprinsipper, inkludert dette dokumentet og øvrige dokumenter i HSØs styringssystem for informasjonssikkerhet.
3.1.3.4	Utforming, drift, bruk og administrasjon av informasjonssystemer samstemmer med aktuelle lov(er), forskrift(er) og kontraktsfestede krav til sikring.
3.1.3.5	Anskaffelsen/systemet med underliggende komponenter skal supporteres i kontraktsperiodens levetid
3.1.3.6	Anskaffelser av tjenester og utstyr underlagt sikkerhetsloven og forskrifter, må særskilt behandles.

Identifisering	
3.2.1.1	Det skal kun benyttes personlige brukere. Fellesbrukere eller på annen måte deling av brukerkontoer skal ikke forekomme.
3.2.1.2	Alle kontoer skal entydig knyttes opp mot en digital identitet, og ivareta kravene om uavviselighet og sporbarhet ved autentisering.

Autentisering	
3.2.2.1	Autentisering skal gjøres mot sentral autentiseringsløsning (IAM) ihht. sikkerhetsprinsipper og krav for IAM.
3.2.2.2	Autentisering skal støtte identitetsutveksling ved hjelp av SAML forsterket med kryptografisk signering, eller tilsvarende.
3.2.2.3	Passord skal transporteres kryptert etter gjeldende policy i Helse Sør-Øst.

3.2.2.4	Passord skal lagres som hash etter gjeldende policy i Helse SørØst.
3.2.2.5	Systemet skal kunne håndheve vedtatt instruks for passordkompleksitet.
3.2.2.6	Passord skal aldri oppbevares skriftlig, annet enn i godkjent hvelv.
3.2.2.7	Regelmessige og planlagte oppgaver på IKT-systemene skal kjøres av servicekontoer. Servicekontoer skal standardiseres og herdes ihht herding av systemer og tjenester.
3.2.2.8	Autentiseringen må ha tilstrekkelig styrke ihht gjeldende policy i Helse Sør-Øst.
3.2.2.9	Det skal benyttes to-faktorautentisering ved: · Tilgang fra eksterne nettverk (ekstranett, Internett, leverandører). · Tilgang fra klientnettverk mot drift, forvaltning og adminløsninger.
3.2.2.10	Passordhvelv skal benyttes for alle ikke-personlige kontoer så som service- og administratorkontoer.
3.2.2.11	Informasjonssystemer skal støtte Single Sign-On (SSO).
3.2.2.12	Ansatte i andre virksomheter skal kunne automatisk autentiseres vha en internasjonal standard og protokoll for sikker utveksling av identiteter mellom ulike organisasjoner tilsvarende SAML (Security Assertion Markup Language).

3.2.2.13	Applikasjonen skal ha egen tilgangskontroll, med autentisering og autorisering mot sentral tjeneste.
3.2.2.14	Avsender skal kunne digitalt signere utvalgte dokumenter med kvalifisert sertifikat.

Autorisering	
3.2.3.1	Brukerkontoer skal ikke gis administrative rettigheter. For behovsbaserte formål skal separate personlige kontoer med utvidede rettigheter opprettes.
3.2.3.2	Tilganger skal være basert på rollestyring.
3.2.3.3	Tilganger skal være på et lavest mulig nivå iht. dokumentert behov.
3.2.3.4	Tilganger til personopplysninger skal begrenses til behov knyttet til brukerens roller og organisasjonstilhørighet.
3.2.3.5	Privilegerte tilganger tildeles kun når det foreligger gyldig grunnlag for databehandling.
3.2.3.6	Privilegerte tilganger tildeles kun i henhold til tjenestlig og dokumentert behov.

Sporbarhet	
3.2.4.1	Alle relevante handlinger skal logges. Relevante handlinger skal måles opp mot informasjonssystemet, men som et minimum skal følgende logges: · Alle typer innlogginger, inkl. forsøk på innlogginger · Oppretting, endring og sletting av informasjonsobjekter · Oppretting, endring og sletting av andre brukere · Innsyn eller endring i personopplysninger · Endringer, eller forsøk på endringer, i systemkonfigurasjonen.

3.2.4.2	Alle IKT-systemer skal logge hendelser i et standardisert format, i tråd med beste praksis for det enkelte IKT-systemet. Formålet er å sikre at logger beholder samme format og lesbarhet uavhengig av programvareversjoner og -oppdateringer, at loggene er ikke krever spesialprogramvare for å leses, og at loggene er er formatert på en måte som legger til rette for autoamtisk korrelering og logganalyse.
3.2.4.3	Alle IKT-systemene skal tilgjengeliggjøre logger for gjennomgang og eksport.
3.2.4.4	Logger som er relevante for informasjonssikkerheten skal kunne overføres til sentralt loggmottak.
3.2.4.5	Logger skal tilgangsstyres slik at de beskyttes mot manipulering/endring.
3.2.4.6	Logger skal ha tidsstempling og klokken benyttet til tidsstemplingen skal være synkronisert mot sentral NTPtjeneste.
3.2.4.7	Før databehandling iverksettes skal det være avklart at logger gjennomgås manuelt eller automatisk basert på forhåndsdefinerte kriterier med det formål å avdekke mulige sikkerhetsavvik.
3.2.4.8	Logger skal oppbevares i tråd med krav. Som minimum gjelder 24 måneders lagring for sikkerhetslogger, lagring utover dette må spesifiseres i avtale. For pasientjournallogger eller andre logger knyttet til behandlingsrettede registre, gjelder egne krav.
3.2.4.9	Tilganger skal loggføres. I tillegg skal endringer i tilganger og hvem som beslutter endringer i disse også loggføres.
3.2.4.10	Bruk av privilegerte tilganger i systemer i HSØ er uavviselig.

Sperring	
3.2.5.1	Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne begrense tilgangen til vedkommendes pasientjournal til definerte enkeltpersoner, enkeltroller og/eller enkeltgrupper.

3.2.5.2	Begrensning i tilgang til journal herunder dokumenter og dokumenttyper skal kunne avgrenses i tid.
3.2.5.3	Det skal være mulig i et behandlingsrettet helseregister og etter forespørsel fra en pasient, å kunne sperre eller begrense tilgangen for alle opplysninger knyttet til en pasientbehandling.

Infrastruktursikkerhet	
3.3.1.1	Tjenesten kan etableres på Sykehuspartners infrastruktur
3.3.1.2	Tjenesten kan etableres ihht Sykehuspartners sonemodell

Klientsikkerhet	
3.3.2.1	Klienter skal leveres av Sykehuspartner. Hvis ikke dette er mulig, gjelder etterfølgende likevel krav fra og med 3.3.2.2 til og med 3.3.2.9.
3.3.2.2	Klienter som ikke er levert gjennom Sykehuspartner skal sonemessig segmenteres fra klienter levert av Sykehuspartner.
3.3.2.3	Klienter skal ha kryptert harddisk.
3.3.2.4	Klienter skal ha automatisk installasjon av sikkerhetsoppdateringer og antivirussignaturer.
3.3.2.5	Klienter skal ha automatisk låsing av skjerm m/ passord.
3.3.2.6	Brukere skal ikke ha administrasjonsprivilegier på egen klient. Brukere skal ikke kunne deaktivere lokale sikkerhetskontroller.
3.3.2.7	Klienter skal kun ha godkjent og risikovurdert programvare installert.
3.3.2.8	Klienter skal alltid benytte VPN når man er utenfor Virksomhetens infrastruktur, for eksempel private eller offentlige nettverk.
3.3.2.9	Klienter skal autentiseres gjennom klientsertifikater for å kunne koble seg på Virksomhetens nettverk.

Klientsikkerhet	
3.3.2.1	Klienter skal leveres av Sykehuspartner. Hvis ikke dette er mulig, gjelder etterfølgende likevel krav fra og med 3.3.2.2 til og med 3.3.2.9.
3.3.2.2	Klienter som ikke er levert gjennom Sykehuspartner skal sonemessig segmenteres fra klienter levert av Sykehuspartner.
3.3.2.3	Klienter skal ha kryptert harddisk.
3.3.2.4	Klienter skal ha automatisk installasjon av sikkerhetsoppdateringer og antivirussignaturer.
3.3.2.5	Klienter skal ha automatisk låsing av skjerm m/ passord.
3.3.2.6	Brukere skal ikke ha administrasjonsprivilegier på egen klient. Brukere skal ikke kunne deaktivere lokale sikkerhetskontroller.
3.3.2.7	Klienter skal kun ha godkjent og risikovurdert programvare installert.
3.3.2.8	Klienter skal alltid benytte VPN når man er utenfor Virksomhetens infrastruktur, for eksempel private eller offentlige nettverk.
3.3.2.9	Klienter skal autentiseres gjennom klientsertifikater for å kunne koble seg på Virksomhetens nettverk.

Applikasjonssikkerhet	
3.3.4.1	Applikasjonen skal ha definert applikasjonsforvaltning i tråd med regionale føringer, hvor roller og ansvar mht. forvaltning av applikasjonen er avklart.
3.3.4.2	Det skal legges til rette for effektiv og hurtig installasjon av sikkerhetsoppdateringer.
3.3.4.3	Applikasjonen skal benytte en trelagsarkitektur for å begrense eksponering av bakenforliggende database.

