Masteroppgave

NTNU
Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Sarita Sunder

Informasjonssikkerhetskultur i spesialisthelsetjenesten

En sosio-teknisk casestudie av Akershus universitetssykehus

Masteroppgave i Informasjonssikkerhet
Veileder: Stewart Kowalski
Juni 2023

NTNU
Kunnskap for en bedre verden

Sarita Sunder

Informasjonssikkerhetskultur i spesialisthelsetjenesten

En sosio-teknisk casestudie av Akershus universitetssykehus

Masteroppgave i Informasjonssikkerhet
Veileder: Stewart Kowalski
Juni 2023

Norges teknisk-naturvitenskapelige universitet
Fakultet for informasjonsteknologi og elektroteknikk
Institutt for informasjonssikkerhet og kommunikasjonsteknologi

NTNU

Kunnskap for en bedre verden

Abstract

Digitization has made it possible to deliver healthcare services of good quality. The use of technology has led to security related challenges and there is a drastic increase in the number of cyber attacks directed at Norwegian hospitals. Research shows that healthcare personnel lack knowledge about information security and that this vulnerability is constantly exploited by threat actors during cyber attacks. The need for security awareness and training programs is therefore significant. However, this work has been challenging to conduct in practice as healthcare personnel often prioritize patient safety over training in information security.

This master's thesis present a new training concept that potentially could contribute to increase the focus towards information security. The concept combines aspects of information security and patient safety in one training program to ensure more frequent training. The master's thesis will therefor answer the research question "Which preconditions should be satisfied for Norwegian hospitals to include information security as a part of patient safety education?". An extensive literature study was performed to map similar research in the field. The healthcare organizations are complex and there is a need for cooperation between different organizational levels before new methods can be tested in practice. Therefore, a case study of Akershus University Hospital was conducted and qualitative interviews of key personnel at strategic, tactical, and operational level were carried out. The aim was to map whether the training concept is applicable in practice based on their experiences and motivation for improving their skills in information security. A socio-technical analysis of the collected data was then performed to form a decision-making basis for whether the concept is applicable in practice and the preconditions for realizing this work.

The results shows that the majority believe the concept is applicable and that healthcare personnel are motivated to participate in such a training program. However, some challenges arise from the existing safety culture which may impact the implementation of this concept. The results of this study cannot be generalized as there is a need for further research. However, the study forms a solid basis for further work with the possibility of testing the concept in practice.

Sammendrag

Økt digitalisering har gjort det mulig å levere helsetjenester av god kvalitet. Bruk av teknologi har imidlertid dannet grobunn for sikkerhetsrelaterte utfordringer og det observeres en drastisk økning i antall cyberangrep rettet mot norske sykehus. Forskning viser at helsepersonell ikke har tilstrekkelige kunnskaper i informasjonssikkerhet og at denne sårbarheten stadig utnyttes av trussel aktører under cyberangrep. Behovet for sikkerhetsrelatert kompetanseheving er derfor stort. Det viser seg imidlertid at dette arbeidet er utfordrende da helsepersonell ofte prioriterer pasientsikkerhet fremfor opplæring i informasjonssikkerhet.

I dette masterprosjektet presenteres det derfor et nytt opplæringskonsept som potensielt kan bidra til å rette fokuset mot informasjonssikkerhet i en hektisk hverdag. Konseptet kombinerer aspekter i informasjonssikkerhet og pasientsikkerhet i et opplæringsforløp for å sikre at det gis hyppigere opplæring sammenlignet med i dag. Masteroppgaven besvarer forskningsspørsmålet: "Hvilke forutsetninger bør oppfylles for at norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet?». En omfattende litteraturstudie ble gjennomført for å undersøke om det finnes tilsvarende forskning på feltet. Sykehussystemet er svært komplekst og for å tilrettelegge for en ny arbeidsmetode kreves det et samarbeid mellom ulike organisatoriske nivåer før metoden kan testes i praksis. I den forbindelse ble det utført en casestudie av Akershus Universitetssykehus der en rekke kvalitative intervjuer av nøkkelpersonell på strategisk, taktisk og operativt nivå ble gjennomført. Det ble undersøkt om opplæringskonseptet er anvendbart i praksis basert på deres erfaringer og motivasjon for kompetanseheving. Deretter ble en sosio-teknisk analyse av innhentet data gjennomført for å danne et beslutningsgrunnlag for om konseptet er anvendbart i praksis og hvilke forutsetninger som må oppfylles for å realisere dette arbeidet.

Resultatene fra undersøkelsen viser at majoriteten mener konseptet er nyttig og at helsepersonell har motivasjon til å delta på et slikt opplæringsprogram. Det fremkommer likevel utfordringer ved den eksisterende sikkerhetskulturen som kan ha en innvirkning på gjennomførelsen av dette arbeidet. Resultatene fra undersøkelsen kan på nåværende tidspunkt ikke generaliseres da det er behov for ytterligere forskning. Studien danner imidlertid et solid grunnlag for videre arbeid med mulighet for å teste konseptet i praksis.

Innhold

Figurer

Tabeller

Forord

Det er med stor glede og entusiasme at jeg nå presenterer min masteroppgave innenfor to fagfelt jeg virkelig brenner for; helse og informasjonssikkerhet. Som tidligere utdannet sykepleier med erfaring fra spesialisthelsetjenesten, har det vært utrolig spennende å kunne anvende mine erfaringer og kunnskaper i denne oppgaven. Det har gitt meg muligheten til å utforske hvordan helsesektoren kan arbeide mot en mer robust sikkerhetskultur.

Jeg ønsker å rette en stor takk til Akershus Universitetssykehus som har vært oppdragsgiver for denne masteroppgaven. En spesiell takk rettes til eksterne veiledere, Kåre Magne Stennes og Espen Thorsen Frank som gjennom hele prosjektperioden har stilt opp, gitt nyttig innspill og bidratt til inspirerende refleksjon. Deres støtte, veiledning og innsikt har vært til stor hjelp gjennom hele prosjektet. Jeg ønsker å takke alle informanter som stilte opp til intervju. Denne oppgaven hadde ikke vært mulig å gjennomføre uten dere. Videre takker jeg min interne veileder, Stewart Kowalski som har vært en stor inspirasjon gjennom hele prosjektperioden. Til slutt vil jeg rette en stor takk til min kjære familie for deres støtte og oppmuntring gjennom den lærerike reisen. Gjennom 5 år på NTNU er jeg stolt over å ha fullført min mastergrad som symboliserer dedikasjon, lærdom og ekspertise innen feltet. Jeg sitter igjen med verdifull kompetanse og ser frem til å innta arbeidslivet.

Kapittel 1

Introduksjon

Bruk av teknologi har lenge vært kjernen i det å utvikle helsetjenester av god kvalitet. Det benyttes elektroniske systemer for å effektivisere arbeidsprosesser og helsepersonell har fått mer tid til å utføre direkte pasientbehandling (Berntsen, 2022; Direktoratet for eHelse, 2020). Bruk av digitale systemer åpner imidlertid opp for sikkerhetsrelaterte utfordringer som kan påvirke pasientsikkerheten (Direktoratet for eHelse, 2020). Det prosesseres daglig et stort kvantum data relatert til pasientbehandling, forskning og forbedring av helsetjenester (Meld. St. 7 (2019-2020)). Slik data anses å være svært ettertraktet av trusselaktører da det ofte benyttes som et pressmiddel for å oppnå ulike mål. Sykehusene på sin side er sårbare som følge av at helsepersonell mangler kunnskaper om informasjonssikkerhet og hvordan de kan beskytte sykehuset sine informasjonsverdier (Berntsen, 2022). Slike faktorer blir stadig utnyttet av trusselaktører og bidrar til å øke risikoen for å bli utsatt for alvorlige cyberangrep. Under slike hendelser kan sykehusdriften rammes i form av bortfall av IKT-tjenester, noe som kan føre til at pasienter ikke mottar nødvendig helsehjelp (Helsetilsynet, 2020). Dette viste seg da Helse-Sør Øst ble utsatt for et cyberangrep i utgangen av 2017. Konsekvensene av angrepet førte at nødrutiner ble iverksatt som følge av at kommunikasjonssystemer mellom pasienter, sykehus og ambulansetjenesten ble påvirket (Bruvoll, Thuv & Enemo, 2020).

Nasjonale ekspertorganer estimerer at antall alvorlige cyberangrep på nasjonalt nivå vil øke i tiden fremover (NSM, 2023a). HelseCERT rapporterer i tillegg at det er over 90 prosent sannsynlig at digitale systemer i helsesektoren på et tidspunkt rammes (Helsenett, 2022). Dette kan trolig henge sammen med den sikkerhetspolitiske krisen Norge ble involvert i ved utspring av krigen mellom Russland og Ukraina i 2022. På bakgrunn av at Norge har bistått Ukraina, har forholdet til Russland blitt mer anspent. Konsekvensene har blant annet ført til at aktører fra Russland har utført en rekke cyberkampanjer mot norske virksomheter (NSM, 2023a). Sammen med Kina, Iran og Nor-Korea utgjør Russland en av de største truslene mot det digitale domenet i Norge. Disse aktørene har en enorm kapasitet, kapabilitet og motivasjon til å holde på i lang tid. De utvikler stadig nye verktøy

og teknikker for å gjennomføre sofistikerte angrep (Politiets Sikkerhetstjeneste, 2023; Etterretningstjenesten, 2023). Senest i starten av 2023 opplyste en rekke nasjonale medier at ti norske sykehus stod på listen til den pro-russiske hacktivistgruppen Killnet, over mål å ramme (Kristensen et al., 2023). Ett av sykehusene på denne topplisten var Akershus Universitetssykehus (Ahus).

Ahus ønsker på dette tidspunktet å styrke sikkerhetskulturen på sykehuset og stiller derfor som oppdragsgiver for denne masteroppgaven. På bakgrunn av dagens trusselbilde, er det viktig at norske sykehus er forberedt på å bli utsatt for potensielle cyberangrep (Direktoratet for eHelse, 2020). Politiets Sikkerhetstjeneste (2023) opplyser imidlertid at enkle grep kan bidra å tette sårbarheter som stadig utnyttes for å gjennomføre suksessfulle angrep. Ahus har derfor et ønske om å øke kunnskaper om hvordan helsepersonell ved sykehuset kan bli bedre rustet til å motstå cyberangrep. Denne oppgaven skal derfor undersøke hva sykehuset trenger for å styrke sin sikkerhetskultur.

1.1 Nøkkelord

Cyberangrep, dataangrep, informasjonssikkerhet, sikkerhetskultur, pasientsikkerhet, sykehus, helsepersonell, opplæring og internundervisning.

1.2 Problemstilling

På bakgrunn av dagens risikobilde, viser forskning i fagmiljøet at det er nødvendig med et større fokus på informasjonssikkerhet i helsesektoren. Kompetanseheving er vesentlig for at helsepersonell skal kunne redusere sannsynligheten for at uønskede hendelser oppstår. Den største utfordringen kan relateres til at helsepersonell i spesialisthelsetjenesten ikke har tilstrekkelig kunnskaper for å mitigere potensielle angrep der menneskelige faktorer spiller en vesentlig rolle. I tillegg mangler de kunnskaper om hvordan brudd på informasjonssikkerhet kan påvirke deres daglige arbeid i møtet med pasienter og pårørende (Riksrevisjonen, 2021). Andre utfordringer kan relateres til at flere opplever økt arbeidsbelastning og stressnivå, samt tidspress og lite ressurser på arbeidsplassen (Rizzoni et al., 2022). Det resulterer i at det største fokuset rettes mot pasientsikkerhet, og at informasjonssikkerhet bortprioriteres. Når klinikere først har mulighet, prioriteres det å kontinuerlig gi opplæring i pasientsikkerhet der medisinske prosedyrer er i fokus. Utfordringen blir derfor at informasjonssikkerhet som fagfelt blir nedprioritert og at helsepersonell ikke får den opplæringen de trenger som følge av mangel på kapasitet (Conventry & Branley, 2018).

På bakgrunn av dette skal denne masteroppgaven undersøke om det er mulig å inkludere aspekter ved informasjonssikkerhet i opplæring av pasientsikkerhet for å øke frekvensen av opplæringen, samt rette fokuset mot informasjonssikkerhet. En

slik tilnærming vil kreve et tett samarbeid mellom strategisk, taktisk og operativt nivå i helseforetaket. På sykehuset er det ofte slik at rutiner og prosedyrer har vært etablert i mange år (O'Brien, Ghafur & Durkin, 2021). Målet med masteroppgaven er imidlertid å undersøke om et nytenkende opplæringskonsept kunne gjort det enklere å gi opplæring innen informasjonssikkerhet. Resultatet av rapporten skal bidra å legge føringer for om dette kan realiseres i praksis og eventuelt hvordan dette kan gjøres.

1.3 Begrunnelse, motivasjon og fordeler

Opplæring i informasjonssikkerhet og pasientsikkerhet gis i separate opplæringsprogram i dag. Hovedutfordringen er at opplæring i informasjonssikkerhet ikke tilbys like frekvent som i pasientsikkerhet. Ved å inkorporere informasjonssikkerhet og pasientsikkerhet i ett felles opplæringsforløp, kan helsepersonell muligens få jevnere opplæring, og dermed også øke kunnskaper i informasjonssikkerhet. Forsking viser fellestrekk mellom opplæring i digital sikkerhet og pasientsikkerhet da begge har til felles at de fokuserer på menneskelige faktorer og innovasjon (Flott et al., 2021). Fordelen ved å utforme et felles opplæringskonsept er også at helsepersonell potensielt blir bedre rustet til å detektere og forebygge fremtidige forsøk på cyberangrep. Dersom det viser seg at et slikt opplæringskonsept er gjennomførbart i praksis, kan denne kunnskapen også overføres til andre sykehus og helseforetak i både privat og offentlig sektor.

1.4 Forskningsspørsmål

Basert på introduksjonen og problembeskrivelsen, er målet å undersøke om det er mulig å innlemme informasjonssikkerhet i opplæring for pasientsikkerhet. Det store forskningsspørsmålet er derfor:

"*Hvilke forutsetninger bør oppfylles for at norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet?»*

Det første steget vil bli å undersøke om det anses å være mulig å gjennomføre i praksis, og deretter hva som potensielt trengs av Ahus som helseforetak for å legge til rette for en slik tilnærming. For å skape diskusjon og refleksjon, vil det utformes et opplæringskonsept som kan benyttes for å illustrere hvordan en slik opplæring kan se ut. Konseptet skal deretter formidles gjennom intervju for å innhente faglige perspektiver på anvendbarheten i praksis. Det å ha et konkret eksempel å forholde seg til, kan potensielt bidra til å øke forståelsen for nødvendigheten av tilnærmingen. I tillegg kan det bidra til å skape nye tankeprosesser som legger til rette for utprøvning. Forskningsspørsmålet skal besvares ved å gjennomføre en omfattende litteraturstudie der det innhentes eksisterende forskning på feltet. I tillegg vil det utføres intervjuer av nøkkelpersonell, samt en sosio-teknisk analyse

for å danne et grundigere beslutningsgrunnlag basert på en helhetlig vurdering av helseforetaket. Til slutt vil resultatet kunne si noe om hvilke sosio-tekniske faktorer som preger sikkerhetskulturen ved Ahus, og hva de kan arbeide med videre for å styrke sikkerhetskulturen i helseforetaket.

1.5 Planlagte bidrag

Denne masteroppgaven vil generere nye resultater ved å undersøke om en ny opplæringsmetode er anvendbar i praksis og hvilke forutsetninger som må til for å realisere et slikt arbeid. Formålet med konseptet er egentlig å effektivisere opplæringen som blir gitt i dag, men grunnet tidsrammene som er gitt for prosjektperioden, vil det ikke være mulig å teste effektiviteten. Før konseptet kan testes i praksis, er det nødvendig å samhandle med strategisk, taktisk og operative avdelinger for å kartlegge om det faktisk er gjennomførbart. Ved et positivt resultatet, kan verdien overføres til andre sektorer og bidra til en eventuell utprøving i praksis. Eksempelvis benytter kommunehelsetjenesten mer teknologi nå sammenlignet med tidligere. De har fokus på velferdsteknologi og smarthus som skal gjøre det enklere for eldre og andre syke å bo i hjemmene sine lenger fremfor å måtte innlegges på sykehus eller sykehjem (Hoffmann, 2013). I likhet med teknologien på sykehus, åpner også bruk av slik teknologi opp for at det kan oppstå cyberangrep der pasienter, helsepersonell og helseinstitusjoner blir rammet (Skjelvik & Yang, 2022). Resultatene av masteroppgaven kan dermed også bidra til å øke kunnskapene til annet helsepersonell som arbeider på andre sykehus, sykehjem, hjemmetjeneste, legekontorer og lignende, både i privat og offentlig sektor. Resultatene fra denne masteroppgaven kan bidra til å endre arbeidsmetodikk for å sikre hyppigere opplæring innen informasjonssikkerhet uavhengig hvilken type helseforetak en arbeider ved.

1.6 Avgrensninger

På et sykehus finnes det naturligvis mange systemer for å holde sykehusdriften i gang. Dette kan være alt fra systemer som brukes til direkte pasientbehandling og forskning til systemadmninistratorer, finansielle, sentralbord og regnskapsføring som holder oversikt over regnskap og forsikringer. I denne masteroppgaven begrenses omfanget til å omhandle systemer som håndteres av helsepersonell. Bakgrunn for det er at dette er yrkesgrupper som regnes å ha lite kunnskaper om informasjonssikkerhet da de fokuserer på pasientsikkerhet. Det betyr likevel ikke at det er mindre sannsynlighet for at andre sykehusavdelinger kan bli utsatt for angrep. På bakgrunn av at menneskelige faktorer også utnyttes under angrep, vil denne masteroppgaven hovedsakelig fokusere på hvordan helsepersonell kan få bedre opplæring i en hektisk arbeidshverdag.

1.7 Oppgavestruktur

I dette kapittelet presenteres strukturen for rapporten og innhold i de ulike kapitlene.

Kapittel 1 - Introduksjon
Det første kapittelet introduserer leseren til temaet og problemstillingen som ligger til grunn for denne masteroppgaven. Forskningsspørsmålet presenteres, og det blir redegjort for hvordan denne oppgaven kan bidra til det eksisterende kunnskapsfeltet. Ved å utforske dette emnet, søker oppgaven å fylle et gap i forskningen og å bidra med ny innsikt og perspektiver.

Kapittel 2 - Bakgrunn og teori
I denne delen av oppgaven gis det en innføring i relevant bakgrunnslitteratur som er nødvendig for å forstå og analysere temaet i denne masteroppgaven. Gjennom å belyse en grundig gjennomgang av eksisterende teori, definisjoner og forklaringer, etableres det et solid fundament som vil støtte oppgavens videre analyser og funn.

Kapittel 3 - Metode
Metodikken som er brukt for gjennomføringen av denne oppgaven blir presentert i dette kapittelet. Metode for litteratursøk og datainnsamling blir nøye beskrevet, inkludert de valgte forskningsmetoder og innsamlingsprosedyrer. Dette kapittelet gir også et innblikk i hvordan oppgaven har håndtert forskningsetiske hensyn.

Kapittel 4 - Eksisterende arbeid
Resultatene fra litteratursøket blir nøye presentert og fremlegger nasjonale og internasjonale perspektiv på problemstillingen. Dette kapittelet benyttes for å innhente resultater som kan sammenlignes mot resultatet av casestudien.

Kapittel 5 - Presentasjon av nytt opplæringskonsept
Som en del av denne oppgaven vil det bli gitt en presentasjon av et nytt opplæringskonsept som er utviklet. Kapittel 5 tar sikte på konseptets fordeler og ulemper hvor de blir nøye vurdert og diskutert, og dets potensial for anvendelse innenfor det relevante feltet blir utforsket for fremtidig implementering.

Kapittel 6 - Resultat
Resultatene fra innsamlet data og den sosio-tekniske analysen blir presentert i dette kapittelet. Gjennom en systematisk gjennomgang og analyse av dataene, blir viktige funn og trender identifisert. De sosiale og teknologiske aspektene som påvirker fenomenet blir nøye undersøkt.

Kapittel 7 - Diskusjon
Kapittelet diskuterer og tolker funnene som er presentert i kapittel 6. Ved å sam-

menligne de resultatene med tidligere forskning, blir det utforsket ulike perspektiver og tolkninger. Diskusjonen tar sikte på å forklare funnene, avdekke eventuelle sammenhenger og utfordre eksisterende kunnskap på området.

Kapittel 8 - Konklusjon og videre arbeid
I det følgende oppsummeres hovedfunnene og diskusjonen fra tidligere kapitler. Kapittelet avsluttes med å belyse mulighetene for videre arbeid.

Kapittel 2

Bakgrunn og teori

Dette kapittelet presenterer grunnleggende teori masteroppgaven bygger på og gir leseren et innblikk i relevante bakgrunnskunnskaper.

2.1 Begrepsforståelse

Det første delkapittelet gir innføring i sentrale begreper som blir brukt gjennom hele rapporten.

2.1.1 Cyberangrep

Et cyberangrep er en ondsinnet aktivitet som gjennomføres i det digitale domenet, der en trusselaktør anvender ressurser i datanettverket i forsøk på å samle inn, forstyrre, nekte eller ødelegge informasjonssystemressurser eller selve informasjonen som aksesseres (NIST, 2023). Cyberangrepene har endret seg betraktelig de siste tiårene. På 60-tallet var hacking ofte assosiert med ansatte i virksomheter som testet systemene sine med et mål om å forbedre eksisterende systemer i henhold til effektivisering. Særlig etter 80-tallet da datamaskiner også kunne kjøpes av privatpersoner, ble det enklere for trusselaktører å gjennomføre cyberangrep. Da var det ikke lenger et fokus på å kun forbedre systemer, men også på personlig gevinst. Dette kunne være alt fra å piratkopiere programvarer, utvikle skadevare og aksessere informasjonssystemer for å stjele data. På 2000-tallet ble det særlig interesse for å ramme sikkerhetssystemene til de statlige organisasjonenene i landet. Fra den tid og til i dag har Internett stadig blitt en stor del av hverdagen til mange. Det benyttes avanserte metoder for å gjennomføre sofistikerte angrep (Kaspersky, 2023). I dag bryter ofte trusselaktørene seg inn datasystemene for å stjele verdifull informasjon, modifisere innhold eller å generelt ødelegge informasjonen. Handlingene utføres som regel ved å installere skadevare uten at brukeren av systemet er bevisst over det, slik at trusselaktøren selv får kontroll over systemet som er rammet. Hensikten med disse angrepene kan være alt fra å spre frykt i samfunnet, økonomisk vinning, ta hevn, for nysgjerrighetens skyld eller for politiske interesser (Martinsen, 2023).

2.1.2 Informasjonssikkerhet

Begrepet informasjonssikkerhet utgjøres av de tre grunnpilarene i CIA-triaden; konfidensialitet, integritet og tilgjengelighet (Whitman & Mattford., 2017). På sykehuset betyr konfidensialitet at helsedata ikke skal aksesseres av uautoriserte aktører, og at helsepersonell skal overholde taushetsplikten sin for å hindre spredning av pasientinformasjon. Innenfor konfidensialitet er det også et fokus å ivareta personvern for at innbyggerne skal ha tillitt til sykehuset. Integritet omfatter at pasientdata som er lagret i sykehuset sine informasjonssystemer skal være av korrekt opphav slik at helsepersonell kan gi nødvendig helsehjelp. Modifisering av viktig pasientinformasjon kan føre til at pasienten får feil behandling og i verste fall føre til livstruende situasjoner. Tilgjengelighet omhandler at informasjon alltid er tilgjengelig når helsepersonell har behov for å utøve profesjonsrelaterte arbeidsoppgaver. Dette er svært vesentlig for at helsepersonell skal kunne lese og dokumentere nødvendig informasjon om pasientene. Informasjonssikkerhetsbegrepet omfatter også at all informasjon skal lagres på en forsvarlig måte og ikke deles med personer som ikke har et behandlingsansvar for pasienten (Direktoratet for eHelse, 2022; Riksrevisjonen, 2021).

2.1.3 Pasientsikkerhet

Primært brukes begrepet pasient om personer som tilbys og mottar hjelp fra helsetjenesten, eller en person som selv kontakter helsevesenet med en forespørsel om helsehjelp (Helsedirektoratet, 2018). Med pasientsikkerhet menes det at et hvert helseforetak skal tilby helsetjenester av god kvalitet slik at de kan forhindre, forebygge og begrense uønskede konsekvenser, eller skader som følge av svakheter i helsesystemene (Frich, 2011). Innenfor pasientsikkerhet er det svært essensielt at pasienter ikke utsettes for unødig skade som følge av helsetjenestenes prosesser (Itryggehender, 2021). I tillegg til å følge medisinske prosedyrer, inkluderer også pasientsikkerhet at digitale systemer og strukturer i organisasjonen ivaretas slik at alle pasienter får nødvendig helsehjelp (Frich, 2011).

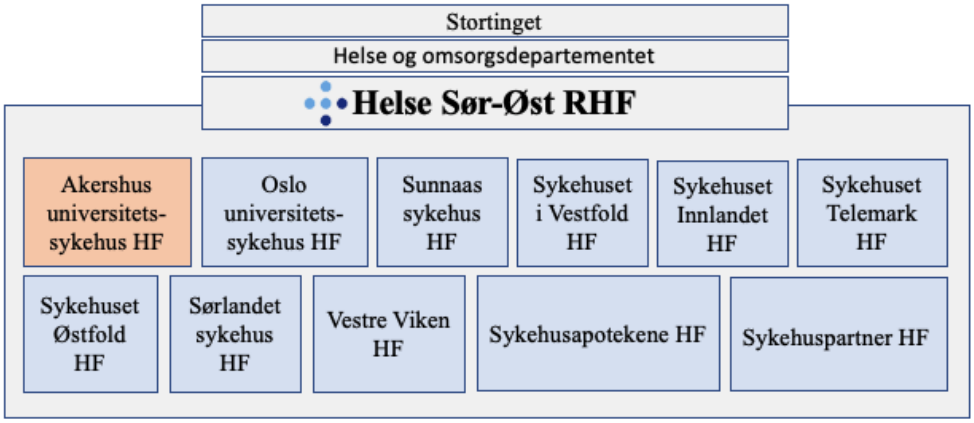
2.1.4 Samspillet mellom informasjonssikkerhet og pasientsikkerhet

I helseforetakene har det fra tidligere vært en kultur der det skilles mellom pasientsikkerhet og informasjonssikkerhet. Tanken har vært at informasjonssikkerhet er et teknisk problem som håndteres av IT-personell, mens pasientsikkerhet ivaretas av helsepersonell som leger og sykepleiere. Det er imidlertid vesentlig å påpeke at informasjonssikkerhet ikke bare er et teknisk problem, men en utfordring som alle nivåene i helseforetaket har ansvar for. Det betyr at alle sykehusansatte inkludert helsepersonell må spille på et lag for å bekjempe brudd på informasjonssikkerhet (O'Brien, Ghafur & Durkin, 2021; Chua, 2021). Internasjonale forskere påpeker faktisk at cybersikkerhet er pasientsikkerhet. Dette utsagnet henger sammen med at brudd på informasjonssikkerhet direkte kan gi store konsekvenser og skader for pasienter som følge av at helsepersonell ikke har muligheten til å gi nødven-

dig helsehjelp (Warner, 2022). Eksempelvis kan pasienter settes i en livstruende situasjon som følge av at helsepersonell ikke har tilgang til systemer som danner behandlingsgrunnlag. Ringvirkninger av dette kan være at det skapes store forsinkelser der timeavtaler, behandlinger og operasjoner avlyses eller ikke kan gjennomføres som normalt. Dette medfører at pasienter må vente og eventuelt overføres til nærliggende sykehus for å få behandling i tide. På universitetssykehuset i Düsseldorf i Tyskland i 2020, ble det for første gang rapportert at en kvinne mistet livet som følge et cyberangrep. Pasienten hadde en livstruende tilstand som gjorde at hun umiddelbart måtte transporteres til det nærmeste sykehuset for behandling. Siden sykehuset hun skulle overføres til var 20 mil unna, stod ikke livet til å reddes under transport (O'Brien, Ghafur & Durkin, 2021). Helsetjenesten bygger på prinsippet om rett behandling, på rett sted til rett tid (Meld. st. 47, 2009).

For å imøtekomme dette, kan ikke informasjonssikkerhet bli sett på som et sekundært problem. Det må integreres i alle ledd av av helsetjenesten (Warner, 2022). O'Brien, Ghafur & Durkin (2021) hevder likevel at det er mange som ser på informasjonssikkerhet som noe abstrakt fordi at brudd på informasjonssikkerhet ikke nødvendigvis skader pasienten eller medfører umiddelbar død. Likevel påpeker de at det kan oppstå ringvirkninger som kan påvirke pasientens helsmessige, sosiale og økonomiske forhold. Det at pasientdata eksempelvis kommer på avveie kan også føre til at innbyggerne får mindre tillitt til helsepersonell og helseforetakene. På bakgrunn av det er det essensielt å se på informasjonssikkerhet og pasientsikkerhet i sammenheng, fremfor to isolerte fagfelt.

2.2 Helse Sør-Øst



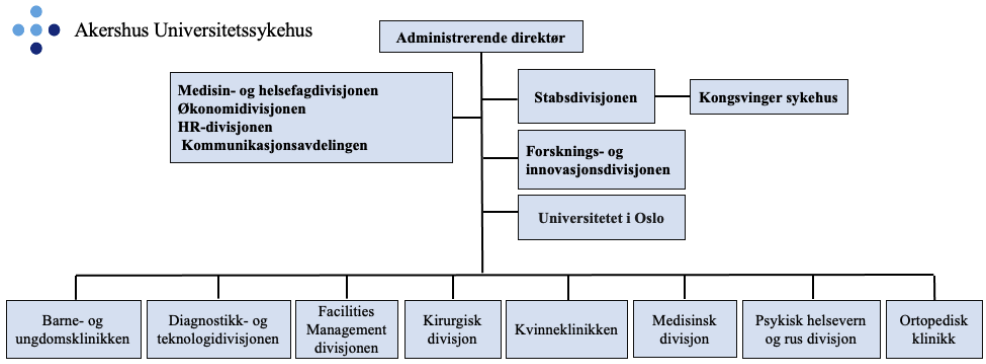
Figur 2.1: Oversikt over helseforetakene Helse Sør-Øst består av (Helse Sør-Øst, 2022).

Helse Sør-Øst ble etablert i 2007, og er et regionalt helseforetak som er statlig eid av Helse og omsorgsdepartementet. Som figur 2.1 viser, består Helse Sør-Øst av totalt 11 lokale helseforetak som til sammen tilbyr spesialisthelsetjenester til 3,1 millioner mennesker i Oslo, Vestfold, Telemark, Innlandet, Viken og Agder. Sammenlagt består sykehusene av 81.000 medarbeidere som hver dag arbeider med å tilby forsvarlige helsetjenester. Ahus er et lokalsykehus som eies av Helse Sør-Øst (Helse Sør-Øst, 2023).

Ansvaret for informasjonssikkerheten i Helse Sør-Øst fordeler seg på de ulike nivåene i helseforetaket. Helse– og omsorgsdepartementet har et overordnet ansvar for å utvikle nasjonale strategier for alle sykehus. Helse Sør-øst har videre ansvar for å iverksette tiltak som imøtekommer krav fra øvre hold. De har også ansvaret for å utvikle ytterligere og mer spesifikke strategier for alle sine helseregioner. Sykehuspartner er den regionale IKT-leverandøren til Helse Sør-Øst. De har ansvar for at den tekniske sikringen av regionale datautstyr og digitale systemer ivaretas. Hvert helseforetak er selv ansvarlig for å ivareta informasjonssikkerhet i sin virksomhet, og etablering av sikkerhetskultur slik at både systemer og utstyr brukes på en sikker måte (Helse Sør-Øst, 2023; Sykehuspartner, 2022).

2.2.1 Akershus Universitetssykehus HF

Ahus er et lokal- og områdesykehus eid av Helse Sør-Øst RHF. Sykehuset skal dekke et tjenestetilbud for om lag 594 000 innbyggere i Follo, Romerike, Kongsvinger, Alna, Grorud og Stovner. Hovedfokuset ligger på pasientbehandling, forskning, undervisning og pasientopplæring (Akershus Universitetssykehus, 2023a). Organisasjonskartet nedenfor viser hvordan Ahus er strukturert i ulike divisjoner.



Figur 2.2: Ahus sitt organisasjonskart (Akershus Universitetssykehus, 2023b).