3.3.4.4	Applikasjonen skal følge etablert endrings- og oppdateringsregime for operativsystemet.
3.3.4.5	Applikasjonen skal støtte utskrift via Sikker Print.
3.3.4.6	Applikasjonen skal aldri lagre eller overføre passord i klartekst, jf. 3.2.2.4
3.3.4.7	Applikasjonen skal kryptere data som går i transitt i henhold til kryptoinstruksen.
3.3.4.8	Bruk av ressurser skal inn i regime for overvåking og justering, og det bør foretas beregninger over framtidige kapasitetsbehov for å sikre at systemet oppnår påkrevd ytelse.

Angrepsflate	
3.3.6.1	Alle tjenester som eksponeres eksternt skal penetrasjonstestes, uavhengig av sikkerhetsnivå.
3.3.6.2	Alle tjenester som eksponeres eksternt skal plasseres i virksomhetens DMZ.
3.3.6.3	Kommunikasjon skal alltid initieres av tjenesten i det høyeste sikkerhetsnivået.

4.6 Terminering	
3.3.7.1	Avhending av utstyr skal skje i henhold til instruks
3.3.7.2	Ved terminering av tjenesten skal: -brannmursåpninger lukkes -brukerkontoer deaktiveres -system og administratorkontoer fjernes -leverandørtilgang fjernes -Tjenesten settes inaktiv i tjenestekatalogen

Drift	
3.4.1.1	Administrasjon av virksomhetens servere og tjenester skal gjøres gjennom en egen administrasjonsinfrastruktur med tofaktorautentisering.
3.4.1.2	Administrasjonsinfrastruktur skal ikke ha tilgang til Internett eller andre eksterne nettverk.
3.4.1.3	Enhver AD gruppe skal ha en eier som har forvaltningsansvaret.
3.4.1.4	Forvaltning av privilegerte tilganger er en del av helhetlig sikkerhetsarkitektur.
3.4.1.5	All bruk av privilegerte tilganger skjer igjennom en helhetlig driftsløsning for HSØ.
3.4.1.6	Bruk av privilegerte tilganger er mulig i HSØ til enhver tid uavhengig av hendelser i det ordinære produksjonsmiljøet.

Dokumentasjon	
3.4.2.1	Det skal være etablert rutiner for tjenesten, der rutinene for henholdvis bruk og forvaltning er innbyrdes harmonisert.
3.4.2.2	Endringer i en tjeneste skal dokumenteres i systemdokumentasjonen.
3.4.2.3	Systemdokumentasjon skal være lagret og holdes oppdatert på godkjent område for oppbevaring i minst fem år etter siste endring.
3.4.2.4	Det skal være opprettet planer for business continuity og disaster recovery for systemer som er definert som krikalitet 1.
3.4.2.5	Det skal gjennomføres opplæring i policy og prosedyrer som er relevant for alle roller i systemet. Dette innbefatter samtlige brukere og administratorer av systemet, samt eventuelle kontraktører og tredjepartsbrukere.

(Helse Sør Øst RHF, 2020b)

5.7 Forsknings-etikk

I henhold til helseforskningsloven skal etiske, medisinske, helsefaglige, vitenskapelige og personvern-messige forhold ivaretas (Helseforskningsloven, 2009).

Regionale komiteen for medisinsk og helsefaglig forskningsetikk (REK)

For medisinsk og helsefaglig forskning på mennesker, humant biologisk materiale eller helseopplysninger er det krav om forhåndsgodkjenning av prosjektet. I henhold til Helseforskningsloven skal disse forhåndsgodkjenningene som hovedregel sendes til den regionale komiteen for medisinsk og helsefaglig forskningsetikk (REK).

("Godkjenning av medisinsk og helsefaglig forskning," 2017).

Dette forskningsprosjekt, med referanse 108609, er godkjent av REK med begrunnelse at forskningsprosjektet er av vesentlig interesse for samfunnet.

Det er også godkjent av Norsk senter for forskningsdata med referansekode 889368 , med begrunnelse i at det ikke skal behandles direkte eller indirekte opplysninger som kan identifisere enkeltpersoner.

6 Risikovurdering

I dette kapittelet vil jeg utføre en risiko- og sårbarhetsanalyse basert på innsikt jeg har fått fra teori-kapitel 4, som omhandler bla. helselovgivning og informasjonssikkerhet. Jeg vil også benytte meg av behovskartleggingen utført av Making Waves, samt tjenestebeskrivelse av Videotjenesten til hjelp-113-appen. Et viktig hjelpemiddel for analysen er sikkerhetsprinsippene, et sett strukturerte og konkrete krav som stilles til bla. databehandling av helseopplysninger.

Resultatene som er kommet frem i en spørreundersøkelse blant AMK-operatører har gitt meg verdifull innsikt i hvordan AMK-operatørene utfører sitt arbeid og hva de selv vektlegger når de skal vurdere informasjonssikkerheten i tjenesten. Spørreundersøkelsen er gjennomført blant AMK-operatører som har mellom 1- 5 års erfaring fra arbeid med å svare nødsamtaler. Alle respondentene oppgir at de har testet ut videosamtale-tjenesten i inntil 3 måneder og samtlige har benyttet denne i mer enn 20 nødsamtaler.

Alle respondentene oppgir at de anser video som et veldig godt verktøy for å kunne hjelpe pasienten på best mulig måte. Den beskrives som «Et helt uvurderlig verktøy. En ny æra innen akuttmedisin». Det har og stor verdi for å avklare hvordan HLR utføres, samt vurdering av diverse skader/kutt o.l.

Den største fordelen beskrives som «å ha «øyer» på stedet». Det er også med på å avgjøre hvor mange ressurser man skal sende og om det er behov for bistand av lege.

En annen AMK-operatør sier at videotjenesten er med på å underbygge de opplysningene innringer formidler og avklarer i tvilstilfeller. Man kan iverksette livreddende strakstiltak og verifisere at instruksen man gir faktisk blir fulgt. Vi har reddet mange liv allerede på den tiden vi har hatt tilgang til video som verktøy.

I spørreundersøkelsen fremkommer det at ingen av AMK-operatørene har betenkeligheter i forhold til hvordan informasjonssikkerheten er ivaretatt i tjenesten. De vurderer informasjonssikkerheten som godt i varetatt i og med at der er end-til -ende kryptering.

Tjenesten blir vurdert «som et meget sikkert system som er kryptert og som ikke lagres. En responder understreker at det er en stor fordel og nærmest en forutsetning at det ikke lages.

6.1 Risiko og sårbarhetsanalyse

En risikovurdering er et øyeblikksbilde av tjenesten som blir vurdert og er en vurdering ut fra informasjon som er tilgjengelig på det tidspunkt vurdering blir gitt.

For å sikre god håndtering av identifiserte risikoer, er det anbefalt å ha et aktivt forhold til de fire T-ene for risikohåndtering.

Tolerate (Akseptere)	Det er ikke mulig å fjerne all risiko. Noe risiko kan derfor aksepteres, men det er viktig at risikoen er identifisert, forstått og akseptert av berørte parter.
Treat (Behandle)	Iverksette tiltak for å redusere risikoen, enten ved å redusere sannsynligheten for at den inntreffer eller ved å redusere konsekvensene det vil medføre at risikoen inntreffer.
Transfer (Overføre)	Noe av den finansielle risikoen kan muligens overføres til forsikringsselskap, gjennom kontraktsmessige forhold med en tredje part, eller ved at mulige berørte parter aksepterer den risikoen de kan bli påført. Merk at overføring av risiko knyttet til sensitiv informasjon i liten grad vil være et alternativ.
Terminate (Fjerne)	Dersom en identifisert risiko anses som uakseptabel og denne ikke kan kontrolleres, behandles eller overføres, kan løsningen være å eliminere alle aktiviteter/elementer som påfører denne risikoen.

Risikovurdering Helse Sør-Øst se vedlegg 5

6.1.1 Identifisering av risiko

En risikovurdering av informasjonssikkerheten ved en videosamtale-tjenesten har mange ulike perspektiv. I denne oppgaven er det fokusert på følgende perspektiv.

Innringers perspektiv

Pasientens perspektiv

AMK-operatørs perspektiv

Driftsperspektiv / Teknisk perspektiv

Forvaltnings perspektiv

For å vurdere mulige konsekvenser av den identifiserte sårbarheten har jeg benyttet konsekvensskalaen som er beskrevet i kapittel 5.4.8. Og tilsvarende for sannsynlighetsvurderingen har jeg støttet meg på sannsynlighetsskalaen i kapittel 5.4.7.

6.1.1.1 Innringers perspektiv

Både behovskartleggingen til Making Waves og spørreundersøkelsen bland AMK-operatørene har gitt meg innsikt til å identifisere sårbarheter knyttet til innringers rolle.