Ahus består totalt av 12 000 ansatte som hver dag arbeider for å levere helsetilbud innenfor medisin, psykisk helsevern og rusbehandling. Som organisasjonskartet viser, er administrerende direktør foretakets øverste ledelse (Akershus Universitetssykehus, 2022b). Under vedkommende er sykehusledelsen og stabsdivisjonen

som arbeider med hvilke tjenestetilbud som skal gis til pasienter, opplæring til helsepersonell og rådgivning til kliniske avdelinger. Forsknings- og innovasjonsdivisjonen arbeider med forskning av ulike sykdommer som rammer pasienter (Akershus Universitetssykehus, 2022a). Siden Ahus er et universitetssykehus, har de et tett samarbeid med Universitetet i Oslo der studenter får muligheten til praktiske studier og erfaring (Akershus Universitetssykehus, 2023a). Organisasjonskartet viser også de kliniske divisjonene helseforetaket består av. Hver av de kliniske divisjonene styres av egne direktører. En divisjon består også av flere avdelinger, som igjen styres av avdelingsledere (Akershus Universitetssykehus, 2023b). Innenfor disse avdelingene arbeider helsepersonell som leger, sykepleiere, helsefagarbeidere, radiografer, bioingeniører, ernæringsfysiologer, fysioterapeuter, ergoterapeuter og lignende. I neste kapittel presenteres hvilke sensitive dataer de kan ha tilgang til.

2.3 Verdifull pasientdata

Figur 2.3: Digitale helsesystemer (Sykehuspartner, 2022)

En del av kjernevirksomheten på sykehuset består av kritiske datasystemer som skal bidra å effektivisere og forbedre pasientbehandlingen. Disse systemene består av store mengder pasientdata som både lagres og transporteres mellom intern og ekstern infrastruktur. Helseopplysninger og annen informasjon som kan si noe om pasientens helsetilstand regnes å være sensitive opplysninger. Dette kan inkludere

alt fra både fysisk og psykisk helse som gir informasjon om diagnoser, helseplager og pågående eller tidligere mottatt behandling fra helsevesenet (SIKT, 2023; Datatilsynet, 2019). Slik informasjon kan gjøre pasienter sårbare på grunn av livssituasjonen de befinner seg i, og informasjonen skal derfor beskyttes (Direktoratet for eHelse, 2023a). Helsepersonell har aksess til store mengder sensitive helseopplysninger tilhørende pasienter ved Ahus.

Figur 2.3 illustrerer kategorier av helsesystemer som hver eneste dag benyttes for å levere et helhetlig tjenestetilbud (Sykehuspartner, 2022). Disse sykehussystemene består av alt fra pasientjournaler, monitorering, bildediagnostikk, prøvetaking, medikamenthåndtering og kommunikasjonssystemer. Til tross for at helsepersonell har tilgang til disse systemene, stilles det strenge krav til hva de har rett til å aksessere av data. Pasientjournalforskriften (2021) belyser hvordan helseopplysninger skal behandles for å yte helsehjelp av god kvalitet, samt sikre at personvern og pasientsikkerheten ivaretas. Helsepersonelloven (2021) vektlegger også viktigheten av ivaretakelse av taushetsplikt for at innbyggerne skal opprettholde tilliten til helseforetaket. Det skal være trygt for pasienter å samhandle med spesialisthelsetjenesten, og de skal ikke unngå å oppsøke hjelp i frykt for å dele sensitive helseopplysninger. Til tross for at helsepersonell har innsyn i pasientjournaler, er det forbudt å lese eller søke etter pasientinformasjon uten behandlingsgrunnlag.

2.4 Attraktivt mål for cyberangrep

Sykehussystemene er attraktive mål for cyberangrep da de inneholder store mengder sensitive dataer. Forskning viser at pasientdata er verdt mer enn kredittkortdetaljer på Dark Web (Branley-Bell et al., 2021). Det kan henge sammen med at trusselaktører kan benytte denne informasjonen til å gjennomføre en rekke kriminelle handlinger i andres navn. Ved å ha tilgang til fødsels– og personnummer, demografisk data og helsedata, kan kriminelle tilegne økonomiske gevinster der de via identitetstyveri. Eksempelvis kan de søke lån i offerets navn, sende falske skattemeldinger for å få skatterefusjon, dyre medisinske behandlinger og tilegne forsikringsgoder. Hvis de får tak i kredittkortdetaljer, kan banken raskt detektere svindel og dermed blokkere kortet, men misbruk av helsedata er mye vanskeligere å detektere da det kan brukes på så mange forskjellige måter før det blir detektert. Innen den tid har ofte også de kriminelle hatt mer økonomisk vinning sammenlignet med det de ville fått ved bruk av kredittkort. Ved å målrettet angripe sykehusssystemene og stjele slik informasjon, kan kriminelle selge dette videre til andre kriminelle på Dark Web uten en stor risiko for å bli oppdaget (Alder, 2022; Finklea, 2017). Chinthapalli (2017) legger også til at prisen for en pasientjournal er $10 og at dette tilsvarer 10 ganger mer sammenlignet med det å selge kredittkortdetaljer. Med andre ord, kan trusselaktører tjene mye dersom de evner å stjele pasientjournaler.

Det som gjør det motiverende for trusselaktører å angripe sykehussystemer, er at

de for det første vet at sykehusene ikke investerer i de største og beste sikkerhetsteknologiene (Conventry et al., 2020). Dette kan være ugunstig da datanettverket består av mange tekniske klienter som sender informasjon mellom ulike nettverkskomponenter. Sårbarheter i disse sytemene åpner opp for at de kan bli utsatt for en rekke angrep og at sikkerhetsbarrieren ikke fungerer som ønsket (Witts, 2023; Branley-Bell et al., 2021). For det andre, er det kjent at pasientjournaler er et enkelt mål for dataangrep da helsepersonell fokuserer på pasientbehandling fremfor å sikre informasjon og teknologi (Khiralla, 2020). I tillegg er det kjent at helsepersonell er en yrkesgruppe som er overarbeidet, utbrent og har et høyt stressnivå i arbeidshverdagen. Dette kan være medvirkende psykososiale faktorer som kan medføre at det oppstår menneskelige feil i arbeidet med informasjonssikkerhet (Conventry et al., 2020). Det vil si at det er en risiko for at det oppstår avvik som følge av uvitenhet, stress, tidsbegrensninger, og lignende (Branley-Bell et al., 2021). Slike forhold sammen med lite kunnskaper om informasjonssikkerhet utnyttes av angripere (Warner, 2022).

2.5 Cyberangrep rettet mot sykehus

Det finnes mange ulike type cyberangrep et sykehus kan bli utsatt for, der det enten utnyttes tekniske eller menneskelige sårbarheter. I denne masteroppgaven fokuseres det imidlertid på angrep som utnytter menneskelige faktorer hos helsepersonell som et steg for å angripe. Det er særlig to kjente og alvorlige dataangrep som rettes mot helsetjenesten; *phishing* og *løspengevirus* (Yeng, Fauzi & Nimbe, 2022; Chinthapalli, 2017; Spence et al., 2017).

Phishing er en form for sosial manipulering der en trusselaktør utgir seg for å være en annen person over en kommunikasjonskanal, eksempelvis e-post. I denne e-posten skjuler det seg også en fil eller lenke som inneholder skadevare som kan lastes ned av brukeren, og navigere vedkommende til et tredjepartssystem for å uthente konfidensiell informasjon. Phishingangrep bruker primært to ulike teknikker, ofte i kombinasjon. Det første som skjer, er at trusselaktøren utvikler en falsk nettside som samler inn sensitiv informasjon om feks brukernavn og passord, og deretter manipulerer en lenken som peker til denne nettsiden. Denne lenken legges ved i e-posten i håp om at offeret skal klikke på den. Dersom vedkommende klikker på den, og samtidig legger igjen brukernavn og passord, eller kortinformasjon, kan trusselaktøren fange opp dette og dermed bruke denne påloggingsinformasjonen i det respektive systemet det tilhører (Whitman & Mattford., 2017). Lenken de lager utvikler de ved hjelp av sofistikerte verktøy som ligner legitime lenker. De bruker også avanserte metoder for å utforme falske e-poster. Dette gjør det ekstremt vanskelig for helsepersonell å oppdage de uten å få opplæring (Rizzoni et al., 2022). Når de skal konstruere den falske e-posten bruker de teknikker innen sosial manipulering. De innhenter informasjon fra åpne kilder og utgir seg for å være en person den ansatte har tillitt til slik at e-posten virker legitim. For å hindre slike angrep benyttes sikkerhetsmekanismer i brannmuren for

å filtrere falske e-poster slik at de ikke havner i inboksen til helsepersonell. Disse systemene påstår at de klarer å filtrere store mengder av disse e-postene. Siden trusselaktører er kjent med dette, har de også utviklet enda mer avanserte metoder som gjør at de klarer å komme seg forbi sikkerhetsbarrierene (Khiralla, 2020). Sykehuspartner opplyser at Ahus daglig blir utsatt for forsøk på cyberangrep. De har dekteksjonsverktøy som kan bidra å avdekke om angripere forsøker å tilegne uautorisert aksess til sykehussystemer, svindle ansatte eller stjele pasientjournaler (Vinningland, 2023). Det sees likevel at en mindre andel e-poster faktisk når frem til brukeren, og det er her de menneskelige faktorene spiller inn for om angrepet blir en suksess eller ikke (Rizzoni et al., 2022).

Løspengevirus er et annet angrep som ofte rammer sykehuset. Løspengevirus er en programvare som inneholder ondsinnet kode, og som er utviklet for å kryptere informasjon i offerets system. I helsesektoren kan dette eksempelvis være pasientjournalen. Når systemet er kryptert, vil ikke helsepersonell lenger ha tilgang til systemene sine da de blir låst ute(Whitman & Mattford., 2017). Det betyr at sykehuset må iverksette manuelle prosedyrer for å opprettholde sykehusdriften. Angriperen på sin side ønsker gjerne en stor pengesum for å overlevere dekrypteringsnøkkelen som skal låse systemet opp igjen slik at normal drift kan gjenopprettes (Conventry et al., 2020). Chernyshev Zeadallt & Baig (2019) legger til at begge angrepsmetodene ofte benyttes i kombinasjon for å ramme systemer da phishingangrep regnes å være den mest populære teknikken som benyttes for sosial manipulering for å nå ansatte, mens løspengevirus er den skadevaren som er mest brukt for å ramme kritiske systemer da det er enkelt og tar lite tid å gjennomføre angrepet (Cohen, 2021). Når metodene anvendes i kombinasjon, sendes det ofte en forfalsket phishing e-post med en skadelig lenke som inneholder løspengevirus. Når lenken klikkes på, lastes skadevaren automatisk ned og direkte ned på offerets klient, og aktiveres slik at målsystemene låses (Paloalto networks, 2023).

Forskning viser at helsepersonell har en høyere risiko for å klikke på skadelige lenker eller overse sikkerhetsmekanismer som følge av at de har en hektisk arbeidshverdag. Det viser seg også at ansatte som klikker på slike lenker ofte er årsaken til hvorfor løspengevirusangrep er suksessfulle i helsevesenet (Yeng, Fauzi & Nimbe, 2022). I tillegg er spesialisthelsetjenesten særlig utsatt da trusselaktører vet at sykehusledelsen er mer villig til å betale store summer for å gjenopprette pasientdata sammenlignet med andre organisasjonser (Chinthapalli, 2017; Yeng, Fauzi & Nimbe, 2022). I 2020 bestod om lag 50 prosent av alle dataangrep av løspengevirus (Cohen, 2021).

Det finnes en rekke eksempler på at helsepersonell har klikket på skadelige lenker i e-poster som har inneholdt løspengevirus. Dette avsnittet presenterer noen av dem. I 2013 fikk en ansatt tilsendt en phishing e-post med en lenke til et dokument som senderen mente måtte evalueres. Da offeret åpnet lenken trigget dette

nedlastning av skadevare som ga angriperen tilgang til 90 000 pasientjournaler (The Hipaa Guide, 2023). I 2016 ble Hollywood Presbyteruan Medical Center i USA utsatt for dette angrepet da en ansatt klikket på en skadelig lenke til et Word dokument. Løspengeviruset som ble aktivert het Locky og låste helsesystemene i en uke. Det påvirket alt fra pasientjournaler, til blodprøveresultater, bildediagnostiske undersøkelser og lignende Helsepersonell hadde derfor ikke mulighet til å gi nødvendig helsehjelp. Det endte opp med at sykehusledelsen betalte $17,000 US dollar for å få tilbake systemet. I 2022 måtte tre amerikanske sykehus under Memorial Health Systen avlyse operasjoner og sende pasienter til nærliggende sykehus med ambulanser som følge av Løspengevirus. Også pasienter som hadde behov for øyeblikkelig hjelp måtte fraktes da helsepersonellet ikke hadde tilgang til de digitale helsesystemene (Oftebro, 2021). Disse cyberangrepene viser hvordan brudd på informasjonssikkerheten kan påvirke pasientsikkerheten og hvilke alvorlige konsekvenser som kan oppstå som følge av menneskelige feil. På bakgrunn av den raske teknologiske utviklingen, er det ikke mulig for sykehuset å beskytte seg mot alle potensielle angrep rettet mot helseforetakets infrastruktur. Det Ahus imidlertid kan gjøre, er å styrke sikkerhetbarrieren for å gjøre det mer teknisk utfordrende for trusselaktørene å bryte barrierene (Riksrevisjonen, 2021).

2.6 Sikkerhetskultur

For å sikre at helsepersonell blir godt rustet til å oppdage og forebygge cyberrelaterte trusler, er det essensielt at Ahus har et fokus på sikkerhetsstyring. Det vil si at de systematisk må identifisere, og kontinuerlig legge til rette for aktiviteter som er nødvendige for at helsepersonell skal kunne læres opp i informasjonssikkerhet (NSM, 2023b). I dette arbeidet er det essensielt å styrke sikkerhetskulturen på sykehuset. Nasjonale sikkerhetsmyndigheter (NSM, 2023c) definerer sikkerhetskultur som atferd knyttet til sikkerhet. Det vil si: *Summen av den ansattes kunnskap, motivasjon, holdninger og atferd som kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd*" (NSM, 2023c, avsnitt 1). Alle helseforetak har en sikkerhetskultur uavhengig om den er god eller dårlig, men det viktigste er at kompetansen kontinuerlig øker for å forberede seg på en eventuell hendelse.

Flere helseforetak i Norge har erkjent at de har svakheter i sikkerhetskulturen som gjør at de mangler risikoforståelse og bevissthet relatert til dataangrep. Dette er en menneskelig sårbarhet som enkelt kan utnyttes av aktører (Riksrevisjonen, 2021). En hektisk hverdag og lite fokus på informasjonssikkerhet kan gjøre det utfordrende å tilegne fagkunnskaper på området (Branley-Bell et al., 2021). Dette kan resultere i at helsepersonell ikke er bevisst over hvordan deres handlinger kan påvirke informasjonssikkerheten. Det er gjennomført nasjonale og internasjonale undersøkelser på dette fagområdet. Riksrevisjonen (2021) utforte en undersøkelse av de fire helseregionene i Norge; Helse Sør-Øst, Helse Midt-Norge, Helse Vest og Helse Nord for å kartlegge hvordan helseforetakene i regionen forebygger cyberangrep mot sine IKT-systemer. Conventry et al. (2020) utførte en tilsvarende

studie for helseforetak i Irland, Italia og Hellas. Det som er interessant, er at begge studiene blant annet viser at helsepersonell ofte utfører handlinger i arbeidet sitt som kan virke praktisk for dem, men upraktisk for sikkerheten. Eksempelvis unngikk ansatte å låse datamaskinen for å spare tid for å logge seg inn. Warner (2022) påpeker at dette gjøres av helsepersonell for å skape en god arbeidslyt, men at det igjen fører til at hvem som helst kan få tilgang til systemet. Riksrevisjonen (2021) legger til at datasystemene oppleves som tungvinte og at ansatte derfor lager egne snarveier for å gjøre ting når arbeidsdagen i tillegg er hektisk. I tillegg synes helsepersonell at det tar for lang tid å logge seg av og på systemene, og når de blir akutt tilkalt for bistand, er det lett å glemme å logge av. Videre viste studien til Conventry et al. (2020) at passordene de ansatte lagde for ulike systemer var svake og ble brukt på flere systemer, samt skrevet ned da de synes det var vanskelig å huske de. Riksrevisjonen (2021) belyste i tillegg at ansatte ikke vet hvordan de lager sterke passord. I begge studiene viste det seg også at de ikke evnet å identifisere falske e-poster. I phishingsimuleringen til Riksrevisjonen (2021), viste det seg at av totalt 2300 e-poster som ble sent, var det 893 personer (39%) som klikket på den falske lenken, 565 (25%) som ga opplysninger og 277 (12%) som faktisk lastet ned en fil, sammenlagt for alle sykehusene. Til tross for at sykehusene i studien til Conventry et al. (2020) fraråder ansatte å klikke på lenker, gjør de det fordi de mener pasienter, pårørende og kollegaer sender vedlegg. Andre utfordringer var at ansatte bruker private USB-enheter som potensielt kan inneholde skadevare. Det er ikke alltid at sykehusets antivirus klarer å stoppe skadevaren fra å spre seg på sykehusnettet. Noen ansatte brukte også private enheter uten tillatelse til arbeidsoppgaver. Ved eventuell tyveri av datamaskiner, kan ikke sykehuset slette sensitive filer og en angriper vil få tilgang til de. I tillegg har sensitive dokumenter blitt liggende på fellesarealer som vaktrom og pauserom uten tilstrekkelig fysisk sikring. Riksrevisjonen (2021) belyser at mange ansatte ikke vet hvor de skal lagre sensitiv informasjon da de ikke vet forskjellen på fellesområder og lokalt område på egen datamaskin. Dette resulterer i at en lagrer dokumenter på feil lokasjon. Disse studiene viser at sikkerhetsatferden ikke er tilfredsstillende, og at dette er et globalt problem (Branley-Bell et al., 2021). På nasjonalt nivå vet en at sikkerhetsnivået blant de ulike helseforetakene noenlunde ligger det samme nivået (Riksrevisjonen, 2021). Slik atferd kan ses i mange helseforetak, og det er derfor det er viktig at sykehuset fokuserer på å etablere en god sikkerhetskultur slik at ansatte er klar over hvordan deres atferd kan påvirke informasjonssikkerheten (Branley-Bell et al., 2021).