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
1	Både innringer og AMK-operatør blir mer konsentrert om det tekniske ved oppkobling av videosamtalen, at innringer og AMK-operatør blir mindre fokusert på pasienten.	Det er fare for at innringer og AMK-operatør går glipp av viktig endringer i pasientens tilstand, da de er mer fokusert på teknologien enn pasientens tilstand	**3**	**2**	**6**	Ved nye prosedyrer og nye tjenester kan det ta litt tid før AMK-operatør og innringer er fortrolig med den nye tjenesten. Sannsynlighet settes til middels	**1**
2	Det er fare for at publikum på et skadested kvier seg for å ta kontakt med AMK, for de ønsker ikke å komme i en situasjon hvor de blir spurt om videooverføring.	Det kan ta kritisk lang tid før AMK-sentralen blir kontaktet og verdifulle tid kan gå tapt før pasient får den hjelp han eller hun trenger	**2**	**2**	**4**	Ved nye prosedyrer og nye tjenester kan det ta litt tid før innringer og publikum blir fortrolig med den nye tjenesten. Sannsynlighet settes til middels	**1**

6.1.1.3 Pasientens perspektiv

Sårbarheten fra pasientens perspektiv er i hovedsak inspirert fra gjeldende lovverk knyttet til personvern, så som pasient og brukerrettighetsloven

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
3	Det kan oppstå uenighet blant de involverte i en hendelse hvorvidt de ønsker at videosamtale skal benyttes.	Det er fare for at AMK-operatøren ikke får benytte videotjenesten, og dermed potensielt ikke gi best mulig helsehjelp	2	2	4	Den enkelte involverte i en hendelse kan ha ønske om å ikke bli identifisert i en sårbar situasjon.	**2**

6.1.1.5 AMK-operatørens perspektiv

Sårbarhetene fra AMK-operatørens perspektiv er inspirert av kravene i sikkerhetsinstruksene knyttet til autorisering, sporbarhet og dokumentasjon. Spørreundersøkelsen har også gitt meg verdifull innsikt for å vurdere sårbarheter fra en operatør sitt perspektiv.

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
4	Arbeidsstasjonen til AMK - operatøren er synlig for uvedkommende via f.eks vindu	Uvedkommende kan få tilgang til sensitive personopplysninger	2	1	2	Da det tidligere kun er benyttet telefon i kontakt mellom AMK og innringer, kan man ved innføring av videosamtale komme i skade for å ikke tenke over at operatør sin skjerm nå viser sensitive opplysninger.	3
5	Det er uklare prosedyrer for når videooverføring skal tilbys.	AMK-operatøren blir usikker i sin vurdering av i hvilke situasjoner videosamtale skal tilbys. Dette kan føre til at det blir praktisert ulike både hos den enkelte AMK-operatør, men også hos de forskjellige AMK-sentralene	2	2	4	Ved innføring av nye tjenester medfører det stor sannsynlighet for at operatørene er usikker på i hvilke situasjoner det skal benyttes/ tilbys videotjenesten.	4

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
6	AMK-operatøren får innsyn i situasjoner som kan bli svært belastende psykisk.	Det kan bli en stor mental belastning for AMK-operatøren å se mennesker i en svært kritisk situasjon, med svært begrenset mulighet for å avhjelpe situasjonen pasienten befinner seg i. Dersom det er barn som er i den kritiske situasjonen vil trolig inntrykkene vil den mentale belastningen trolig forsterke seg.	3	3	9	Dersom AMK-operatøren ikke er mentalt forberedt på og har liten erfaring fra krevende hendelser, er sannsynlighet stor for at operatøren kan oppleve hendelse som mentalt belastende.	5
7	AMK-operatøren starter videosamtale uten at samtykke er gitt	Dersom AMK-operatøren starter Videosamtalen uten at samtykke er gitt, vil innringer få en SMS med lenke til å starte kameraet. I en stresset situasjon kan innringer komme til å akseptere denne uten å tenke over konsekvensene,	1	1	1	For at både innringer og AMK-operatør skal være trygg på den nye teknologien med videosamtale mellom AMK og skadested, er det svært viktig at AMK-operatørene får mye og variert trening med å benytte denne. Det anbefales også at før denne tjeneste tilbys befolkningen nasjonalt, at det gjennomføres	-

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
						opplysningsarbeid for å forberede innringere om at dette er en teknologi som kan bli tatt i bruk.	
8	Det er fare for at AMK-operatøren blir så avhengig av å få tilgang til videosamtale at når dette ikke er tilgjengelig, blir AMK operatøren usikker i sine vurderinger.	Dersom innføring av videosamtale mellom AMK og innringer blir en uunnværlig støtte for AMK-operatøren i hans eller hennes vurderinger, er det det fare for at ved et evt. bortfall av tjenesten vil AMK-operatøren føle usikkerhet i sine faglige vurderinger.	2	1	2		-

6.1.1.7 Driftsperspektiv / teknisk perspektiv

For å komme frem til sårbarhetene i et drifts perspektiv har jeg hovedsakelig hentet inspirasjon fra bla. kravene i sikkerhetsinstruksene som omhandler drift, angreps-flater og applikasjonssikkerhet.

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
9	Uvedkommende kan avlytte datastrøm mellom AMK-operatør og innringer og på den måten få tilgang til sensitive personopplysninger.	Uvedkommende kan få tilgang til sensitive personopplysninger	**3**	**2**	**6**	En trusselaktør må ha evne ,motivasjon og kompetanse til å prøve å få urettmessig tilgang til datastrømmen. Sannsynlighet settes til lav.	**6**
10	Innringer har mulighet til å ta opp film av det som blir streamet.	Innringer kan distribuere opptaket som er gjort av en hendelse og på den måte tilgjengeliggjøre sensitive personopplysninger til uvedkommende	**4**	**2**	**8**	Det er beskrevet at det ikke skal være mulig å ta opp datastrømmen som kommer fra innringers kamera, så sannsynligheten vurderes som liten	**7**
11	Ved å benytte videotjenesten til telefonen bruker telefonen betydelig mer batteri enn ved en vanlig telefonsamtale og det er derfor fare for at samtalen blir brutt pga. mangel på strøm.	Innringer, som er i en akutt situasjon mister telefonkontakt med AMK og blir på den måten fratatt hjelp fra disse.	**3**	**3**	**9**	Sannsynligheten regnes for relativt stor, da telefonen benyttes generelt mye i hverdagen og derfor har varierende batteristatus, samt at man ikke er forberedt på	**8**

						når en akutt hendelse inntreffer.	
12	Ved store hendelser, med mange involverte, er det fare for at dersom mange ringer inn samtidig og benytter videosamtale, kan kommunikasjonsnettet kollapse pga manglende kapasitet.	Det blir vanskelig å varsle og gjennomføre livsviktig kommunikasjon mellom nødetatene og publikum, samt koordinering av redningsoppdraget	**3**	**3**	**9**	Sannsynligheten for dette regnes for moderat, infrastrukturen mange steder i Norge ikke er dimensjonert for mye trafikk.	**9**
13	Denne tjenesten blir eksponert utenfor databehandlers infrastruktur, da AMK-operatør sendes en lenke til innringer som gir mulighet for oppkobling av videostrøm mellom AMK-operatør sitt IKT-utstyr og innringer.	Denne sårbarheten kan gi en trussel-aktør tilgang til databehandlers infrastruktur. Sensitiv personopplysninger kan bli eksponert for uautoriserte.	**3**	**3**	**9**	Der foreligger trolig aktører med moderat evne og moderat vilje til å forsøke å få uautorisert tilgang til databehandlers infrastruktur.	**10**

6.1.1.8 Forvaltnings perspektiv

For å komme frem til sårbarhetene i ett forvaltnings-perspektiv har jeg hentet inspirasjon fra bla. kravene i sikkerhetsinstruksene som omhandler databehandling og leverandørstyring.

#	Mulig trusselscenario og hendelse	Mulig virkning (Konsekvens)	K (1-4)	S (1-4)	(K x S) (1-16)	Begrunnelse (Sannsynlighet)	Tiltak nr.
14	Der stilles krav til leverandør av tjenesten at alle leverandører og underleverandører som skal behandle helse og personopplysninger skal kunne dokumentere egen informasjonssikkerhet iht. ISO 27001	Det er fare for at sensitive personopplysninger kan bli tilgjengelig for uvedkommende, dersom ikke leverandør og underleverandør har et bevist forhold til informasjonssikkerhet for tjenestene de leverer.	4	3	12	Sannsynligheten regnes som liten da de fleste litt større leverandører har erfaring med behandling av personopplysninger og har et bevist forhold til disse i sine rutiner, prosedyrer og planer.	11

6.1.2 Anbefalt risikoreduserende tiltak

Tiltak nr.	ID	Risiko (1-16)	Mulig sårbarhet	Beskrivelse av tiltak	Ansvarlig
1	1	6	Både innringer og AMK-operatør blir mer konsentrert om det tekniske ved oppkobling av videosamtalen, at innringer og AMK-operatør blir mindre fokusert på pasienten.	1.1 For at både innringer og AMK-operatør skal være trygg på den nye teknologien med videosamtale mellom AMK og skadested, er det svært viktig at AMK-operatørene får mye og variert trening med å benytte denne. 1.2 Det anbefales også at før denne tjeneste tilbys befolkningen nasjonalt, at det gjennomføres opplysningsarbeid for å forberede innringere om at dette er en teknologi som kan bli tatt i bruk.	1.1 Ledelsen ved de ulike AMK-sentralene. 1.2 Norske helsemyndigheter
	2	4	Det er fare for at publikum til et skadested kvier seg for å ta kontakt med AMK, for de ønsker ikke å komme i en situasjon hvor de blir spurt om videooverføring.	Tiltak 1.2 vil ha positiv effekt for denne sårbarheten	Norske helsemyndigheter
2	3	4	Det kan oppstå uenighet blant de involverte i en hendelse hvorvidt de ønsker at videosamtale skal benyttes.	Det anbefales at før denne tjeneste tilbys befolkningen nasjonalt, gjennomføres det grundig opplysningsarbeid for å forberede innringere om at dette er en teknologi som kan bli tatt i bruk.	Norske helsemyndigheter Involverte i en hendelse.

Tiltak nr.	ID	Risiko (1-16)	Mulig sårbarhet	Beskrivelse av tiltak	Ansvarlig
				I følge veitrafikkloven $ 12 har involverte , publikum og andre plikt på seg til å hjelpe til ved en hendelse. De som er innblandet i trafikkuhell, har gjensidig plikt til å oppgi navn og adresse De som er innblandet i uhellet, skal søke å hindre fjerning av spor og endring av andre forhold av betydning. Det er ifølge straffeloven § 387 straffbart å ikke yte hjelp eller å hindre skadelidende hjelpe .	
3	4	2	Arbeidsstasjonen til AMK -operatøren er synlig for uvedkommende via f.eks vindu	Det er veldig viktig at når det innføres videotjeneste i AMK-sentralene, at man er bevist at nå er det ikke bare lyd , men også bilder som blir eksponert i lokalet. Man må derfor hindre innsyn fra uvedkommende og publikum inn AMK-sentralen	Respektive Helseforetak som er ansvarlig for AMK-sentralen
4	5	4	Det er uklare prosedyrer for når videooverføring skal tilbys.	Før Videotjeneste tas i bruk er det viktig at det utarbeides og gjøres kjent robuste prosedyrer for bruk av tjenesten.	Respektive Helseforetak som er ansvarlig for AMK-sentralen
5	6	9	AMK-operatøren får innsyn i situasjoner som kan bli svært belastende psykisk.	Det er viktig at AMK-operatøren er seg bevist og danner seg et inntrykk av og forbereder	Respektive Helseforetak som er

Tiltak nr.	ID	Risiko (1-16)	Mulig sårbarhet	Beskrivelse av tiltak	Ansvarlig
				seg på hva de kan komme til å se når de tilbyr videotjeneste ved en hendelse. Gode debrifingsrutiner og kollegaordninger kan redusere belastningen for den enkelte operatør.	ansvarlig for AMK-sentralen
6	7	1	AMK-operatøren startervideosamtale uten at samtykke er gitt	For at både innringer og AMK-operatør skal være trygg på den nye teknologien med videosamtale mellom AMK og skadested, er det svært viktig at AMK-operatørene får mye og variert trening med å benytte denne. Det anbefales også at før denne tjeneste tilbys befolkningen nasjonalt, at det gjennomføres opplysningsarbeid for å forberede innringere om at dette er en teknologi som kan bli tatt i bruk.	Respektive Helseforetak som er ansvarlig for AMK-sentralen
7	8	2	Det er fare for at AMK-operatøren blir så avhengig av å få tilgang til videosamtale at når dette ikke er tilgjengelig, blir AMK operatøren usikker i sine vurderinger.	For at AMK-operatøren skal bli så trygg i sine vurderinger som mulig er det viktig å utføre gjentatte øvelser og simuleringer av ulike situasjoner, både med og uten videotjenesten tilgjengelig.	Respektive Helseforetak som er ansvarlig for AMK-sentralen
8	9	6	Det er fare for at uvedkommende kan få tilgang til data som går i datastrømmen fra innringers kamera og inn til AMK-sentralen.	Tjenesten benytter ende-til-endekryptering.	Tjenesteansvarlig leverandør
9	10	8	Innringer kan distribuere opptaket som er gjort av en hendelse og på den måte	Det er svært viktig at leverandør har kontroll på teknologi som er benyttet i bl.a ulike	Leverandør

Tiltak nr.	ID	Risiko (1-16)	Mulig sårbarhet	Beskrivelse av tiltak	Ansvarlig
			tilgjengeliggjøre sensitive personopplysninger til uvedkommende	telefonmodeller og nettlesere for å forhindre at opptak av datastrømmen ikke er mulig	
10	11	9	Ved å benytte videotjenesten til telefonen bruker telefonen betydelig mer batteri enn ved en vanlig telefonsamtale og det er derfor fare for at samtalen med AMK blir brutt pga. mangel på strøm.	Det er svært viktig at videotjenesten er så lite batterikrevende som mulig. Dersom tjenesten blir almen kjent og benyttet er det også en mulighet for at publikum blir mer bevist batterikapasiteten på egen mobiltelefon, samt å ha ekstra batteri tilgjengelig.	Leverandør Forbrukere
11	12	9	Ved store hendelser, med mange involverte, er det fare for at dersom mange ringer inn samtidig og benytter videosamtale, kan kommunikasjonsnettet kollapse pga manglende kapasitet.	Ved en nasjonal lansering av tjenesten er det viktig at det blir vektlagt at publikum ved en større hendelse begrenser datakommunikasjon til kun å gjelde kommunikasjon som går til og fra nødetatene. Teleoperatørene oppfordres til å bygge ut kapasiteten spesielt i distriktet. Myndighetene pålegger teleoperatørene en minste kapasitet på telenettet, for bedre å kunne takle stort press på infrastrukturen	Myndigheter Teleoperatørene Publikum
12	13	9	Denne tjenesten blir eksponert utenfor databehandlers infrastruktur, da AMK-operatør sendes en lenke til innringer som gir mulighet for oppkobling av	Der må gjennomføres en penetrasjonstest, for å avdekke om det er mulig for trussel-aktør å urettmessig å få tilgang til informasjon i lenken AMK-operatør tilbyr innringer, eller på	Databehandler

Tiltak nr.	ID	Risiko (1-16)	Mulig sårbarhet	Beskrivelse av tiltak	Ansvarlig
			videostrøm mellom AMK-operatør sitt IKT-utstyr og innringer.	annen måte kan få tilgang til denne datastrømmen.	
13	14	9	Der stilles krav til leverandør av tjenesten at alle leverandører og underleverandører som skal behandle helse og personopplysninger skal kunne dokumentere egen informasjonssikkerhet iht. ISO 27001	Ved kontraktinngåelse for levering av tjenesten må det stilles krav til leverandør om dokumentasjon for sertifisering og andre reguleringer som omhandler informasjonssikkerhet	Leverandør

6.1.3 Vurdering av tiltak

Tiltak nr.	ID	Rest-risiko (1-16)	Beskrivelse av tiltak	Vurdering av konsekvens-reduserende effekt	Vurdering av sannsynlighets-reduserende effekt
1	**1** 2	**3**	1.1 For at både innringer og AMK-operatør skal være trygg på den nye teknologien med videosamtale mellom AMK og skadested, er det svært viktig at AMK-operatørene får mye og variert trening med å benytte denne.	Tiltaket har ingen konsekvensreduserende effekt	Tiltakene vurderes som egnet for å redusere sårbarhet. 1.1 God og variert opplæring, trening og realistiske øvelser vil gi AMK-operatøren trygghet i forhold til den nye tjenesten som han har tilgjengelig. 1.2 Ved målrettet opplysningsarbeid og kampanjer nasjonalt vil tjenesten bli allmenn kjent. Den kan også involveres i det opplæringsmateriellet og retningslinjer som utarbeides for grunnleggende førstehjelpskurs for publikum.
2	**3**	**2**	Det anbefales at før denne tjeneste tilbys befolkningen nasjonalt, gjennomføres det grundig opplysningsarbeid for å	Tiltaket har ingen konsekvensreduserende effekt	**Se tiltak 1**

			forberede innringere om at dette er en teknologi som kan bli tatt i bruk.		
3	**4**	**2**	Det er veldig viktig at når det innføres videotjeneste i AMK-sentralene, at man er bevist at nå er det ikke bare lyd, men også bilder som blir eksponert i lokalet. Man må derfor hindre innsyn fra uvedkommende og publikum inn AMK-sentralen	Tiltaket har ingen konsekvensreduserende effekt	De fleste sentraler har trolig en bevist utforming for å kunne skjerme sentralen for innsyn, men det er viktig at man er bevist på at man har fått en ny datakilde, som kan eksponere sensitive personopplysninger
4	**5**	**2**	Før Videotjeneste tas i bruk er det viktig at det utarbeides og gjøres kjent robuste prosedyrer for bruk av tjenesten.	Tiltaket har ingen konsekvensreduserende effekt	Ved utarbeidelse av robuste rutiner vil AMK-operatøren bli trygg i sin vurdering av når tjenesten skal tilbys. Tiltaket anses som sannsynlighets-reduserende
5	**6**	**3**	Det er viktig at AMK-operatøren er seg bevist og danner seg et inntrykk av og forbereder seg på hva de kan komme til å se når de tilbyr videotjeneste ved en hendelse. Gode debrifingsrutiner og kollegaordninger kan redusere belastningen for den enkelte operatør.	Tiltaket har ingen konsekvensreduserende effekt	AMK-operatører som har fått god opplæring og trening samt deltatt på realistiske øvelser vil ha en større forutsetning til å håndtere den psykiske belastningen som krevende synsinntrykk kan medføre. Gode rutiner for debrief og kollegastøtte vil også hjelpe på for å få bearbeidet evt. psykiske reaksjoner. Tiltaket vurderes til å ha stor sannsynlighets-reduserende effekt
6	**9**	**2**	Det er fare for at uvedkommende kan få tilgang til	Tiltaket har ingen konsekvensreduserende effekt	Ved at det benyttes kjent teknologi, samt anerkjente PKI-

			data som går i datastrømmen fra innringers kamera og inn til AMK-sentralen.		leverandører er sannsynligheten for at uvedkommende skal lytte av datastrømmen redusert
7	**10**	**8**	Det er svært viktig at leverandør har kontroll på teknologi som er benyttet i bl.a. ulike telefonmodeller og nettlesere for å forhindre at opptak av datastrømmen ikke er mulig	Tiltaket har ingen konsekvensreduserende effekt	For å holde seg innenfor lovverket, samt å skape tillit i befolkningen, er det helt avgjørende at det ikke er mulig å lagre videostrømmen. Tiltaket vil ha stor sannsynlighetsreduserende effekt.
8	**11**	**9**	Det er svært viktig at videotjenesten er så lite batterikrevende som mulig. Dersom tjenesten blir almen kjent og benyttet er det også en mulighet for at publikum blir mer bevist batterikapasiteten på egen mobiltelefon, samt å ha ekstra batteri tilgjengelig.	Tiltaket har ingen konsekvensreduserende effekt	Vi er i dag blitt veldig avhengig av mobiltelefonen. Den benyttes i svært mange sammenhenger. De fleste brukerne har derfor ett bevist forhold til batterikapasitet. Ved at publikum blir godt informert om at denne tjenesten eksistere og har ekstra batterikapasitet i reserve, samt at mobiltelefonene får stadig bedre batterikapasitet reduseres sannsynligheten noe.