Ved å etablere gode sikkerhetsrutiner og tilrettelegge for kontinuerlig opplæring kan en bidra å redusere sannsynligheten for at det oppstår uønskede hendelser som gir fatale konsekvenser for sykehusdriften. Opplæringen bør skje kontinuerlig over tid slik at den bidrar til å endre holdninger og sikkerhetsatferd. Det er først da en kan si at sikkerhetsarbeidet har vært vellykket. Sikkerhetskulturen bør resultere i at helsepersonell endrer sikkerhetsatferd og holdninger. Dette kan gjøres gjennom bevisstgjøring, etablerte prosedyrer og rutiner, skape engasjement og

kommunisere og diskutere hvordan sikkerhetsbrudd kan påvirke deres arbeid på sykehuset (Branley-Bell et al., 2021).

Kapittel 3

Metode

Gjennom masterprosjektet skal det samles inn informasjon som kan bidra å besvare forskningsspørsmålet. Informasjon vil hentes ut ved samtaler med nøkkelpersoner, litteratursøk og gjennom intervjuer. Dette kapittelet presenterer de ulike metodene som benyttes for datainnsamling, analyse og hvordan resultatene presenteres.

3.1 Møtevirksomhet med veileder og oppdragsgiver

Gjennom masterprosjektet vil det holdes jevnlige møter for å sikre progresjon og kvalitet i arbeidet som utføres. Stewart Kowalski er veileder for dette prosjektet. Han er professor ved NTNU, campus Gjøvik. Gjennom prosjektet vil det i starten holdes ukentlige møter for å diskutere faglige temaer knyttet til oppgaven, men også sikre at administrative søknadsprosesser blir gjort korrekt. Utover prosjektperioden, når arbeidet har startet, vil møtene arrangeres ved behov. I tillegg til dette, vil veilederen lese over utkast, og gi tilbakemeldinger på hva som kan forbedres.

Som nevnt tidligere, er det Ahus som er oppdragsgiveren for denne masteroppgaven. I den forbindelse fikk kandidaten to eksterne veiledere å forholde seg til. I starten var dette Kåre Magne Stennes og Espen Thorsen Frank. Det er primært førstenevnte som har hovedansvaret for oppfølgning, men begge vil kunne besvare henvendelser. Det avtales at all møtevirksomhet gjennomføres digitalt over Teams. I starten av prosjektet gjennomføres det møter hver andre uke og deretter ved behov.

3.2 Presentasjon av problemstilling

I starten av prosjektet gjennomfører kandidaten en digital presentasjon med introduksjon til temaet i masteroppgaven og hvilken problemstilling som skal undersøkes. Både intern og ekstern veileder er til stede under denne presentasjonen.

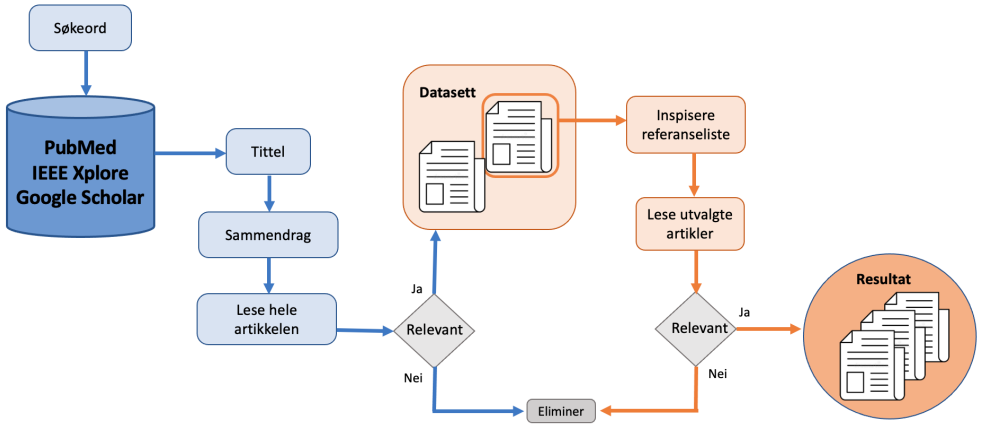
Hensikten er å skape en felles forståelse over hva som skal undersøkes og hvordan det skal utføres. Dette skal bidra til at oppdragsgiver også har mulighet til å komme med forslag til forbedringer. Etter at alle parter kommer til en felles enighet om hvordan de ulike undersøkelsene kan gjennomføres, starter datainnhentingen.

3.3 Metode for datainnsamling

En omfattende del av prosjektet innebærer å innhente materiale som publisert forskning og rapporter utgitt av nasjonale organer. Når det innhentes data for å løse problemstillingen, gjøres dette primært på to forskjellige måter. Det første er å gjennomføre litteratursøk for å identifisere eksisterende arbeid, og det andre er å innhente egne resultater gjennom ulike intervjuer.

3.3.1 Identifisere eksisterende arbeid

Det første som gjøres når problemstillingen er fastsatt, er å undersøke hva som finnes av eksisterende litteratur for den gitte problemstillingen. Målet er å innhente data om andre prosjekter som kan ha hatt tilsvarende forskningsfokus, for å identifisere deres resultater og vurderinger. Her vil det legges vekt på å søke etter rapporter utgitt av helseorganisasjoner. Formålet med å innhente disse rapportene er å kartlegge deres arbeid med informasjonssikkerhet og pasientsikkerhet.



Figur 3.1: Figuren viser prosessen for litteratursøket.

I det andre steget vil det gjennomføres en litteraturstudie for både nasjonale og internasjonale forskningsstudier. Hensikten med det er å bygge videre på erfaringer fra deres studier og identifisere relevant arbeid. Gjennom forprosjektet ble det avdekket at det ikke finnes nok forskning på feltet. For å øke kvaliteten på litteratursøket og samtidig øke sannsynligheten for positive funn, vil søkeprosessen utføres slik figur 3.1 viser. Første steg er å utvikle søkeord og deretter gjennomføre

strukturerte søk etter artikler i en litteraturdatabase. Litteraturen som blir identifisert gjennomgås, og dersom den er av relevanse vil den inkluderes i et datasett. Når det er gjort, vil snøballmetoden benyttes for å øke sannsynligheten for å finne en relevant artikkel. Denne metoden går ut på å undersøke referanselisten i en artikkel for å identifisere om det finnes nye artikler som kan gi mer informasjon om temaet (Wohlin, 2023). Fordelen ved å benytte en slik tilnærming er at en kan oppdage ytterligere litteratur når det ikke finnes så mye forskning på feltet enda. Siden en filtrerer artikler fra referanselisten til en artikel som anses å gi god informasjon, kan en anta å identifisere nye artikler. Det er likevel verdt å nevne at det finnes en risiko for at det oppstår skjevheter ettersom metoden innhenter anbefalinger fra andre kilder (Ghaljaie et al., 2017). Forskning viser likevel at opptil 51 prosent av referanser i en systematisk oversiktsartikkel er identifisert ved å gjennomføre snøballmetoden (Greenhalgh et al., 2023). Dette viser at metoden kan være anvendbar. De neste delkapitlene beskriver nærmere prosessen i litteratursøket og valgene som er tatt.

3.3.2 Metodiske valg for litteratursøk

Dette kapitlet belyser ulike metodiske valg som blir gjort for å gjennomføre litteratursøket.

Valg av litteraturdatabase

Det første steget er å velge relevante databaser som inneholder artikler som kan bidra å besvare problemstillingen. Det finnes mange ulike litteraturdatabaser med publiserte artikler av god kvalitet. Det må derfor tas et valg for hvilke databaser som skal inkluderes i studien. Valget gjøres basert på hvilke fagområder det skal søkes informasjon om, hvilke databaser som er brukt i tidligere fag og hvilke som anbefales i forskningsmiljøet på NTNU. Denne masteroppgaven vil hovedsakelig fokusere på temaer fra to ulike fagfelt; teknologi og helse. I den forbindelse er det vesentlig å finne databaser som inneholder litteratur fra disse fagfeltene.

Den første databasen som benyttes er *Google Scholar*. Denne databasen er utviklet av Google og er en type søkemotor som benyttes for å innhente akademisk litteratur innenfor alle mulige fagområder (NTNU, 2023a). Fordelen med å anvende denne databasen er at den også gir muligheten til å identifisere det som heter «Grå publikasjon», som er datamateriale som ikke har blitt publisert på tradisjonell måte (Cowan, 2023). Dette kan være fordelaktig med tanke på at det finnes lite forskning på fagfeltet som skal undersøkes. Det å starte i denne databasen kan bidra å identifisere informasjon som kanskje ellers ikke finnes i andre databaser. Siden søkemotoren også inneholder artikler og forskning som ikke har blitt publisert tradisjonelt, må en være kritisk når en vurderer påliteligheten til de ulike artiklene. For å sikre at artiklene som identifiseres er pålitelig og validert, er det svært essensielt å benytte academic liberary databaser i tillegg. Slike databaser inneholder publisert forskning av høyere kvalitet.

IEEE Xplore: Digital Liberary er en kjent database som inneholder et stort omfang av tekniske forskningsartikler, e-bøker og standarder. Litteraturen i denne databasen tilhører fagområder innen elektronikk og informatikk, og anses derfor å være svært relevant for litteratursøket. Fordelen ved å benytte denne databasen er at den også er benyttet i tidligere prosjekter, og er i tillegg anbefalt av NTNU når det søkes etter teknologisk forskning (NTNU, 2023b).

Siden en stor del av masteroppgaven består av en problemstilling knyttet til sykehus, er det svært relevant å gjennomføre tilleggssøk i en medisinsk database. Dette kan særlig være relevant for å avdekke forskning som har blitt utført innen informasjonssikkerhet. En svært anerkjent database med medisinsk forskning er PubMed. Den regnes å være den største databasen innen biomedisin og helsefaglig forskning, og anses derfor å være svært aktuell å benytte. PubMed er tilgjengelig for alle og NTNU har laget en egen brukerveiledning for hvordan en kan gjennomføre presise søk (NTNU, 2023c).

Tanken bak å benytte tre ulike databaser for å gjennomføre artikkelsøk er å øke sannsynligheten for å identifisere artikler som kan bidra å besvare problemstillingen. For å øke denne sannsynligheten ytterligere, er det essensielt å utvikle søkeord som kan bidra å identifisere relevante artikler. Neste delkapittel forklarer hvordan det er gjort.

Metode for å utvikle søkeord

Det andre steget i litteraturstudien er å utvikle søkeord som kan bidra å identifisere relevante artikler. Dersom en ikke gjør det, men heller velger å søke i fritekst bestående av tilfeldige ord kan en risikere å få mange irrelevante treff (NTNU, 2023c). Å finne riktige søkeord kan være avgjørende for hvilke resultater en sitter igjen etter litteraturstudiet. I den forbindelse er det ønskelig å anvende kjente verktøy som kan bidra å identifisere emneord i de valgte databasene. Som nevnt tidligere er det terminologi fra medisin og teknologi som er i fokus. For å finne relevante søkeord eller nøkkelord vil det brukes to tesaurus skreddersydd for de ulike databasene. En tesaurus er en liste bestående av kontrollert vokabulær med terminologi og emneord som brukes i de ulike litteraturdatabasene. Å bruke de skal gjøre det enklere og effektivt å gjennomføre presise søk (Erasmus University Library, 2023).

Når det skal velges tesaurus, gjøres det å på bakgrunn av valgte databaser. Det finnes en rekke oppslagsverk som kan benyttes, men for å effektivisere litteratursøkene, benyttes det vokabulær som er utviklet for de valgte databasene. Fordelen ved dette er at en vet at de respektive nøkkelordene er å finne i databasene. For å utvikle søkeord ved søk i IEEE Xplore, benyttes *The IEEE Thesaurus 2023*. Dette vokabulæret er basert på ANSI/NISO Z39.4-2021, som er en amerikansk nasjonal

standard utviklet av National Information Standards Organization (NISO, 2021). Vokabulæret består av om lag 11500 beskrivende ord innenfor ingeniørfag, teknologi og annen forsking, og er utviklet av fageksperter (IEEE, 2023). Ved å benytte søkeord fra denne listen kan derfor bidra å identifisere mer beskrivende materiale. En annen fordel ved dette vokabulæret er at det ikke kun inneholder tekniske nøkkelord, men også medisinske.

Siden PubMed også benyttes for artikkelsøk, er det vesentlig å finne tesaurus for denne databasen også. For medisinske og helsefaglige søkeord, anbefaler NTNU å benytte oppslagsverket MeSH. Dette verktøyet er utviklet av National Library of Medicine, og anses å være svært bra da det allerede er mye brukt i medisinske databaser som Medline og Pubmed (NTNU, 2023d). Selv om dette verktøyet anses å godt i seg selv, er en svakhet at den naturligvis ikke består av tekniske søkeord og teminologi. En annen ulempe med MeSH er at nyere artikler kan risikere å ikke bli funnet som følge av at de mangler MeSH ord (NTNU. 2023c). Dette kan være uheldig da potensiell relevant datamateriale ikke blir identifisert, og at dette kunne vært svært verdifult for å besvare problemstillingen. I slike situasjoner kan det være hensiktsmessig å teste søkeord fra det andre oppslagsverket.

I utgangspunktet kunne en tenkt at det hadde vært nok å benytte et oppslagsverk for å finne gode søkeord. Særlig IEEE kunne vært svært relevant å benytte da det både inneholder medisinsk og teknologisk terminologi. Hensikten med å benytte to ulike verktøy er at problemstillingen som skal undersøkes er svært ny og det er lite forskning på feltet. For å gjøre et mer omfattende litteratursøk, vil det derfor være essensielt å inkludere flere databaser for å øke sannsynligheten for å finne flere publiserte artikler.

På bakgrunn av at søkene gjennomføres i engelske litteraturdatabaser, er søkeordene på engelsk. Søkeordene under er hentet fra tesaurus som beskrevet og benyttes når det skal gjennomføres konkrete søk.

Søkeord uthentet fra tesaurus	
IEEE tesaurus 2023	**MeSH tesaurus**
Information Security	Patient safety
Cybersecurity	nservice Training
Awareness	Culture
Patient	Patient education
Training	Cybersecurity
Hospital	Educational model

Tabell 3.1: Oversikt over relevante søkeord som har blitt uthentet fra listene.

Bakgrunn for valg av disse søkeordene er at de inkluderer nøkkelord som de ønskede artiklene består av. Det vil brukes 'AND' operator for å kombinere medi-

sinske og tekniske søkeord for å finne de mest relevante artiklene som kan bidra å besvare problemstillingen. Resultatet av litteratursøket presenteres i kapittel 4.