9	**12**	**9**	Ved en nasjonal lansering av tjenesten er det viktig at det blir vektlagt at publikum ved en større hendelse begrenser datakommunikasjon til kun å gjelde kommunikasjon som går til og fra nødetatene. Teleoperatørene oppfordres til å bygge ut kapasiteten spesielt i distriktet. Myndighetene pålegger teleoperatørene en minste kapasitet på telenettet , for bedre å kunne takle stort press på infrastrukturen	Tiltaket har ingen konsekvensreduserende effekt	Ved å bevisstgjøre publikums telefonbruk, ved større hendelser, kan dette øke forståelsen for at kapasiteten i nettet blir reservert for nødetatene. Ved å tydeliggjøre nytten av bla. denne typen tjenester for myndigheter, kan det være med på å stille krav til utbyggerne av datanettet. Tiltakene vil trolig har effekt på sannsynligheten både på kort og på lengre sikt
10	**13**	**9**	Der må gjennomføres en penetrasjonstest, for å avdekke om det er mulig for en trussel-aktør å urettmessig få tilgang til informasjon i lenken AMK-operatør tilbyr innringer, eller på annen måte kan få tilgang til denne datastrømmen .	Tiltaket har ingen konsekvensreduserende effekt	Ved å gjennomføre en penetrasjonstest vil en avdekke hvorvidt dette er en sårbarhet som en trussel-aktør kan benytte seg av, og dermed sette inn tiltak for å redusere sannsynligheten.
11	**14**	**12**	Ved kontraktinngåelse for levering av tjenesten må det stilles krav til leverandør om dokumentasjon for sertifisering og andre reguleringer som omhandler informasjonssikkerhet	Tiltaket har ingen konsekvensreduserende effekt	Ved at det stilles krav til leverandør om dokumentasjon for deres informasjonssikkerhetsarbeid økes deres bevissthet rundt dette og dermed reduseres sannsynlighet.

6.2 Gjeldende lovverk til hinder for praktiske gjennomførbare løsninger

Et av spørsmålene i spørre-undersøkelsen var dersom AMK-operatøren får innsyn i en opplagt kriminell handling. Skal dette videreformidles til politiet?

Ifølge rundskriv 15-09-2015 Helsepersonellets taushetsplikt – rett og plikt til å utlevere pasientopplysninger til politiet, har helsepersonell generelt ikke plikt til å varsle politiet om dette. Taushetsplikten etter helsepersonelloven er begrunnet i hensynet til pasientens personvern og integritet, og i behovet for at befolkningen har tillit til helsepersonell og til helsetjenesten. Tilliten til at helsepersonell ikke utleverer helseopplysninger til politi eller andre kan være avgjørende for at den enkelte oppsøker helsetjenesten ved behov, melder fra om alvorlig sykdom- eller skade, og ikke tilbakeholder viktige helseopplysninger. (Politiet, 2015)

6.3 Avveining av hensynene

I behovsanalysen til Making Waves ble det konkludert med at tjenesten kan levers slik den er beskrevet, innenfor rammene av gjeldende lovverk. Dette er under forutsetning av videostrømmen ikke kan lagres, hverken på innringers enhet eller på AMK-operatøren sitt Ikt-utstyr. Dette for å best mulig ivareta personvernet til de involverte, som er i en sårbar situasjon og i mange tilfeller ikke samtykkekompetente i den aktuelle situasjonen. Det samme kommer frem i spørreundersøkelsen blant ansatte på AMK-sentralene.

Når en sammenligner svarene fra spørreundersøkelsen med behovsanalysen ser vi at de stemmer godt overens med hverandre. Det som antas som et godt hjelpemiddel for å hjelpe pasienter ved en akutt hendelse viser seg ved utprøving, å bli helt uvurderlig.

7 Konklusjon

I denne oppgaven har jeg fordypet meg i den prehospitale kjeden, slik den er bygd opp i Norge. Kjeden er helsevesenets forlengede arm ut til publikum og kjeden hjelper pasienter i en akutt situasjon og består bl.a. av AMK-sentralene, ambulansetjeneste og akutt mottak på sykehusene. I denne oppgaven har jeg fokusert spesielt på AMK-sentralene og deres funksjon. Hovedansvaret til AMK-sentralene er å redde liv og begrense skade ved medisinske nødsituasjoner. For å gi rett helsehjelp, samt å disponere tilgjengelige ressursene på best mulig måte, er det helt avgjørende at AMK-operatøren har god forståelse for hendelsen som innringer befinner seg i. De hjelpemidler dagens AMK-operatører har til rådighet i sitt arbeid er, Norsk medisinsk indeks for vurdering av alvorlighetsgrad, dataprogrammer for registrering av hendelser, kart-tjeneste for lokalisering av hendelse samt Nødnett for kommunikasjon med bla. de andre nødetatene.

Den teknologiske utviklingen har gitt helsevesenet nye hjelpemidler for å gi best mulig helsehjelp, samt best mulig utnyttelse av ressursene. Uttrykk som telemedisin, videokonsultasjon og velferdsteknologi er blitt dagligtale i helsevesenet.

Denne teknologiske utviklingen har AMK Oslo i samarbeid med Stiftelsen Norsk luftambulanse NLA nytte gjort seg. De har utviklet en tjeneste som muliggjør videosamtale mellom AMK-operatør og innringer.

Denne tjenesten imøtekommer det ønsket som ble avdekket i en behovskartlegging blant AMK-operatører. For å gi best mulig helsehjelp uttrykket deltakerne et felles ønske om å kunne se den situasjonen innringer og pasient befinner seg i. «Å ha øyner der ute»

Som grunnlag for å få en forståelse av AMK-operatørenes ønsker og behov for funksjonaliteten i en slik tjeneste, har jeg støttet meg på behovskartleggingen utført av Making Waves for Vestre Viken prehospitale klinikk. Denne har gikk meg verdifull innsikt i arbeidshverdagen til en AMK-operatør, med arbeidsrutiner og hvilke dataprogram AMK-operatørene er avhengig av i sitt arbeid.

Men med dagens trusselbilde, hvor det har vært gjentatte forsøk på å få tilgang til sensitive personopplysninger, er det fare for at en trussel-aktører kan prøve å få tilgang til opplysninger i en slik videotjenesten. I denne oppgaven har jeg derfor sett på hvilke lover og instrukser som gjelder for personvern og informasjonssikkerheten i helsevesenet generelt og hvordan disse er ivaretatt i en slik tjenesten.

For å få en oversikt over hvilke lover og vedtekter som ivaretar personvernet for pasienter og stiller krav til aktørene i helsevesenet har jeg benyttet meg av Normen, en bransjestandard for informasjonssikkerhet i helsevesenet. Denne er basert på gjeldende lover og instrukser.

Videotjenesten som AMK Oslo har utviklet i samarbeid med NLA har vært utprøvd ved AMK-sentraler ulike steder i Norge. Disse testene har gitt verdifull innsikt i hvordan både AMK-operatørene og innringer vurderer bruken av tjenesten. En spørreundersøkelse blant AMK-operatørene som har testet tjenesten, ville derfor gitt ett godt bilde av hvordan tjenesten fungerer. Men det kom inn for få svar på spørreundersøkelsen til å gi et sikkert bilde av hvordan AMK-operatørene opplever at den nye tjenesten fungerer i deres arbeid. De innkomne svar er allikevel tatt med i oppgaven, da dette gir verdifull innsikt i betydningen av tjenesten.

For å se hvilke personverns-messige utfordringer implementering av en slik tjeneste møter, har jeg utført en risikoanalyse av en tjeneste som har funksjonalitet for å tilby videosamtale mellom AMK-operatør og innringer.

Som det går frem av min sårbarhets og risiko-analyse, er det svært viktig at AMK-operatør får god opplæring før tjenesten tas i bruk. Dette er også et ønske som er beskrevet i behovskartleggingen ved at tjenesten må være tidseffektiv, samt at den må føles trygg å bruke. I et av svarene fra AMK-operatørene som deltok i spørreundersøkelsen, er man bekymret for at operatør og innringer blir for opptatt med den tekniske løsningen, slik at innringer og AMK-operatør blir mindre fokusert på pasienten. Det går ut over pasienten, at man må bruke tid på å forklare hva personen skal trykke på. Ved å gi de ansatte som skal benytte tjenesten god og variert opplæring, tydelige og robuste rutiner, samt realistiske øvelser vil denne sårbarheten bli svært redusert.