Metode for å filtrere artikler

Når søkeordene er brukt for å søke, er det neste å filtrere hvilke artikler som skal undersøkes videre. Det gjøres ingen begrensninger i forhold til land som inkluderes. Fordelen ved å inkludere internasjonale resultater, er å potensielt lære av andre land som har erfaring innenfor problemstillingen. Videre ville det i tillegg vært relevant å filtrere artikler ytterligere basert på årstall for publisering. Fordelen ved dette er at teknologien og medisin utvikler seg raskt, noe som gjør at det hele tiden publiseres ny forskning. For å holde tritt med dagsaktuell informasjon er det hensiktsmessig å filtrere på årstall. I denne oppgaven derimot utforskes en problemstilling som ikke er så kjent, men som kanskje er kjent i andre land. Ved å lære av andre land, kan en i Norge uthente vurderinger og erfaringer andre har gjort seg i mange år. Ved å filtrere på antall år kan en risikere å gå glipp av viktig informasjon som potensielt har eksistert i andre land i en lenger periode. I mange tilfeller kan et søk gi resultater på flere sider, men det avgrenses at det er de tre første sidene som undersøkes i første omgang. Da leses overskriften og sammendraget dersom det er relevant. Dersom artikkelen er av interesse vil den gjennomleses nøyere. Fordelen ved å sette en avgrensning på tre sider, er at de aktuelle artiklene ofte dukker opp på de første sidene. Ulempen ved å gjøre dette er at en en risikerer å gå glipp av artikler som kunne vært nyttig. I slike tilfeller, dersom en på den tredje siden fortsatt ser at søket inneholder relevante artikler, kan de neste sidene også undersøkes videre. Hvis ikke, så avsluttes søket. Formålet er å være effektiv i søkeprosessen.

3.4 Metode for gjennomførelse av casestudie

Etter innhenting og vurdering av eksisterende litteratur, er det neste steget å utføre en casestudie av Ahus. I dette kapittelet presenteres hvordan casestudiet gjennomføres og hva som skal innhentes av informasjon. Videre belyses hvordan informasjon analyseres og presenteres.

3.4.1 Forskningsmetode

Som nevnt i introduksjonen, skal det undersøkes om det er mulig å inkludere informasjonssikkerhet i opplæring av pasientsikkerhet. Når det vurderes hvilken forskningsmetode som skal tas i bruk, er det vesentlig å vurdere hva en ønsker å samle inn av data. Til å starte med, vurderes det om det skal gjennomføre kvalitativ eller kvantitativ forskning. I utgangspunktet kunne en tilnærming vært å gjennomføre en kvantitativ spørreundersøkelse blant helsepersonell på Ahus. Dette kunne ha bidratt til å samle inn synspunkter de har for å inkludere informasjonssikkerhet i opplæring av pasientsikkerhet. Fordelen ved en slik tilnærming kunne

vært å sende ut et digitalt spørreskjema som helsepersonell kunne fylt ut etter sitt tidsskjema. En hadde ikke vært avhengig av å sette opp en tidsluke for gjennomføring av intervju og det hadde vært en større mulighet til å inkludere flere i studien. Et spørreskjema kunne også blitt sendt ut til en større andel informanter slik at datagrunnlaget hadde vært større. Ulempen med denne tilnærmingen kunne ha vært at det er vanskeligere for informantene å stille spørsmål dersom de ikke forstår budskapet. Siden mange av informantene regnes å ha helsefaglig bakgrunn, antas det at de ikke har nok kunnskaper om informasjonssikkerhet, noe som kan gjøre det vanskeligere å besvare spørsmålene som blir stilt. På den andre siden er problemstillingen et nytt tema, og en har ikke like mye kunnskaper om hvordan det kan gjennomføres i praksis. Derfor ville kvalitative intervjuer vært mer gunstig. I tillegg er det ønskelig å undersøke informantenes synsvinkler, refleksjoner og holdninger, ikke statistisk data og sammenhenger mellom variabler. Forskningsspørsmålet som skal undersøkes er også komplekst og innovativt, og det er derfor ønskelig å gjøre en dypdykk av fenomenet som skal undersøkes. I en kvantitativ studie derimot fokuseres det ofte på innhenting av numerisk data, men i dette masterprosjektet er målet å beskrive deltakernes perspektiver (Young, 1981). I den forbindelse anses det som mest hensiktsmessig å anvende en kvalitativ forskningsmetode fremfor kvantitativ.

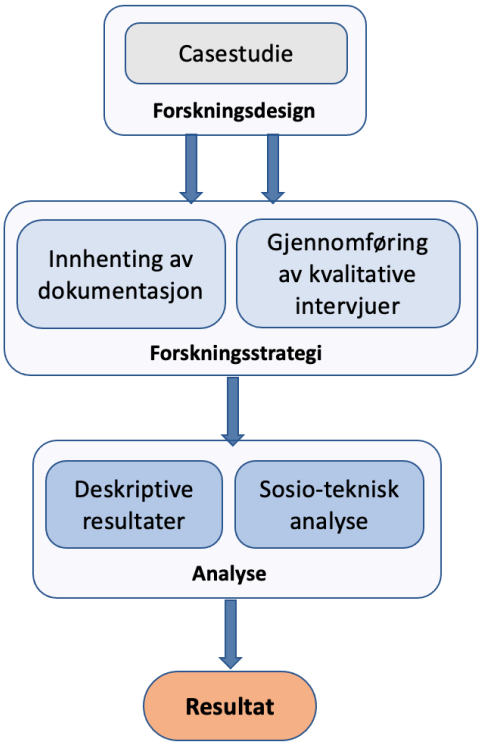
Innenfor kvalitative studier finnes det mange forskningsmetoder for å samle inn og analysere data. I denne masteroppgaven må forskningsmetoden vurderes ut i fra kriterier for hva som må tas i betraktning ved valg av metode. For det første skal et nytt fenomen undersøkes blant en spesifikk gruppe på sykehuset. Det skal gjennomføres dypere samtaler som kan bidra å besvare problemstillingen på flere nivåer i organisasjonen. I tillegg skal det vurderes om dagens praksis kan endres ved å innhente dokumentasjon om prosedyrer. Ut ifra disse tre betraktningene, er det særlig tre forskningsmetoder som vurderes hver for seg; casestudie, aksjonsforskning og kvalitative intervjuer (Swann, 2002; Young, 1981). Alle forskningsmetodene er kvalitative og kan på ulike måter benyttes. Problemstillingen som skal undersøkes er ikke knyttet til kun en kontekst, men mange ulike avdelinger og nivåer i organisasjonen. I den forbindelse anses det som aktuelt å vurdere casestudie, aksjonsforskning eller kvalitative intervjuer.

I en casestudie kan en foreta en grundig analyse av en organisasjon på en systematisk måte. Denne forskningsmetoden støtter analyse av datakilder som dokumentasjon og intervjuer, noe som anses å være svært aktuelt i denne masteroppgaven (Gerring, 2004). Aksjonsforskning på sin side har et stort fokus på å løse de praktiske problemene sammen med de som opplever problemene, der målet er å skape endring. Bruk av denne metoden skal også støtte innhenting av dokumentasjon og gjennomføring av intervjuer (McNiff, 2013).

Hovedforskjellen på disse forskningsmetodene er at i aksjonsforskning fokuseres det på et konkret samarbeid mellom forsker og praktikere for å skape en forbed-

ring i praksis på kortere sikt, men i en casestudie prøver en å forstå og beskrive en problemstilling uten å nødvendigvis skape en endring i praksis så raskt. I realiteten kan både aksjonsforskning og casestudie designes i samme forskningsprosess, eksempelvis slik at casestudie brukes for å innhente datagrunnlag fra Ahus, og deretter benytte disse dataene til å skape endring i praksis ved å gjennomføre aksjonsforskning. Det hadde vært en mulighet, men på bakgrunn av oppgavens art og tidsrammen for prosjektet, er det mest foretrukket å gjennomføre en casestudie. Det er fordi at det i førsteomgang er et mål å finne ut av om hvilke tanker personell på Ahus har om det å innføre et nytt opplæringskonsept, ikke nødvendigvis at det skal skje endringer med en gang. Det betyr likevel ikke at denne masteroppgaven ikke vil bidra til endringer i praksis. I fremtiden, eksempelvis i videre arbeid kan det gjennomføres et aksjonsforskning for å arbeide videre med denne problemstillingen da dette er en omfattende prosess i seg selv. På bagrunn av vurderingene som er gjort, vil forskningsmetoden bestå av en hybrid av casestudie og kvalitative intervjuer. Hvordan forskningsstudien er designet presenteres i neste kapittel.

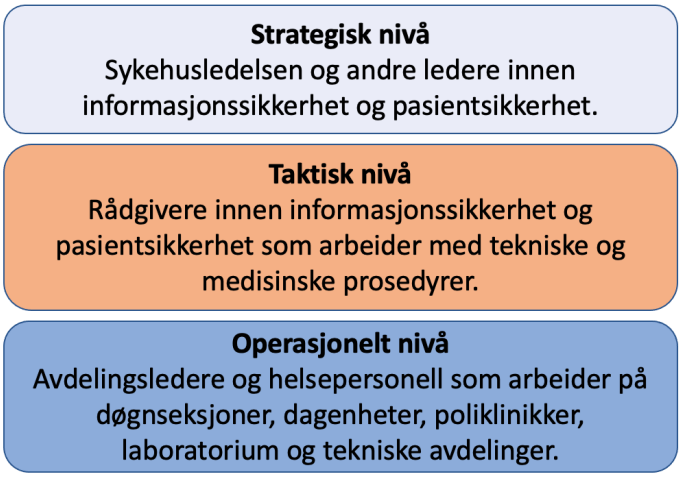
Design av casestudie



Figur 3.2: Illustrasjon av forskningsprosessen.

For å samle inn informasjon som kan bidra å besvare problemstillingen på en systematisk måte, er det svært essensielt å designe fremgansmetoden i casestudien. Som nevnt i introduksjonen, er problemstillingen:
"*Hvilke forutsetninger bør oppfylles for at norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet?»*

For å besvare dette velges først og fremst caset i fokus. I denne masteroppgaven er det Ahus som organisasjon som er i fokus. Fordelen ved det er at de fleste sykehusene i Norge ligger cirka på det samme sikkerhetsnivå i ifølge Riksrevisjonen (2021). Det betyr at ved å sette Ahus som organisasjon i caset, kan en anta at en kanskje ville få tilsvarende resultater ved gjennomføring av casestudie på et annet sykehus i nærheten. Ahus som organisasjon består av ulike nivåer. Dette kan ses på som strategisk, taktisk og operasjonelt nivå slik denne figuren viser (Riksrevisjonen, 2021).



Figur 3.3: De tre organisasjonsnivåene på Ahus.

Sett i lys av informasjonssikkerhetledelse vil en på strategisk nivå fokusere på langsiktig planlegging for opplæring av informasjonssikkerhet. Disse personene er de som utvikler strategier, tar større beslutninger for sykehuset og består gjerne av sykehusledelsen. På taktisk nivå arbeider ansatte som etablerer delplaner og handlingsplaner basert på strategiene. Organisasjonsnivået består også av personell som utvikler prosedyrer og rutiner innenfor informasjonssikkerhet og pasientsikkerhet. De som arbeider på operativt nivå, er gjerne de som har ansvar for daglige aktiviteter (White, 2009). På et sykehus vil dette være helsepersonell som arbeider i avdelingene. I utgangspunktet kan det være hensiktsmessig å fokusere på de som arbeider med informasjonssikkerhet på disse nivåene, men i denne masteroppgaven er det svært aktuelt å inkludere de som også arbeider med pasientsikkerhet. Det er fordi at det skal undersøkes om informasjonssikkerhet kan inngå i opplæringen av pasientsikkerhets, og da er det vesentlig å kommunise-

re med personell fra begge fagfelt der det er mulig. I utgangspunktet kunne en også eksempelvis ha valgt å fokusere på ett av disse tre lagene, men det er svært ønskelig å inkludere alle på bakgrunn av å kunne sammenligne hvordan de ulike perspektivene er, og om de påvirker hverandre.

3.4.2 Innhenting av dokumentasjon

For å besvare problemstillingen, er det ønskelig å samle inn hvilke prosedyrer og rutiner Ahus har for opplæring av informasjonssikkerhet og pasientsikkerhet. For å få tilgang til slik dokumentasjon, sendes det forespørsel til ekstern veileder. Ahus har i tillegg en læringsportal for eksterne brukere med kursmateriell. Ved å registrere seg som ekstern student, vil også relevant kursmateriell innhentes. Formålet med å innhente slik informasjon er å kartlegge kvaliteten i opplæringen, hvor mange som mottar opplæring i sikkerhet i dag, frekvensen for gjennomføring og effekten av tiltaket. Ved å gjøre en slik kartlegging kan en skape et bilde av gapet mellom hvor en er og hvor en eventuelt bør være i fremtiden. Innhenting av slike prosedyrer kan også være verdifullt for å identifisere hva Ahus mener er viktig å inkludere.

Dokumenter som etterspørres er innenfor pasientsikkerhet

- Prosedyrer og rutiner for opplæring innen pasientsikkerhet.
- Oversikt over temaer helsepersonell skal læres opp i.
- Oversikt over hvordan opplæringen skjer og hvor ofte det skjer.

Dokumenter som etterspørres innen informasjonssikkerhet:

- Strategi for opplæring i informasjonssikkerhet.
- Konkrete prosedyrer og rutiner for opplæring av ansatte i IT-sikkerhet.
- Statistikk for hvor mange som har gjennomført kurs.
- Dokumentasjon for evaluering av opplæring i IT-sikkerhet.
- Dokumentasjon for måle effekten av opplæring i IT-sikkerhet.
-

Bakgrunn for ønsket om å innhente prosedyrer innen pasientsikkerhet er å identifisere om informasjonssikkerhet regnes å være en del av pasientsikkerheten fra før av, og eventuelt kartlegge hvordan det kunne ha gått. Dokumentasjonen kan bidra til å gi svar på om Ahus allerede inkluderer informasjonssikkerhet innen pasientsikkerhet.

3.5 Datainnhenting gjennom intervjuer

I tillegg til å innhente eksisterende prosedyrer, er kjernen i denne masteroppgaven å gjennomføre kvalitative intervjuer. Som figur 3.3 beskrev, består organisasjonen av tre ulike lag; strategisk, taktisk og operasjonelt nivå. Siden en vet at forbedringsarbeid eller endringer i seg selv krever å involvere alle lagene, er det ønskelig å intervjue nøkkelpersonell innenfor hvert lag. Både individuelle inter-

vjuer og gruppeintervjuer ble vurdert nøye. Individuelle intervjuer kunne være hensiktsmessig siden en innhenter individuelle perspektiver og at informanten ikke blir påvirket av andre. I realiteten kunne det vært hensiktsmessig å ha et gruppeintervju med de ulike nivåer for å skape diskusjon og potensielt vurdere nye tankemønstre, men på bakgrunn av at de ønskede informantene arbeider under tidspress og har mange arbeidsoppgaver, kan der være mer gunstig for de å ha individuelle intervjuer. Det å ha individuelle intervjuer kan også være hensiktsmessig for å tydeligere kartlegge hvordan de ulike avdelingene gjør det.

3.5.1 Metode for utvalg

Når det skal velges et representativt utvalg av kandidater som kan stille til intervju, er det behov for å finne en metode som tillater å dele populasjoner i undergrupper slik at en kan inkludere tre ulike populasjoner; en for strategisk, en for taktisk og operativt nivå. Et annet kriteria som er viktig i utvalget er at en skal kunne håndplukke utvalget basert på deres posisjon og beslutningsevnen de har til å føre endringer i helseforetaket. Dette er særlig vesentlig på alle tre nivåer. Hvilke kliniske helsepersonell som deltar, kan derimot være mer randomisert da de vil være brukere av systemet. Basert på disse kriteriene, kan en anvende det som kalles stratifisert utvalg da denne metoden tillater å innhente et representativt utvalg fra mindre undergrupper. Undergruppene kalles strata, og gjør det mulig å dele utvalget i de tre populasjonene (Trost, 1986). Deretter vil utvalget plukkes fra disse tre avdelingen. Ulempen ved denne utvalgsmetoden, er at utvalget ofte er randomisert. Det er uheldig da en kan risikere å innhente intervjuobjekter som nødvendigvis ikke har nok kunnskaper å kunne svare på spørsmålene. I denne undersøkelsen er det derimot viktig at en selv kan plukke viktige nøkkelpersoner som til daglig arbeider med de respektive temaene i undersøkelsen. I den forbindelse er det vesentlig å benytte en metode som tillater at utvalget kan håndplukkes. Målrettet prøvetaking, derimot legger til rette for at informanter kan innhentes basert på roller de har i virksomheten. Ulempen denne tilnærmingen er at det kan være tidskrevende, samtidig som at det trengs nøye planlegging (Suri, 2011). Ahus har fra tidligere prosjekter opplevd utfordringer ved innhenting av informanter. Det har vært krevende å intervjue helsepersonell i klinikk da de har lite tid og høy arbeidsbelastning i hverdagen sin. På bakgrunn av dette er det besluttet at kontaktpersoner fra Ahus selv finner intervjuobjekter som kan delta i undersøkelsen. De har også mer oversikt over nøkkelpersonell som kan bidra å besvare problemstillingen. Dette er derfor ikke et problem i denne masteroppgaven da kontaktpersoner fra Ahus vil bistå i dette arbeidet fra starten av prosjektarbeidet for å hindre skjevheter i utvalget.