Også publikum må bli kjent med den nye teknologien som er tatt i bruk ved en nødsamtale. Det anbefales derfor at norske helsemyndigheter, gjennomfører kampanjer og opplysningsarbeid før denne tjeneste tilbys befolkningen nasjonalt. Videre anbefales det at bruk av videotjenesten innføres som en del av grunnleggende førstehjelpskurs for befolkningen generelt.

En annen klar forutsetning som har kommet frem, både i behovskartleggingen, i spørreundersøkelsen og i risikovurderingen, er kravet om at det ikke skal være mulig å lagre datastrømmen som går fra kamera på innringers mobil-enhet til AMK-operatørens datamaskin. Også i veileder for Normen Faktaark 54 – Videokonsultasjon, er lagring av videoopptak holdt utenom. Det er helt avgjørende at innringer ikke kan lagre datastrømmen på egen mobiltelefon. Dette for å best mulig ivareta personvernet til de involverte, som er i en sårbar situasjon og i mange tilfeller ikke samtykkekompetente i den aktuelle situasjonen En må ikke risikere at pasienter i en sårbar situasjon får hendelsesforløpet ved en ulykke, distribuert på bl.a. sosiale medier. Det må heller ikke være mulig å lagre datastrømmen i AMK-sentralens infrastruktur. Dersom en slik lagring var mulig, ville det gitt en høy risiko for at enkelte trussel-aktører hadde høy motivasjon for å prøve å få tilgang til svært sensitiv informasjon.

For å sikre at ikke uvedkommende får tilgang til datastrømmen fra innringers kamera inn til AMK-operatørens datautstyr og dermed inn til databehandlers infrastruktur, er det anbefalt som tiltak at der blir foretatt en penetrasjonstest av tjenesten. Dette for å identifisere sikkerhetshull og systemsvakheter, samt å peke på hvor det trengs å iverksette kortsiktige og langsiktige tiltak for å redusere evt. sårbarheter.

Den største sårbarheten i denne tjenesten, som i de fleste andre tjenester som inneholder sensitive personopplysninger, og som derfor er det viktig å få adressert og kontroll over, er hvordan dataeier og databehandler behandler dataene i tjenesten, våre helseopplysninger. Det er viktig at bl.a. databehandler-avtaler, sertifiseringer og andre forordninger er på plass for å forsikre oss om at de som behandler helseopplysningene våre, har et bevist forhold til disse. Norm for informasjonssikkerhet – Normen, er bransjestandarden som kreves som ett minimum. Tjenesteleverandør må kunne dokumentere hvordan tjenesten er bygget opp for å møte krav om sikkerhets-arkitektur, autentisering, autorisering og sporbarhet. Krav om at pasient kan kreve sperring av deler av eller hele pasientjournalen, er ikke relevant for denne tjenesten, da datastrømmen ikke blir lagret. Det er heller ikke kravet om at det skal utarbeides en DPIA for å sikre at det ikke blir innhentet mer informasjon om pasienten enn det

tjenesten krever. Men det er krav om at det enkelte helseforetak som tar tjenesten i bruk må utarbeide robuste prosedyrer for tjenesten, som er i samsvar med øvrige prosedyrer på den aktuelle AMK-sentral.

I behovsanalysen til Making Waves ble det konkludert med at tjenesten kan levers, slik den er beskrevet innenfor rammene av gjeldende lovverk. Men også de peker på at dette er under forutsetning av at videostrømmen ikke kan lagres, hverken på innringers enhet eller på AMK-operatøren sitt Ikt-utstyr.

Jeg mener denne oppgaven kan konklusjonen med at dette er et svært viktig verktøy for AMK-operatørene, som med gitte forutsetninger, er innenfor akseptable rammer for informasjonssikkerheten til enkeltmennesker i en sårbar situasjon.

AMK-operatørene rapporterer om at de har reddet mange liv allerede på den tiden de har hatt tilgang til video som verktøy. Den beskrives som «Et helt uvurderlig verktøy. En ny æra innen akuttmedisin»

8 Referanser

Carlsen, H. (2013). – Helseapper på mobilen kan bli en personvernutfordring. *NRK*. Retrieved from https://www.nrk.no/viten/kraftig-vekst-i-helseapper-1.10889587

Christie, W., Hoholm, T., & Mørk, B. E. (2018). Innovasjon og samhandling i helsevesenet. *Praktisk økonomi & finans, 34*(1), 32-46. doi:10.18261/issn.1504-2871-2018-01-04 ER

Datatilsynet. (Ed.) (2019a) Datatilsynet. Datatilsynet.

Datatilsynet. (Ed.) (2019b) Datatilsynet.

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjeneste, (2018).

Innovasjonspartnerskap – Videosamtale med Akuttmedisinsk kommunikasjonssentral (AMK). (2019, 26.11.2019). Retrieved from https://vestreviken.no/helsefaglig/forskning-og-innovasjon/innovasjonspartnerskap-videosamtale-med-akuttmedisinsk-kommunikasjonssentral-AMK#utfordring-og-behovsbeskrivelse

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), 1 C.F.R. (2014).

Kvinge, F.-H. (2013). Hvordan samsvarer AMIS-notatet på AMK med ambulansejournalen i ambulansetjenesten i OSlo og Akershus ? *Det midisinske fakultet, universitetet i Oslo*, 33. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/38335/Prosjektoppgavenxendeligxversjonx05.07.13.pdf?sequence=1&isAllowed=y

omsorgsdepartementet, H.-o. (2016). *Sentrale elementer vedrørende organisering av AMK-sentralene*. Helse- og omsorgsdepartementet Retrieved from https://www.regjeringen.no/contentassets/b332572e94304549b8b6db04ad617f76/AMK_utredning_150916.pdf

omsorgsdepartementet, H. G. l. H. o., RHF, A.-L. S. H. N., RHF, K. M. H. H. M.-N., RHF, A. H. B. H. V., RHF, T. K. H. S.-Ø., HF, K. A. L. H. d. f. n., . . . Helsedirektoratet, B. J. (2016). *Sentrale elementer vedrørende organisering av AMK-sentralene*. Retrieved from https://www.regjeringen.no/contentassets/b332572e94304549b8b6db04ad617f76/AMK_utredning_150916.pdf

Platou, P. H.-C. S. (2019, 25.02.2020). Innovasjonspartnerskap – Videosamtale med Akuttmedisinsk kommunikasjonssentral (AMK). Retrieved from https://vestreviken.no/helsefaglig/forskning-og-innovasjon/innovasjonspartnerskap-videosamtale-med-akuttmedisinsk-kommunikasjonssentral-AMK#bakgrunn

Terje Olav Øen, B. H. F. H., seniorrådgiver/prosjektleder, RHF, H. H. V., Per Christian Juvkam, S., Klinikk for akuttbehandling/, AMK, H. M. o. R. H., Arne O. Aksnes, K. K. h., & Åge C. Jensen, A. s. A. B. t. R. v. K. (2018). Håndbok Kommunikasjon og samhandling i akuttmedisinske situasjoner. *Nasjonalt kompetansesenter for helsetjenestens kommunikasjonsberedskap*. Retrieved from https://kokom.no/wp-content/uploads/2019/01/KoKom-h%C3%A5ndbok-2017_6.korrNY.pdf

Waves, M. (2019). Behovskartlegging Sluttrapport utarbeidet av Making Waves på oppdrag fra Vestre Viken . Videosamtaler med Akuttmedisinsk kommunikasjonssentral. Retrieved from https://vestreviken.no/Documents/AMK-innovasjonspartnerskap/Sluttrapport%20om%20behovskartlegging%20for%20videosamtaler%20med%20AMK%20i%20Vestre%20Viken%20121119%20.pdf

Helseregisterloven, 2 C.F.R. (2014).

komiteene, D. n. f. (2020). Hva er særlige kategorier av personopplysninger. Retrieved from https://www.etikkom.no/Aktuelt/gdpr-og-forskning/sos-definisjoner-og-begreper-hva-er-sarlige-kategorier-av-personopplysninger/

Bokmålsordboka. (Ed.) (2020) Bokmålsordboka. Språkrådet.
Datatilsynet. (Ed.) (2019) Datatilsynet. Datatilsynet.
Datatilsynet. (2020). Vurdering av personvernkonsekvenser (DPIA). Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser
De nasjonale forskningsetiske komiteene. (2020). Hva er særlige kategorier av personopplysninger. Retrieved from https://www.etikkom.no/Aktuelt/gdpr-og-forskning/sos-definisjoner-og-begreper-hva-er-sarlige-kategorier-av-personopplysninger/
Helsedirektoratet. (2020). Akuttmedisinske tjenester. Retrieved from https://AMK.beekeeper.no/om
Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), 1 C.F.R. (2014a).
Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), 2 C.F.R. (2014b).
Kokom. (2018). Håndbok Kommunikasjon og samhandling i akuttmedisinske situasjoner In (pp. 4): Nasjonalt kompetansesenter for helsetjenestens kommunikasjonsberedskap.
Meld. St. 16 Nasjonal helse- og omsorgsplan (2011–2015). (2011). *Nasjonal helse- og omsorgsplan (2011–2015)*. Det kongelige helse- og omsorgsdepartementet Retrieved from https://www.regjeringen.no/contentassets/f17befe0cb4c48d68c744bce3673413d/no/pdfs/stm201020110016000dddpdfs.pdf
Nakos - prehospital akuttmedisin. (2019). Kartlegging av den akuttmedisinske kjeden In *RAPPORT nr. 1/2019*
NOU 2015: 17 Først og fremst. (2015). *Først og fremst — Et helhetlig system for håndtering av akutte sykdommer og skader utenfor sykehus*. Retrieved from https://www.regjeringen.no/no/dokumenter/nou-2015-17/id2465765/
Oslo universitetssykehus OUS. (2020). Akuttmedisinsk kommunikasjonssentral (AMK) Retrieved from https://oslo-universitetssykehus.no/avdelinger/prehospital-klinikk/akuttmedisinsk-kommunikasjonssentral-AMK#les-mer-om-akuttmedisinsk-kommunikasjonssentral-AMK
Samtykke, 4 C.F.R. (2019).
Platou, P. H.-C. S. (2019, 25.02.2020). Innovasjonspartnerskap – Videosamtale med Akuttmedisinsk kommunikasjonssentral (AMK). Retrieved from https://vestreviken.no/helsefaglig/forskning-og-innovasjon/innovasjonspartnerskap-videosamtale-med-akuttmedisinsk-kommunikasjonssentral-AMK#bakgrunn
Store norske leksikon. (Ed.) (2019a) Store Norske leksikon.
Store norske leksikon. (Ed.) (2019b) Store Norske leksikon.
Store norske leksikon. (Ed.) (2019c) Store Norske leksikon.
Utredning AMK-sentralene. (2016). *Sentrale elementer vedrørende organisering av AMK-sentralene*. Helse- og omsorgsdepartementet Retrieved from https://www.regjeringen.no/contentassets/b332572e94304549b8b6db04ad617f76/AMK_utredning_150916.pdf

Flight Following – Funksjon. (2020). *Flight Following – Funksjon*. Retrieved from http://www.luftambulanse.no/system/files/internett-vedlegg/46-2012_121129_Flight%20following_vedlegg%20C.pdf

Forskrift om krav til og organisering av kommunal legevaktordning, ambulansetjeneste, medisinsk nødmeldetjeneste mv. (akuttmedisinforskriften), (2015).
Informasjonssikkerhet i helse- og omsorgssektoren § 3.2.2 (2019).
Helse- og omsorgsdepartementet. (2016). *Sentrale elementer vedrørende organisering av AMK-sentralene*. Helse- og omsorgsdepartementet Retrieved from https://www.regjeringen.no/contentassets/b332572e94304549b8b6db04ad617f76/AMK_utredning_150916.pdf

Helse og omsorgsdepartementet. (2016). Personvern og informasjonssikkerhet. Retrieved from https://www.regjeringen.no/no/tema/helse-og-omsorg/e-helse/innsikt/personvern-og-informasjonssikkerhet/id2480194/

Lov om helsepersonell m.v. (helsepersonelloven), (2000).
Lov om helseregistre og behandling av helseopplysninger (helseregisterloven), 1 C.F.R. (2014).
Informasjonssikkerhet i helse- og omsorgssektoren § 3.3 (2019).
Normen. (2020). Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. In.
Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven), (2019).
Forskrift om pasientjournal (pasientjournalforskriften), (2019).
Personvernforordningen (GDPR), (2018).
Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven), (2001).
Store norske leksikon. (Ed.) (2019a) Store Norske leksikon.
Store norske leksikon. (Ed.) (2019b) Store Norske leksikon.

Datatilsynet. (Ed.) (2019) Datatilsynet. Datatilsynet.
Norm for informasjonssikkerhet og personvern i helse- og omsorgstjeneste, (2018a).
Direktoratet for e-helse (2018b). Personvern og informasjonssikkerhet. Retrieved from https://ehelse.no/tema/personvern-og-informasjonssikkerhet
Helse og omsorgsdepartementet. (2016). *Personvern og informasjonssikkerhet*. Regjeringen Retrieved from https://www.regjeringen.no/no/tema/helse-og-omsorg/e-helse/innsikt/personvern-og-informasjonssikkerhet/id2480194/
Jøsang, A. (2018). Introduksjon til informasjonssikkerhet. In (pp. 4). Universitetet i Oslo.
Kongeriket Noregs grunnlov, 102 C.F.R. (1814).
Informasjonssikkerhet i helse- og omsorgssektoren § 3.3 (2019).
Normen. (2020). Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. In.

Andersen, K. H. (2013). Mobil App med helseopplysninger – en mulighetsstudie innenfor det norske lovverket Forord s. III. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/38441/Masteroppgave-Knut-Henrik-Andersen2013Korrigertfeb2014.pdf?sequence=7&isAllowed=y
Aven, T. (2011). Misforstått risiko. Retrieved from https://forskning.no/partner-boker-sikkerhet/misforstatt-risiko/780106
Barzinje, A. M. (2010). Risikovurdering ved lovpålagte tilsyn med informasjonssikkerhet i helseforetak. Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143936/Masteroppgave+til+Ali+Mohammed+Barzinje.pdf?sequence=1
Brørs, & Nordstrøm. (2017). Operatørkrav til avstandsoppfølgingssystem i et kommunalt responssenter - En brukersentrert tilnærming. (24.04.2020). Retrieved from https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2445850
Carlsen, H. (2020). Forbyr ansatte å bruke populær videokonferanse-tjeneste. Retrieved from https://www.nrk.no/norge/forbyr-ansatte-a-bruke-populaer-videokonferanse-tjeneste-1.14968765
Datatilsynet. (2019a). Risiko og risikovurdering. *Datatilsynet.* Retrieved from https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/risikovurdering
Datatilsynet. (Ed.) (2019b) Datatilsynet.
Datatilsynet. (Ed.) (2019c) Datatilsynet.
Direktoratet for e-helse. (2019). *Innbyggerundersøkelse om e-helse 2019 Direktoratet for e-helse*. Retrieved from https://ehelse.no/tema/nasjonale-e-helselosninger/_/attachment/inline/143e2104-bf9c-4a0f-be70-28f9dca18ce6:c9b59c94e94eefc7ea1f5d1e341d72951cbc7c38/Innbyggerundersøkelse%20om%20e-helse%202019.pdf

Direktoratet for økonomistyring. (2016). Grunnkurs i risikostyring. In.
Hotvedt, & Melbye. (2013). Videokonferanse og mobiltelefoner: Nye muligheter for 113. (24.04.2020). Retrieved from https://munin.uit.no/handle/10037/6359
Jøsang, A. (2018). Introduksjon til informasjonssikkerhet. In (pp. 4). Universitetet i Oslo.
Kalveland. (2019). Legekontor utsatt for hackerangrep. Retrieved from https://www.dagensmedisin.no/artikler/2019/10/21/legekontor-utsatt-for-hackerangrep/
Kandidat 670 Det juridske fakultet UIO. (2016). Personvern i elektronisk pasientjournal - Til hinder for forsvarlig helsehjelp. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/54317/670.pdf?sequence=26&isAllowed=y
Klungtveit. (2018). E-tjenesten frykter at Kina hacket pasientinfo om 2,9 millioner nordmenn. Retrieved from https://filternyheter.no/kinesere-hacket-helse-sor-ost-e-tjenesten-frykter-at-pasientinfo-om-29-millioner-nordmenn-er-stjalet/
Kristensen, K. (20115). Lokal snøskredvarsling og vurdering av treffsannsynlighet 25.
Lund Flinck (2017). WannaCrypt: Derfor var det store virusangrepet så farlig Retrieved from https://komputer.no/sikkerhet/wannacrypt-derfor-var-det-store-virusangrepet-sa-farlig
Informasjonssikkerhet i helse- og omsorgssektoren § 3.3 (2019).
Normen v. 5.3. (2020). Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. In.
NTNU. (2020). Informasjonssikkerhet - risikovurdering Retrieved from https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikostyring/pop_up?_36_viewMode=print
Øvreberg, E. (2011). Kan redde liv med videosamtale. Retrieved from https://forskning.no/partner-forebyggende-helse-uit-norges-arktiske-universitet/kan-redde-liv-med-videosamtale/770237
Sør-Øst, H. (2018). Informasjonssikkerhet og personvern er styrket etter datainnbruddet. Retrieved from https://www.helse-sorost.no/nyheter/informasjonssikkerhet-og-personvern-er-styrket-etter-datainnbruddet
Standard Norge. (2020). Risikostyring. Retrieved from https://standard.no/fagomrader/kvalitet-og-/risikostyring/

Making Waves. (2019). *Behovskartlegging*

Sluttrapport utarbeidet av Making Waves på oppdrag fra Vestre Viken 31. oktober 2019 Videosamtaler med Akuttmedisinsk kommunikasjonssentral. Retrieved from Vestre Viken: https://vestreviken.no/Documents/AMK-innovasjonspartnerskap/Sluttrapport%20om%20behovskartlegging%20for%20videosamtaler%20med%20AMK%20i%20Vestre%20Viken%20121119%20.pdf

Blekesaunet, A. Forskning - Forelesning 3. In.
Ellingsen, S. D. o. S. (2009). Forståelse av kvantitativ helseforskning - en introduksjon og oversikt. *Nordisk Tidsskrift for Helseforskning 2 2009*. Retrieved from https://septentrio.uit.no/index.php/helseforsk/article/view/244/234
Fangen, K. (2015). Kvalitativ metode. *De nasjonale forskningsetiske komiteene*. Retrieved from https://www.etikkom.no/FBIB/Introduksjon/Metoder-og-tilnarminger/Kvalitativ-metode/
Mathiesen;Slyngstadli. (2017, 11.05.20). Informasjonssikkerhet - risikovurdering. *Innsida NTNU.* Retrieved from https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikostyring
Sigrunn Drageset, S. E. (2009). Forståelse av kvantitativ helseforskning - en introduksjon og oversikt *Nordisk Tidsskrift for Helseforskning, 2*. Retrieved from https://septentrio.uit.no/index.php/helseforsk/article/view/244/234
Store norske leksikon. (Ed.) (2019) Store Norske leksikon.
Svanæs, D. *Hva er forskning ?* Retrieved from https://www.idi.ntnu.no/emner/it3402/brukersentrert.pdf

Svensberg, K., & Kristine Heitmann. (2014). Kvalitativ forskning – en gullgruve for farmasøyter. *Vitenskap*. Retrieved from https://admin.farmatid.no/sites/default/files/nft_6_2014_s_28-31_0.pdf
Tjora, A. (2011). *Kvalitative forskningsmetoder i praksis*: Gyldendal akademisk.