3.5.2 Variasjon i intervjuguide

På grunnlag at ulike profesjoner og roller skal intervjues, må intervjuspørsmålene tilpasses de ulike nivåene. Eksempelvis kan en ikke stille like spørsmål til informantene på de ulike nivåene fordi at personellet har ulike arbeidsoppgaver.

Dersom noen arbeider med å utforme langsiktige strategier, vil det naturligvis være interessant å kartlegge deres perspektiv for å inkludere informasjonssikkerhet i strategier for pasientsikkerhet. På operativ avdeling så har informantene helt andre arbeidsoppgaver, og da må spørsmålene tilpasses det arbeidet. Det betyr at det vil ses en variasjon i noen av spørsmålene som sendes ut, mens andre er like. De tre ulike spørreskjemaene ligger som vedleg A.

3.5.3 Intervjuprosessen

Intervjuet gjennomføres digitalt over Teams med varighet fra cirka 30 minutter – 1 time. Det blir en dialog rundt spørsmålene som stilles og dersom det er behov for ytterligere forklaringer vil det gis.

3.5.4 Etiske og juridiske aspektere

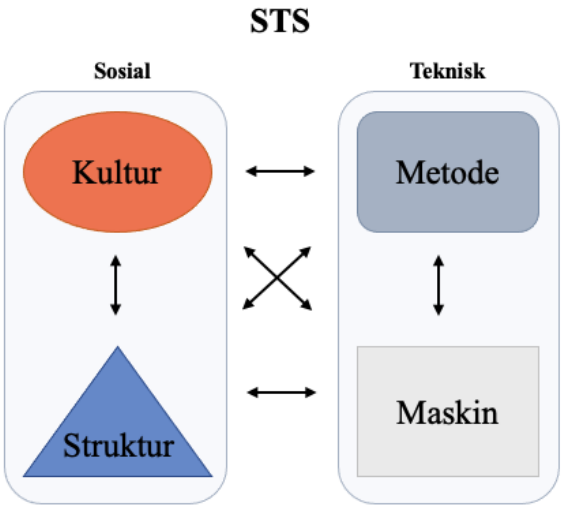
I forkant av intervjuet sendes det et informasjonsskriv om prosjektet og intervjuobjektenes rettigheter i vedlegg B. For å ivareta intervjuobjektenes personvern under intervjuprosessen, har det blitt sendt en søknad til Norsk Senter for Forskningsdata. Denne søknaden ble godkjent, og ligger som dokumentasjon i vedlegg C. På bakgrunn av anonymisering vil ikke intervjuene legges ved som vedlegg. Dette er et bevisst valg som er gjort for å hindre at enkeltpersoner skal gjenkjennes. I selve oppgaven blir informanter pseudonymisert for å sikre at de ikke kan identifiseres, men samtidig tildeles en beskrivende kategori (Datatilsynet, 2015). Kategoriene "medisineller teknologiblir brukt avhengig av hvilken fagekspertise de besitter og divisjon de tilhører. Innenfor kategorien medisin vil alle helsepersonell som arbeider med direkte pasientbehandling eller kvalitetsforbedringer for pasientsikkerhet inkluderes. Kategorien teknologi omfatter de som arbeider med tekniske systemer eller informasjonssikkerhet. Det er verdt å nevne at Ahus har helsepersonell som arbeider i teknologiske avdelinger til tross for at de har en helsefaglig bakgrunn. Siden deres arbeidsoppgaver ikke lenger har med direkte pasientbehandling å gjøre, vil de falle innunder den teknologiske kategorien. Hensikten med disse kategoriene er å danne grunnlag for sammenligning av informantenes perspektiver. Det vil være mulig å identifisere om det foreligger typiske svar for en gitt kategori. Bruken av disse kategoriene kommer først til syne i den sosio-tekniske analysen som skal gjennomføres.

3.6 Bearbeiding og analyse av innsamlet data

Når datagrunnlaget innhentes, vil det bearbeides og analyseres videre. Det første vil være å gå gjennom skriftlige dokumenter for å sjekke prosedyrer for å kartlegge kvaliteten og om prosedyrene anes å være tilstrekkelig. Deretter vil intervjumateriell studeres nøye og deskriptive resultater vil presenteres der det er mulig. Deretter vil de samlede resultatene analyseres videre ved bruk av en sosio-teknisk metode.

3.6.1 Sosio-teknisk modell

I denne rapporten anvendes en model kalt Socio technical system model (STS) presentert av Kowalski (1994). Denne modellen er primært brukt innen rotårsaksanalyse, men kan også brukes i andre sammenhenger. Den benyttes særlig for å finne medvirkende årsaker til hvorfor ulike dataangrep oppstår, på et dypere nivå. I denne masteroppgaven innhentes det inspirasjon av denne modellen da den er kjent fra et tidligere prosjekt, og at den gir et overordnet vurdering, samtidig som et dypere grunnlag for vurderinger. Det vil si at det hentes inspirasjon fra metoden, men at det gjøres noen modifiseringer relevant for denne problemstillingen. Bakgrunn for at det benyttes en sosio-teknisk modell for å skape et beslutningsgrunnlag, er at denne modellen vurderer submoduler for flere aspekter av en organisasjon og mulighetene for å anse om noe kan være hensiktsmessig å gjennomføre i praksis med de forutsetningene helseforetaket har. Den gir muligheten til å identifisere og vurdere faktorer på ulike nivåer i og utenfor helseforetaket, og ulike submoduler innad i hver modul. I tillegg viser forskning at informasjonssikkerhet har blitt addressert som et kompleks sosio-teknisk system av organisatoriske, teknologiske og miljømessige faktorer. Det er fordi systemet kan være så komplekst at en må se på det fra flere perspektiver (Pollini et al., 2022). Ved å bruke en slik modell så kan en se på ulike faktorer fra forskjellige moduler. For å kunne gjøre informasjonssikkerhet til en naturlig del av helsepersonellets daglige aktiviteter, må sosio-kulturelle tiltak kunne støtte de tekniske sikkerhetsmetodene som er laget i virksomheten og omvendt (AlHogail, 2015). Det betyr at det ikke eksempelvis bare kan etableres prosedyrer dersom sykehuskulturen og strukturen ikke tillater det. Dette er bakgrunn for hvorfor et det er ønskelig å ta en beslutning på bakgrunn av en sosio-teknisk analyse.



Figur 3.4: Moduler og submoduler i STS modellen (Kowalski, 1994)

Modellen er presentert i figur 3.4 og er delt i to hovedmoduler der den ene pre-

senterer sosiale faktorer som kan benyttes for vurderingsgrunnlag og den andre presenterer tekniske faktorer. Som figuren viser er hver av modulene igjen delt inn i submoduler som definererer hovedmodulene på et dypere nivå. Formålet er å undersøke om alle de fire submodulene er i balanse. Ofte er ting sammensatt og kan påvirkes av både sosiale og tekniske aspektere. For å kunne anskaffe et beslutnignsgrunnlag, vil det tas inspirasjon i denne modellen. Informasjonen som skal analyseres innhentes ved intervjuene. Kowalski (1994) beskriver kultur om kunnskaper og handlinger som vises av individer. Struktur beskriver hvordan helseforetaket er strukturert som en organisasjon, eller hvordan arbeidet er strukturert. Metode omhandler all type arbeid i form av prosedyrer og rutiner som etableres for maskinene. Maskinene er en systemkomponent i seg selv. I denne oppgaven vil maskin omhandle den sikkerhetsatferden enheten blir utsatt for. Pilene illustrerer hvordan endringer i en submodul påvirker andre moduler.

En metode å bruke STS på kunne vært å kartlegge hvordan Ahus ligger an nå, for å så bruke resultatet på å skape en endring. Målet med å bruke STS i denne oppgaven er å identifisere utfordringer på de ulike nivåene relatert til problemstillingen. Målet med å bruke STS analysen er å skape et vurderingsgrunnlag for å konkludere om det er gjennomførbart i praksis å inkludere informasjonssikkerhet i opplæring for pasientsikkerhet, og kartlegge hvilke faktorer som har en betydning. Det betyr at det vil undersøkes både sosiale og tekniske forhold som kan ha en påvirkning for å dra en konklusjon. Vanligvis ser en kun på svakheter og utfordringer, men i denne masteroppgaven så gjøres det en vri på metoden der det også inkluderes positive sider. Dette er for å skape et helhetsinntrykk av helseforetaket for hvilke muligheter det er for å implementere et nytt opplæringsprogram, og ikke nødvendigvis bare å identifisere svakheter ved å gjøre det. Det å få et helhetsinntrykk av å vurdere både positive og negative sider kan være med å si noe om hvor hensiktsmessig det er i praksis. Hadde en kun fokusert på negative sider, så ville ikke de positive sidene kommet mer frem, noe som kan gjøre det mer utfordrende å dra en konklusjon.

3.6.2 Vekting av identifiserte faktorer

Når resultatene er bearbeidet og faktorer er identifisert, vil det neste seget være å kartlegge hvor stor betydning faktorene har for å kunne inkludere informasjonssikkerhet i opplæringsprogram med pasientsikkerhet. Skåren settes basert på svarene som ble oppgitt under intervju, og hvordan de faktorene potensielt påvirker det å legge til rette for et nytt opplæringsprogram. For å til slutt kunne dra en konklusjon om hvor vidt det er hensiktsmessig, vil både sosiale og tekniske faktorer tildeles en vekt. Dette er fordi at ikke alle faktorer naturligvis veier likt når systemet er så kosmplekst. Hver faktor vil tildeles en skår ut ifra hvor stor betydningen faktoren har for å gjennomføre dette i praksis.

Vekting for å prioritere de viktigste faktorene		
Påvirkning	**Beskrivelse**	**Skår**
Lav	Den identifiserte faktoren har ingen eller mindre betydning for om informasjonssikkerhet og pasientsikkerhet kan inkluderes i ett opplæringsprogram. Denne faktoren vil ikke ha betydning for gjennomførbarheten i praksis.	1
Medium	Den identifiserte faktoren har moderat betydning for om informasjonssikkerhet og pasientsikkerhet kan inkluderes i ett opplæringsprogram. Det betyr at faktoren kan ha en medvirkende betydning for gjennomførbarheten i praksis uavhengig om det gir et positivt eller negativt utfall.	2
Høy	Den identifiserte faktoren har stor betydning for om informasjonssikkerhet og pasientsikkerhet kan inkluderes i ett opplæringsprogram uavhengig om faktoren gir et positivt eller negativt utfall. Det vil si at faktoren bidrar å gi et sterkt vurderingsgrunnlag for om det er gjennomførbart i praksis.	3

Tabell 3.2: Oversikt over verdiene hver faktor kan tildeles.

Bakgrunnen for at det ikke legges stor vekt på om betydningen er positiv eller negativ når det skal gis en skår, er fordi det er ønskelig å både fremheve positive og negative faktorer for å skape et helhetlig blikk over styrker og svakheter i helseforetaket. Resultatet av masteroppgaven vil ikke nødvendigvis gi et ja eller nei svar, men målet er å diskutere gjennomførbarheten i praksis og identifisere de faktorene som må oppfylles for at arbeidet skal lykkes.

I denne analysen anvendes primært tre ulike nivåer for å vekte de ulike faktorene. De faktorene som skårer høyest, vil gi et solid vurderingsgrunnlag, samt direkte eller indirekte kunne ha noe å si for å dra en beslutning for konklusjon. Når alle potensielle sosiale og tekniske faktorer er identifisert, får hver av dem en vekt. Under vektingen vil faktorene deles i to hovedmoduler; sosial og teknisk, fremfor å vekte submodulene hver for seg. Bakgrunn for det er at hovedpoenget er å identifisere de faktorene som kan bidra å gi et sterkt beslutningsgrunnlag for videre analyse og ikke nødvendigvis å analysere hvilke submoduler de tilhører. Hver identifisert faktor vil derfor fordeles i sosial eller teknisk kategori, og deretter tildeles en skår fra 1-3. Deretter vil den totale summen kalkuleres slik at hver modul tildeles en skår gitt i prosent. For å beregne en vekt gitt I prosentandel vil 100 deles på den totale summen vekten som ble gitt for hver av de to modulene og deretter bli multiplisert med modulens opprinnelige skår. Denne metoden har kandidaten tidligere brukt i en rotårsaksanalyse i faget IMT Socioenabled crime.. Metoden kan overføres her.

Vekting for å prioritere de viktigste faktorene
Vekten til hver identifiserte faktor gis en skår mellom 1-3. Den totale vekten av sosiale faktorer (SF) = summen av vekten for alle identifiserte faktorer i den sosiale modulen. Den totale vekten av tekniske faktorer (TF) = summen av vekten for alle identifiserte faktorer i den tekniske modulen. Prosentandel for sosiale faktorer = (100/TF+SF)*SF Prosentandel for tekniske faktorer = (100/TF+SF)*TF

Tabell 3.3: Formel for beregning av den totale vekten gitt i prosent.

Denne beregningen vil kalkulere en fordelingen av faktorene å vise om det er sosiale eller tekniske forhold som påvirker en eventuell innføring av nytt opplæringsprogram. En vekting kan være slik at den ene modulen veier mer enn den andre, ellers så kan begge være i likevekt. Så når faktorene er vektet, vil man etterpå få en analyse der de tyngste faktorene som danner beslutningsgrunnlag fremheves.

3.6.3 Avgrensninger i analysen

En STS analyse kan utføres på fire ulike nivåer; internasjonalt, nasjonalt, organisatorisk og individ nivå. I denne masteroppgaven vil det primært fokuseres på organisatorisk nivå da det er Ahus som er i fokus. I utgangspunktet ville det også vært interessant å vurdere nasjonale aktører i spesialisthelsetjenesten innen informasjonssikkerhet da mye av nasjonale regelverk utarbeides av de på nasjonalt nivå. Eksempelvis kunne det vært Helse- og omsorgsdepartementet, Norsk Helsenett, Direktoratet for e-helse, Helsedirektoratet og tilsvarende (Riksrevisjonen, 2021). Bakgrunn for hvorfor de ikke inkluderes er at det i første omgang er et fokus på å kartlegge aspektere ved opplæring internt hos Ahus. Dersom det viser seg at Ahus opplever utfordringer fra nasjonale myndigheter, er dette noe som kan belyses som utfordringer en kan ta med seg i videre arbeid. I STS analysen vil det organisatoriske nivået deles i tre subkategorier for å undersøke strategisk, taktisk og operasjonelt lag hver for seg som vist i figur 3.3. Bakgrunn for det er at krav for utvikling av prosedyrer ofte utvikles på høyere nivåer enn på operasjonelt lag i seg selv. I all hovedsak er det operasjonelt lag som er i hovedfokuset da det er der målgruppen for opplæringen befinner seg, men siden helseforetaket er komplekst og beslutninger tas på flere nivåer, er det essensielt å inkludere alle for denne undersøkelsen.

3.7 Presentasjon av resultater

På bakgrunn av at det skal innhentes store mengder data både fra eksisterende litteratur, dokumentasjon fra Ahus og gjennom kvalitative intervjuer, vil det være behov for å filtrere den mest interessante og relevante informasjonen som har noe å si for problemstillingen. Slik informasjon vil presenteres både presenteres ved å lage statistiske diagrammer i Excel, men også et STS diagram på slutten av analysen.

Kapittel 4

Eksisterende arbeid

Dette kapitlet presenterer nasjonale og internasjonale rapporter og litteratur for å kartlegge om det eksisterer arbeid på feltet som skal undersøkes i denne masteroppgaven. Først undersøkes rapporter utformet av myndigheter. Deretter beskrives litteratursøket som ble gjennomført, samt resultatene forskningen fremla.

4.1 Offentlige rapporter

Som en del av litteratursøket, ble rapporter utgitt av helsemyndigheter undersøkt for å identifisere om det nevnes noe om viktigheten av å integrere informasjonssikkerhet i pasientsikkerhet. Overordnet viser resultatene at det er nødvendig å gi opplæring i informasjonssikket i helseforetakene, men det gis dog ingen retningslinjer for hvordan det skal gjennomføres i praksis. Et annet funn er det skilles på pasientsikkerhet og informasjonssikkerhet i strategiene og at flesteparten ikke nevner at det må bli sett på i sammenheng. Verdens helseorganisasjon (WHO) er en internasjonal organisasjon som arbeider med å bekjempe globale helseutfordringer. I sin rapport nevner de behovet for at nasjonale helsemyndigheter må legge til rette for å integrere informasjonssikkerhet i pasientsikkerhetsaspektet. Grunnet trusler rettet mot digitale domener, ser de et behov for at helseforetak må styrke sikkerhetskulturen slik at helsepersonell som håndterer informasjonssystemer kan identifisere forsøk på dataangrep. Måten de mener dette gjøres ved å etablere et rammeverk som beskriver hvordan teknologi kan bidra å styrke pasientsikkerheten, samtidig som å identifisere og mitigere risikoer. De mener også at dette arbeidet må inkludere ledere på ulike nivåer, inkludert de som arbeider i klinikken (WHO, 2021).

I Sikkerhetsloven (2019) fremlegger §4-1 at forebyggende sikkerhetsarbeid skal være en sentral del av virksomhetens styringssystem og at sikkerhetstilstanden regelmessig skal kontrolleres. Det nevnes også at virksomheten er ansvarlig for at ansatte har adekvat forståelse for risiko – og sikkerhetsarbeidet. I den sammenheng ble rapporter utarbeidet av helsemyndigheter og regionale helseforetak for å identifisere om de knytter pasientsikkerhet og informasjonssikkerhet på noe

vis. Helsedirektoratet (2019) har utarbeidet en nasjonal handlingsplan for pasientsikkerhet og kvalitetsforbedring som er gjeldende fra 2019 til 2023. Formålet med denne handlingsplanen er å bidra til å levere trygge og sikre helsetjenester (Helsedirektoratet, 2023). For å styrke pasientsikkerheten og kvalitetsforbedring, nevnes det at det er behov for å opprette digitale læringsressurser som helsepersonell kan benytte for å øke kunnskaper. I rapporten nevnes det imidlertid ingenting om behovet for opplæring av informasjonssikkerhet i dette arbeidet (Helsedirektoratet, 2019).

I det nasjonale pasientsikkerhetsprogrammet kalt «I trygge hender», har det også blitt uttrykt et behov for å styrke kompetansemiljøet innen pasientsikkerhet. Målet deres er å redusere antall pasientskader som oppstår ved å styrke pasientsikkerhetskulturen i helse – og omsorgstjenesten (Helsedirektoratet, 2023). For å gjøre dette har de blant annet utarbeidet en tiltakspakke for ledere i pasientsikkerhet. Heller ikke her er det et stort fokus på informasjonssikkerhet. Det som imidlertid nevnes, er at det er nødvendig å etablere skjermede arbeidsstasjoner for å forbedre arbeidet med informasjonssikkerhet (Itryggehender, 2023). Utenom tiltakspakken nevner de at ledere må legge til rette for at helsepersonell utvikler ferdigheter, rutiner og kunnskaper om teknologi i tillegg til å utøve profesjonsrelaterte arbeidsoppgaver. De nevner også at slikt forbedringsarbeid krever et tverrfaglig samarbeid mellom helsepersonell og andre fageksperter. Fra tidligere forskning har de erfart at det kan virke krevende å gjennomføre et forbedringsarbeid og at det fort undervurderes i en travel hverdag. På bakgrunn av det, mener de det er vesentlig å involvere ledere på alle organisasjonsnivåer, og ikke minst sette av tid for å gjennomføre forbedringsarbeidet. Utover dette nevne det ikke noe om informasjonssikkerhet (Itryggehender, 2017).

Direktoratet for eHelse (2023b) har utarbeidet en plan for realisering av nasjonal e-helsestrategi. Denne strategien belyser langsiktige planer for hva som skal prioriteres innenfor digitaliseringsaspektet av helse- og omsorgssektoren mot 2023. Det nevnes det imidlertid at helsepersonell skal evne å anvende digitale systemer for å styrke pasientsikkerheten, men nevner heller ikke noe om å inkludere informasjonssikkerhet. Direktoratet for eHelse (2022) har utformet Normen som skal være en norm for informasjonssikkerhet og personvern i helse – og omsorgssektoren. Normen ble utarbeidet som følge av økt digitalisering i helsesektoren og behovet for å beskytte informasjonsverdier i helseforetaket. Dette dokumentet trekker imidlertid inn at god pasientsikkerhet innebærer ivaretakelse av informasjonssikkerhet og at helsepersonell må få opplæring for å styrke sikkerhetskulturen. Det gis dog ingen retningslinjer for hvordan dette arbeidet skal foregå annet enn at det bør gjennomføres kontinuerlig, og at både gjennomført opplæring og effekt bør dokumenteres. Som en del av Norsk helsenett nevner Ahus at de har skrevet under på å følge denne Normen.

Litteraturen presentert i dette kapitlet viser at det på nasjonalt nivå er behov for

opplæring i informasjonssikkerhet for å styrke pasientsikkerheten, men det gis ingen føringer på hvordan dette kan gjøres i praksis. For hvert fagområde nevnes hverken informasjonssikkerhet eller pasientsikkerhet noe særlig i hverandres rapporter. Dette kan potensielt være et funn som kan påvirke sikkerhetskulturen i praksis, og som vil kartlegges i kapittel 6.

4.2 Resultatet av litteratursøket

Dette delkapittelet beskriver resultatene av litteraturstudien. Først presenteres søkene som ble gjennomført og hvor mange resultater det ga. Deretter belyses relevant litteratur. Tabellen under viser søkene som ble gjennomført, og hvilke søkeord som ble brukt. Tabellen viser også hvor mange artikler som virket relevant basert på tittelen, hvor mange sammendrag som ble lest og hvor mange av de som ble antatt til å være aktuell å lese videre. Etter å ha lest hele artikkelen ble den vurdert for å være med i datasettet slik at snowball method kunne bli brukt på å finne ytterligere referanser.

Litteratursøk			
PubMed			
Søkeord	**Sammendrag**	**Lest**	**Datasett**
Patient safety AND cybersecurity	10	7	Coventry & Branley (2018), Schneider & Wirth (2021), Agboola, Bates & Kvedar (2016).
Information security AND Patient safety	4	2	Sheikh et al. (2021).
Patient safety AND cybersecurity AND Educational model	0	0	0
Patient safety AND cybersecurity AND Training	5	3	Wasserman & Wasserman (2022), Dameff et al. (2019).
Cybersecurity AND Patient education	0	0	0
IEEE Xplore			
Søkeord	**Sammendrag**	**Lest**	**Datasett**
Patient safety AND cybersecurity	7	4	0
cyber security AND awareness AND healthcare	3	1	Ali & Alyounis (2021.)
Information security AND hospital AND awareness	4	2	0
Google Scholar			
Søkeord	**Sammendrag**	**Lest**	**Datasett**
Patient safety AND cybersecurity	7	5	0
Patient safety AND cybersecurity AND culture	5	4	Pollini et al.(2022).

Tabell 4.1: Resultatet av litteratursøket.

Som tabellen viser under søket i PubMed er det to rader i tabellen som er nullet ut. Den første ble det som følge av at det ikke var noen resultater på søket, mens den andre er det fordi det ikke ble observert relevante artikler. Etterhvert som søkene ble gjennomført, viste det seg at det var de samme artiklene som dukket opp igjen i de fleste databasene. Dette ble særlig observert i Google Scholar. Bakgrunn for det kan blant annet være lite variasjon i søkeordene og kombinasjonene som ble brukt eller at det bare er lite forskning på feltet. For å øke sannsynligheten for å finne relevante artikler, ble snowball method brukt som nevnt i kapittel 3. Tabellen nedenfor viser datasettet metoden ble utprøvd på. Tabellen viser først navnet på forfatterne av artikkelen og deretter antall referanser i hver artikkel, hvor mange som ble lest og hvor mange som ble tatt med videre som et resultat.

Snøballmetoden			
Datasett	**Referanser**	**Lest**	**Resultat**
Coventry & Branley (2018)	58	4	0
Schneider & Wirth (2021)	29	2	0
Agboola, Bates & Kvedar (2016)	10	0	0
Sheikh et al., (2021)	130	15	0
Wasserman & Wasserman (2022)	122	9	0
Dameff et al. (2019)	17	2	0
Ali & Alyounis (2021)	17	1	Rajamäki, Nevmerzhitskaya, & Virág (2018).
Pollini et al.(2022)	131	19	AlHogail (2015).

Tabell 4.2: Resultatet av litteratursøket etter å ha brukt snøballmetoden.

Som tabellen viser, var det en stor spredning i antall referanser for hver artikkel og det var kun en artikkel som til en grad antas å være relevant. Det er likevel nevneverdig at flere av artiklene hadde flere nettsider som referanser i sine artikler i tillegg til forskning. Hvor pålitelige og valide alle resultatene er kan derfor diskuteres. På den andre siden observeres det at det finnes svært lite forskning om akkurat det som omhandler problemstillingen i denne masteroppgaven. Å undersøke referanselistene til tross for at noen av artiklene inneholdt referanser av mindre kvalitet, ble derfor ansett som tilstrekkelig. Det var for å undersøke om noen av de bedre referansene potensielt kunne inneholde relevant litteratur. Et annet funn som ble gjort ved å bruke Snowbal method, var at de samme referansene gikk igjen i flere artikler. Dette kan tyde på at det er lite forskning på feltet eller at relevante artikler eventuelt ikke har blitt publisert enda. Det kan også være at søkeordene ikke var tilstrekkelig for å identifisere ønskede artikler. Det neste delkapittelet viser resultatet av litteraturstudien.

4.2.1 Litterære funn

Som nevnt i introduksjonskapitlet skal denne masteroppgaven undersøke om cybersikkerhet kan inkluderes som en del av opplæringen i pasientsikkerhet ved norske sykehus. For å finne ut av det ble det forsøkt å identifisere tilsvarende forskningsartikler fra andre sykehus på internasjonalt nivå. Resultatet fra litteraturstudien viste ingen funn på at en tilsvarende studie har blitt gjennomført av noen andre. Wasserman & Wasserman (2022) nevner at 35 studier har vist at opplæring i cybersikkerhet for helsepersonell har vist å redusere antall dataangrep. Forskere som blant annet Schneider & Wirth (2021) hevder imidlertid at det er svært lite forskning på hvilke metoder som spesifikt kan benyttes for å gi opplæring i IT-sikkerhet til helsepersonell. Dameff et al. (2019) sin studie legger til at det er utviklet få pedagogiske metoder for opplæring av helsepersonell til tross for at det er en sterk kobling mellom pasientsikkerhet og cybersikkerhet. Litteraturen deres beskriver imidlertid at det er et stort behov for slik type opplæring for å øke kunnskaper og bevissthet, samt sikre tilstrekkelig sikkerhetsatferd blant medisinsk fagpersonell. Det at det finnes få metoder gjør det mer utfordrende for helsepersonell å forstå cyberriskikoer i klinisk sammenheng. De hevder også at noe forskning legger frem enkelttiltak en kan iverksette, men at få har utprøvd konkrete opplæringsprogrammer i klinikken.

Forskere er imidlertid enige om at cybersikkerhet er en essensiell del av pasientsikkerhet, og at faget må integreres som en del av pasientsikkerhetsprogrammet. Coventry & Branley (2018) og Wasserman & Wasserman (2022) hevder at på bakgrunn av truslene sykehuset blir utsatt for, så må cybersikkerhet være en del av selve pasientsikkerhetskulturen og sykehuskulturen generelt. De påpeker at en ikke kun skal anse helseforetaket som sikkert ved å utforme prosedyrer, men også trene opp helsepersonell til å bli en slags menneskelig brannmur som kan beskytte informasjonsverdier i helseforetaket. Schneider & Wirth (2021) anser også cybersikkerhet som et pasientsikkerhetsproblem og at helsepersonell må læres opp i hvordan de kan beskytte pasientene de behandler. De utdyper at helsepersonell ikke lenger kan vente på å bli beskyttet av IT-personell, men at de heller selv må fokusere på å bli sikkerhetspartnere slik at de sammen kan bekjempe dataangrep.

For å gjøre dette arbeidet noe enklere, presenterer Ali & Alyounis (2021) et rammeverk kalt Proactive Resilience Educational Framework som kan brukes for opplæring i IT sikkerhet i sykehusavdelingenes miljøer. Rammeverket legger til rette for å øke bevisstheten, kontinuerlig evaluere progresjon og vurdere forbedringer og utvikling. Rajamäki, Nevmerzhitskaya, & Virág (2018) som er utviklerne av dette rammeverket, har laget seks ulike trinn en må igjennom for å fullføre rammeverket. Det første omhandler å etablere generell prosjektledelse for å sikre at opplæringsprosjektet kan gjennomføres i praksis. Steg to er å identifisere cybertrusler og sårbarheter i helsesystemene ved å bruke internasjonale standarder og rammeverk. I tillegg er det et fokus på å kartlegge konkrete behov for opplæring.

I det tredje trinnet gjennomføres det først en interessentanalyse for å kartlegge interessentene i prosjektet, utvikle workshops og indikatorer for å oppdage ulike trusler slik at det skal bli enklere for helsepersonell å detektere potensielle forsøk på angrep. Det fjerde trinnet er å utvikle selve opplæringskonseptet. Det vil si å lage digitalt materiell med innhold, samt kunne tilby det til helsepersonell. Trinnet vil etablere et pilotprosjekt med en øvelse der først IT avdelinger skal teste ut det utviklede opplæringsprogrammet. Når det er gjort skal det testes av helsepersonell og læringsutbyttet skal evalueres. I trinn fem oppsummeres hva som er lært for å lage proaktive strategier for å redusere menneskelige sårbarheter. I trinn seks fokuseres det på hvordan opplæringen kan integreres og formidles til personell. Det handler om hvordan en kan benytte konferanser og andre arrangement for å belyse arbeidet som har blitt gjort. Modellen legger vekt på interaktiv læring og at innholdet skal være direkte relevant for helsepersonellets arbeidshverdag. Et hovedmoment er at tilsvarende opplæringsprogrammer må inkludere temaer for å identifisere risikoer, beskytte informasjonsverdier, detektere forsøk på angrep, respondere for å hindre skader og gjenopprette normal drift. Alle i virksomheten uavhengig nivå bør øve på dette. Det nevnes også at rammeverk som brukes i et helseforetak må være fleksibelt da sykehusavdelinger er i ulik størrelse, har forskjellig kapasitet og driver med forskjellig behandling. Rammeverket er imidlertid ikke testet tilstrekkelig i praksis noe som kan gjøre det utfordrende å sette en standard.

Til tross for lite forskning på feltet vil litteraturen i de neste avsnittene presentere momenter som anses å være vesentlig når cybersikkerhet skal integreres i pasientsikkerhetsdomenet. Coventry & Branley (2018) påpeker viktigheten at kulturforandringen må komme fra det øverste nivået i organisasjonen og forplante seg nedover i helseforetaket som en slags top-ned tilnærming. Helst bør nasjonale organer som helse – og omsorgsdepartementet arbeide for etableringen av denne kulturen i sine strategier, og for å sikre at helseforetakene aksepterer denne kulturendringen. De konkluderer imidlertid med at det trengs mer forskning på feltet. Schneider & Wirth (2021) hevder på sin side at engasjementet for sikkerhet også må komme fra regionalt nivå i tillegg til det nasjonale for at helseforetakene skal se alvoret i behovet for kulturendringen. Innad i helseforetaket legges det også vekt på at samarbeidet mellom sykehusledelsen og IT-sikkerhet må styrkes for å iverksette et passende rammeverk for opplæring på det operasjonelle nivået Agboola, Bates & Kvedar (2016) støtter dette og påpeker at det er nødvendig å implementere et rammeverk på høyere nivå for at helsepersonell skal kunne håndtere cyberrisikoer på sitt nivå. Sheikh et al., (2021) på sin side nødvendigheten av å inkludere klinikere i arbeidet med opplæring i sikkerhet. De utdyper at dersom det strategiske nivået står for opplæring uten å involvere klinikere, så kan det være utfordrende for helsepersonell å gjennomføre kursene da det kanskje ikke er anvendbart i praksis. Opplæringen som gis må utarbeides i samarbeid med klinikere slik at teknologien og arbeidsoppgavene henger sammen.