Elgmork, K. (1985). *Vitenskaplige metoder*: Universitetsforlaget.
Godkjenning av medisinsk og helsefaglig forskning,. (2017). In. Uio Det medisinske fakultetet.
Lov om medisinsk og helsefaglig forskning 1C.F.R. (2009).
Kaarbø, E. (2009 - 2019). Kombinerte metoder. *Sykepleien*. Retrieved from https://sykepleien.no/forskning/2009/10/kombinerte-metoder
Kvinge, F.-H. (2013). Hvordan samsvarer AMIS-notatet på AMK med ambulansejournalen i ambulansetjenesten i OSlo og Akershus ? *Det midisinske fakultet, universitetet i Oslo*, 33. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/38335/Prosjektoppgavenxendeligxversjonx05.07.13.pdf?sequence=1&isAllowed=y
Locus. (2020). Hvor, hva, hvem? Retrieved from http://www.locus.no/helse/category520.html
Making Waves. (2019). *Behovskartlegging*

Sluttrapport utarbeidet av Making Waves på oppdrag fra Vestre Viken 31. oktober 2019 Videosamtaler med Akuttmedisinsk kommunikasjonssentral. Retrieved from Vestre Viken: https://vestreviken.no/Documents/AMK-innovasjonspartnerskap/Sluttrapport%20om%20behovskartlegging%20for%20videosamtaler%20med%20AMK%20i%20Vestre%20Viken%20121119%20.pdf
Malterud, K. (2002). Kvalitative metoder i medisinsk forskning – forutsetninger, muligheter og begrensninger. *Tidsskriftet Den Norske Legeforening, 25*. Retrieved from https://tidsskriftet.no/2002/10/tema-forskningsmetoder/kvalitative-metoder-i-medisinsk-forskning-forutsetninger-muligheter
NSD - Et verktøy for forskning - Strategi 2016 - 2019. (2015). Retrieved from https://nsd.no/om/doc/strategiplan-2016-2019.pdf
SurveyMonkey. (2020). Forskjellen mellom kvantitative og kvalitative undersøkelser. Retrieved from https://no.surveymonkey.com/mp/quantitative-vs-qualitative-research/
Svensberg, K., & Kristine Heitmann. (2014). Kvalitativ forskning – en gullgruve for farmasøyter. *Vitenskap*. Retrieved from https://admin.farmatid.no/sites/default/files/nft_6_2014_s_28-31_0.pdf
Tjora, A. (2011). *Kvalitative forskningsmetoder i praksis*: Gyldendal akademisk.

Kristensen, K. (2015). Lokal snøskredvarsling og vurdering av treffsannsynlighet 25.

Bakkeli, V. (2012). Åpne visjoner og interaksjon på tvers - Smarthusteknologi i en offentlig-privat innovasjonsprosess. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/34357/Bakkelix2012.pdf?sequence=1&isAllowed=y
Blekesaunet, A. (2020). Forskning - Forelesning 3. In.
Svanæs, D. (2015). *Hva er forskning ?* Retrieved from https://www.idi.ntnu.no/emner/it3402/brukersentrert.pdf
Tjora, A. (2011). *Kvalitative forskningsmetoder i praksis*: Gyldendal akademisk.

3M. (2020). 3M, Science. Applied to life Retrieved from https://www.3mnorge.no/3M/no_NO/privacy-protection-ndc/video-news/full-story/~/data-security-in-the-healthcare-sector/?storyid=3ad3a4e2-f8f9-4fd0-b2c7-06584b29aaee
Brudvik, M. (Ed.) (2010) Helsebiblioteket.
DALE, C. (2018). Hva er penetrasjonstesting? In.
Direktoratet for e-helse. (2019). *Tilgangsstyring i helse- og omsorgssektoren. Anbefaling av tillitsmodell for data- og dokumentdeling*. Retrieved from https://ehelse.no/standarder/ikke-standarder/anbefaling-av-tillitsmodell-for-data-

og-dokumentdeling/_/attachment/inline/4b78b44e-dbfe-4f13-9527-4b47e19a5585:a1003d97d50492bed6eb8064a936354b88a5abf0/Anbefaling%20av%20tillitsmodell%20for%20data-%20og%20dokumentdeling.pdf
Faktaark 54 - Videokonsultasjon, (2020).
Helse Sør Øst RHF. (2020a). HSØ - Risikoskala for informasjonssikkerhet. Retrieved from https://www.helse-sorost.no/Documents/Informasjonssikkerhet%20og%20personvern/Styringssystem%20for%20informasjonssikkerhet/Regionalt%20styrende%20dokumenter/Styrende/NO-5%20-%20Vedlegg%20-%20Risikoskala%20for%20informasjonssikkerhet.pdf
Sikkerhetsprinsippene, (2020b).
Forskrift om informasjonssikkerhet ved elektronisk tilgang til helseopplysninger i behandlingsrettede helseregistre, (2011).
Jansen, A. (2018). Fagspråk. Retrieved from https://ndla.no/nb/subjects/subject:25/topic:1:193102/topic:1:189995/resource:1:119607?filters=urn:filter:d97809a8-47b6-4d26-ae5c-1839f4c27940
Johnsen, H. F. (2018). Nød-apper kan redde liv. *Online*. Retrieved from https://www.online.no/apper/nodapper.jsp
Kvinge, F.-H. (2013, s7). Hvordan samsvarer AMIS-notatet på AMK med ambulansejournalen i ambulansetjenesten i OSlo og Akershus ? *Det midisinske fakultet, universitetet i Oslo*, 33. Retrieved from https://www.duo.uio.no/bitstream/handle/10852/38335/Prosjektoppgavenxendeligxversjonx05.07.13.pdf?sequence=1&isAllowed=y
Mathiesen Slyngstadli. (2017, 11.05.20). Informasjonssikkerhet - risikovurdering. *Innsida NTNU.* Retrieved from https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikostyring
Nasjonal sikkerhetsmyndighet. (2020). Grunnprinsipper for IKT-sikkerhet 2.0. Retrieved from https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/de-fire-kategoriene/)
Nødnett. (2017). Nødetatenes kontrollromstilknytning. Retrieved from https://www.nodnett.no/tjenester/kommunikasjonssentraler/kommunikasjonssentraler/
Politiet. (2015). *Helsepersonellets taushetsplikt – rett og plikt til å utlevere pasientopplysninger til politiet* Retrieved from https://www.helsedirektoratet.no/rundskriv/rett-og-plikt-til-a-utlevere-pasientopplysninger-til-politiet/Helsepersonellets%20taushetsplikt%20%E2%80%93%20Rett%20og%20plikt%20til%20%C3%A5%20utlevere%20pasientopplysninger%20til%20politiet%20%E2%80%93%20Rundskriv.pdf/_/attachment/inline/23b06da7-0659-4de6-b2b3-f24bf02cdd0b:e6459016a8c2d6a1b2b9d21f8cced0f4601954a9/Helsepersonellets%20taushetsplikt%20%E2%80%93%20Rett%20og%20plikt%20til%20%C3%A5%20utlevere%20pasientopplysninger%20til%20politiet%20%E2%80%93%20Rundskriv.pdf
QmPlus. (Ed.) (2010).
Regjeringen. (2019). Ny lov skal styrke digitaliseringen i helsesektoren. Retrieved from https://www.regjeringen.no/no/aktuelt/ny-lov-skal-styrke-digitaliseringen-i-helsesektoren/id2675566/
Store norske leksikon. (Ed.) (2019) Store Norske leksikon.
Sykehuset Innlandet HF. (2020a). Dataangrep mot Sykehuset Innlandet HF. In.
Sykehuset Innlandet HF. (2020b). Dataangrep mot Sykehuset Innlandet HF. Retrieved from https://sykehuset-innlandet.no/om-oss/aktuelt/nyheter/dataangrep-mot-sykehuset-innlandet-hf

9 Vedlegg

NR	Dokumenteier	Dokumentnavn	Dato	Dokument
1	Torhild Ulvesæter	Spørreundersøkelsen	07.10.2020	Spørreundersøkelsen.docx
2	Torhild Ulvesæter	Forespørsel Spørreundersøkelse	07.10.2020	Forespørsel_Spørreundersøkels
3	AMK Oslo V / Jørgen Emil Hauge Skogmo	Videooverføring fra Hjelp 113-appen til AMK	07.10.2020	Hjelp113-videooverfÃ¸ring2bf.pdf
4	Helse Sør Øst	Sikkerhetsprinsipper og krav for IKT-infrastruktur og applikasjoner	06.11.2020	NO-19 - Sikkerhetsprinsippe
5	Sykehuspartner	Ros_MAL_risikovurdering	13.11.20	ROS_MAL_Risikovurdering+(HSØ).docx