Schneider & Wirth (2021) hevder at deres undersøkelse viser at helsepersonell ser på opplæring i cybersikkerhet som en byrde når den er utviklet av ikke-medisinsk personell. Utfordringen med dette er at opplæringen ikke er tilpasset deres hverdag, noe som gjør at fagfeltet oppleves ukjent. Det er derfor et stort behov for at IT-sikkerhetspersonell arbeider tett med klinikere for å tilpasse en opplæring de kunne hatt nytte av. I tillegg er det vesentlig å etablere prosedyrer for å måle effekten av programmet. Pasientsikkerheten og helseforetaket i seg selv må inkluderes i alle aspekter av cybersikkerhet, også når det kommer til opplæring. I tillegg bør det etableres prosedyrer og tekniske verktøy for hvordan helsepersonell kan rapportere inn sårbarheter og hendelser knyttet til cybersikkerheten. AlHogail (2015) påpeker imidlertid at det ikke kun er tekniske aspektere som det å utvikle prosedyrer i seg selv som påvirker sikkerhetsnivået, men også ansatte og kulturen i organisasjonen. Pollini et al. (2022) legger til at ferdig utviklede og gode prosedyrer med retningslinjer mister verdi dersom det ikke er et stort nok fokus på å formidle det på riktig måte til målgruppen. I sin studie fant de ut at dersom prosedyrene ikke ble kommunisert tilstrekkelig til tross for at de var utformet, sa brukerne at de ikke hadde tid til å lese de, samtidig som at de ikke visste hvor dokumentasjonen var tilgjengelig, manglet kunnskaper om hvordan de skulle forstå instruksene og at det mangler en grunnleggende motivasjon for å lese de. De mener derfor at riktig kommunikasjon er vesentlig for å kunne øke motivasjonen til at personell selv skal lese dokumentasjon på egenhånd. Både Sheikh et al. (2021) og Schneider & Wirth (2021) påpeker at det vil være et sterkt behov for å ansette noen som har rollen som klinisk informatiker som kan bistå med cyberopplæring på sykehusavdelingen. Ved at en ansatt på operativ avdeling lærer seg aspektere innen cybersikkerhet kan vedkommende ha ansvaret for å formidle kunnskaper om cybersikkerhet blant helsepersonell lokalt på sin avdeling. I tillegg bør det gjennomføres jevnlige cybersikkerhetskampanjer for å synliggjøre fagområdet og gi undervisning for å øke bevisstheten rundt risikoene på sykehuset. For å være fremtidsrettet, mener Wasserman & Wasserman (2022) at flere forskere har foreslått at studenter som har praksis på sykehuset burde gjennomføre ekstraordinær opplæring i IT-sikkerhet for å sikre at fremtidens helsepersonell har kunnskaper om cyberrisikoer før de kastes ut i et sårbart miljø. Dameff et al. (2019) påpeker nødvendigheten av å benytte opplæringsmetoder som allerede er kjent for helsepersonell slik at det ikke skal oppleves som tyngere enn det trenger å være.

Litteraturen presenterer en rekke tankesett for hvordan fokuset på cybersikkerhet og opplæring bør foregå i et helseforetak for å sikre gode resultater. Det presenteres både tiltak og rammeverk som er utviklet for helsesektoren. Til tross for at det er lite forskning på feltet, viser litteraturstudien at det er en felles enighet om at cybersikkerhet er en essensielt del av pasientsikkerheten og at de bør integreres sammen for å styrke kunnskapene som kan bidra å redusere sannsynligheten for å bli utsatt av dataangrep grunnet menneskelige svakheter. Til tross for at flere forskere nevner dette, er det ingen som belyser konkrete opplæringsmetoder som støtter utsagnene og eventuelt forklarer hvordan det kan koordineres i

praksis. Det ble imidlertid nevnt at det er hensiktsmessig å benytte opplæringsmetoder som allerede er kjent for helsepersonell når det skal gis opplæring i informasjonssikkerhet sånn at de slipper å forholde seg til ytterligere komplekse verktøy (Dameff et al., 2019). I dette masterprosjektet skal det derfor foreslås et nytt opplæringskonsept som kan sikre en mer kontinuerlig opplæring for helsepersonell i IT-sikkerhet basert på metoder som benyttes i dag. Dette kan igjen potensielt bidra å øke frekvensen for opplæring som gis i cybersikkerhet, samt legge til rette for at helsepersonell har tid til å gjennomføre opplegget. Neste kapittel presenterer den nye konseptet.

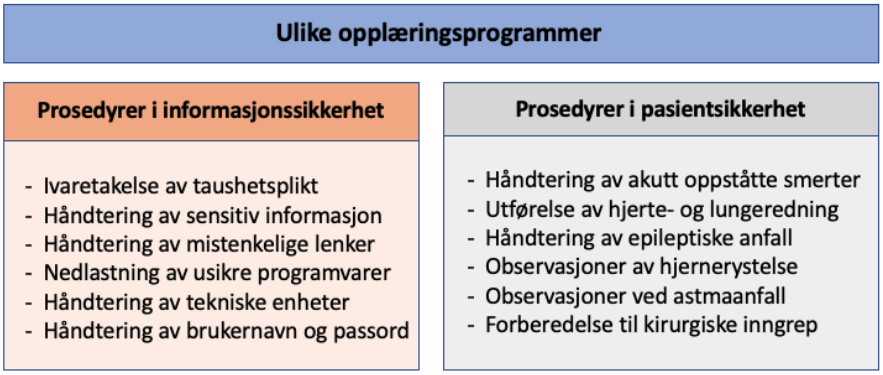
Kapittel 5

Presentasjon av nytt opplæringskonsept

Dette kapittelet fremlegger opplæringskonseptet som blir introdusert under de kvalitative intervjuene. Formålet med opplæringskonseptet er å skape refleksjon, nye tankeprosesser og fremme perspektiver for å drøfte om informasjonssikkerhet kan inkluderes som en del av opplæringen i pasientsikkerhet. I tillegg er det ønskelig at denne type refleksjon bidrar til å identifisere konkrete forutsetninger som må tilfredsstilles på organisatorisk nivå før informasjonssikkerhet faktisk kan inkluderes som en del av opplæringen i pasientsikkerheten. Ved å identifisere disse forutsetningene, vil Ahus ha konkrete faktorer å arbeide mot for å styrke sikkerhetskulturen i helseforetaket. Dette er også bakgrunnen for hvorfor opplæringsmetoden presenteres som et konsept fremfor et konkret opplæringsprogram med spesifikt innhold. Det betyr likevel ikke at metoden ikke kan anvendes i praksis. Dersom resultatene skulle være positive, er det muligheter for å faktisk teste opplæringskonseptet i operative avdelinger.

5.1 Tradisjonell opplæring

Fra tidligere nevner Ahus at de har separate opplæringsprogrammer for opplæring i pasientsikkerhet og informasjonssikkerhet. Helsepersonell er vandt til å følge medisinske prosedyrer i pasientbehandlingen for å sikre at det gis forsvarlig helsehjelp i tråd med faglige retningslinjer. På den andre siden har de opplæring av informasjonssikkerhet som skal bidra å øke kunnskaper, bevisstgjøre sikkerhetsatferd og endre holdninger. Figuren nedenfor viser at begge opplæringene i dag gjennomføres separat.

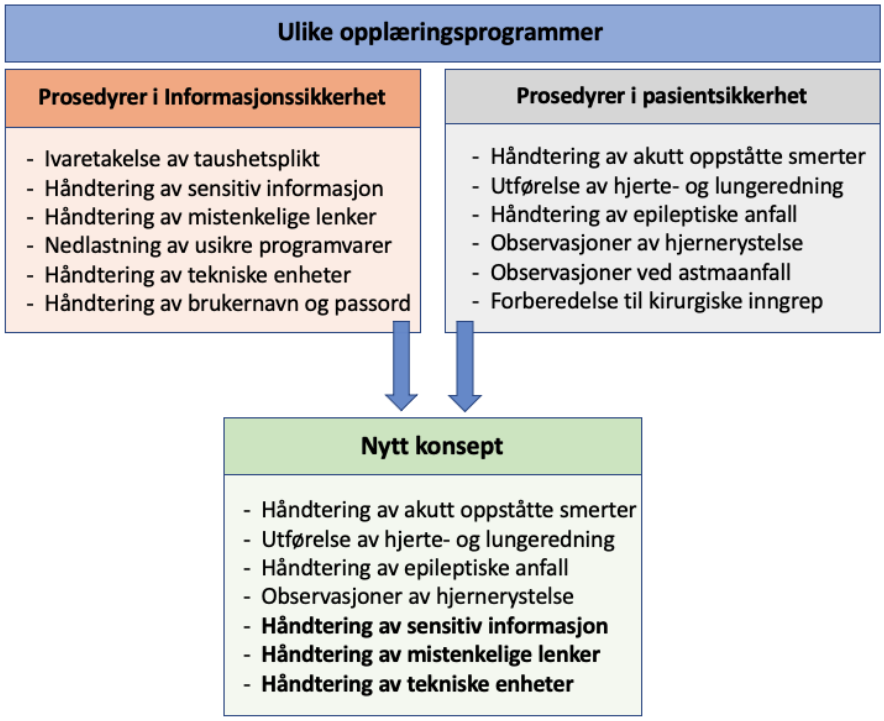


Figur 5.1: Figuren viser at opplæring i pasientsikkerhet og informasjonssikkerhet gis i separate programmer.

For å sikre at både data blir håndtert korrekt og at medisinske prosedyrer følges i henhold til retningslinjer, blir det i dag gjennomført fysisk eller digital opplæring der helsepersonell kan øve seg på de ulike prosedyrene. Figuren ovenfor viser eksempler på prosedyrer innenfor hvert fagfelt. I realiteten antas det at listen er mye lenger og at det finnes et større antall opplæringsprogrammer enn nevnt i denne masteroppgaven. Tidligere erfaringer fra spesialisthelsetjenesten viser også at enkelte avdelinger utformer spesialiserte prosedyrer avhengig av hvilke helsetjenester de tilbyr. Hensikten med figuren ovenfor er derimot kun å illustrere at opplæringen innen begge fagfelt foregår separat. Utfordringen med denne tilnærmingen, er at opplæringen i informasjonssikkerhet nedprioriteres da pasientbehandlingen er i fokus. Det fører til at det ikke gis tilstrekkelig opplæring i informasjonssikkerhet.

5.2 Nytt opplæringskonsept

På bakgrunn av utfordringene nevnt i forrige avsnitt, ble det utviklet et konseptet der prosedyrer i informasjonssikkerhet og pasientsikkerhet inkorporeres i ett felles opplæringsprogram for å sikre jevn formidling av kunnskaper i informasjonssikkerhet. Figuren nedenfor illustrerer et eksempel på et slikt program. Selve metoden for å formidle kunnskaper er nødvendigvis ikke ny, men konseptet kan regnes som innovativt da det er med på å endre tidligere arbeidsmetoder og tankeprosesser i den forstand at det tidligere ikke har vært en kultur for å blande begge fagområder. Siden de cyberrelaterte truslene stadig vokser, vil det også være behov for å tenke annerledes enn tidligere. Denne masteroppgaven skal derfor undersøke om dette konseptet er anvendbart i praksis, og hva som eventuelt må til for at det kan realiseres.



Figur 5.2: Figuren viser et nytt opplæringskonsept som både inkluderer informasjonssikkerhet og pasientsikkerhet i ett program

Figuren visualiserer et nytt konsept der både tematikk innenfor pasientsikkerhet og informasjonssikkerhet inkorporeres i ett opplæringsprogram. Det er viktig å påpeke at temaene som er nevnt i figuren er tilfeldige, og at de ikke er plukket ut basert på alvorlighetsgrad. Det er heller ikke slik at de må utføres i gitt rekkefølge da det selv kan bestemmes av avdelingen ut fra hva de synes er hensiktsmessig og ryddig. Det er heller ikke sånn at det på nåværende tidspunkt stilles krav til hvor mange kategorier av temaer i informasjonssikkerhet som må inkluderes som et minimum, men det ønskes å undersøke om konseptet i seg selv er gjennomførbart i praksis. Det er likevel viktig å påpeke at det må inkluderes minimum ett tema for at en ikke skal miste poenget med konseptet.

5.3 Fordeler ved konseptet

Fordelene ved et slikt konsept kan knyttes til at det hyppigere gis innføring i informasjonssikkerhet sammenlignet med i dag. Den er hovedsakelig rettet mot operative avdelinger da det er de som er i hovedfokuset, men kan også benyttes av andre divisjoner som ønsker det. Fleksibiliteten som kommer med konseptet, gjør at hver enkelt sykehusavdeling selv kan skreddersy sitt eget program avhengig av hva de trenger på sin avdeling. Selve innholdet og tema i informasjonssikkerhet kan bestemmes av avdelingen selv, eller koordineres ved bistand fra informasjons-

sikkerhetsrådgivere på Ahus. Det legges til rette for gjenbruk av prosedyrer i informasjonssikkerhet dersom det er utviklet av avdelingen selv, men åpner også for å inkludere nye prosedyrer. Konseptet kan inkorporeres i en allerede etablert plan for internundervisning, fagdager eller annen opplæring slik at det ikke vil være behov for å planlegge ekstra tid utover den tiden som egentlig var satt av for fagutviklingsformål. Konseptet i seg selv skal derfor bidra til at informasjonssikkerhet kan belyses på en enkel måte.

5.4 Utfordringer ved konseptet

Til tross for fordelene kapittelet ovenfor presenterer, er det nevneverdig at det også kan oppstå utfordringer. Disse kan først og fremst relateres til at det kreves en kulturendring for å akseptere endringer i opplæringen på operativt nivå. Dette gjør at en sykehusavdeling potensielt må bryte et mønster de har hatt over flere år for hvordan de tilbyr helsepersonell opplæring. I tillegg er det en viss sannsynlighet for at de potensielt må bortprioritere noen medisinske temaer som egentlig skulle vært på agendaen for å få plass til informasjonssikkerhet. Et annet scenario kan være at de må sette av litt mer tid for å gjennomføre opplæringen. Dersom resultatkapittelet i denne masteroppgaven viser at Ahus mangler prosedyrer i informasjonssikkerhet, vil det være nødvendig å etablere nye retningslinjer for å realisere konseptet slik at fagstoffet kan inkluderes på agendaen. Som litteraturen beskrev i kapittel 4, var det essensielt å utforme et program som passer daglige gjøremål i en operativ avdeling. Mange sykehusavdelinger kan være like, noe som gjør at det samme innholdet kan anvendes på ulike avdelinger, men andre avdelinger kan eksempelvis bruke ulike digitale systemer eller medisinteknisk utstyr, som gjør at innholdet må tilrettelegges deres hverdag. Dette kan bidra til at det kreves ytterligere ressurser fra taktiske avdelinger for å tilrettelegge for at innholdet er tilpasset disse avdelingen. En annen utfordring kan være dersom noen operative avdelinger ikke tilbyr internundervisning eller fagdager. Det betyr at det vil være behov for å finne et spesifikt tidsrom for å gjennomføre opplæringen i arbeidstiden. Slike faktorer vil imidlertid undersøkes gjennom innhenting av statistikk og utførelse av en sosio-teknisk analyse i neste kapittel.

5.5 Kritikk rettet mot konseptet

En kan lure på hvorfor det trengs et helt nytt konsept fremfor å øke frekvensen av den eksisterende opplæringen i informasjonssikkerhet som tilbys i dag. Svaret på det er at det kan være utfordrende å prioritere å tilby opplæringen i praksis dersom det er valgfritt å gjennomføre og at det ikke rettes fokus mot det. Ahus har selv gjennom møter uttrykt at opplæring i informasjonssikkerhet blir bortprioritert og går i glemmeboken fordi det ikke finnes konkrete metoder som kontinuerlig tilrettelegger for å formidle slik kunnskap i praksis. De operative avdelingene har selv ansvar for å tilby ansatte opplæring, men det har blitt observert at disse tilta-

kene ikke iverksettes. Sannsynligheten for at det vil skje fremover regnes derfor å være lav i følge Ahus. Dersom en ikke anvender konseptet, men generelt øker fokuset på sikkerhet, vil det likevel være behov for å legge til rette for denne opplæring i praksis. Hvis det oppleves som krevende grunnet tid, stress og arbeidsbelastning, kan det igjen enkelt bortprioriteres. Temaer informasjonssikkerhet er ikke så kjent for helsepersonell, og det vil kreves endringer i holdninger og kultur for at sikkerhetsarbeidet skal bli vellykket (NSM, 2023c). Det er derfor ønskelig å teste noe nytt som potensielt kan bidra til en endring i form av at fagområdet belyses oftere. Det anses å være mer fordelaktig å få en innføring i informasjonssikkerhet i ny og ned fremfor at det ikke blir fokusert på i det hele tatt. Dette bekrefter også Ahus.

5.6 Effektivitet

I utgangspunktet er det vært svært aktuelt å kartlegge effekten av dette opplæringskonseptet for å teste om det øker effektiviteten av opplæring sammenlignet med metoden som benyttes i dag. Sykehussystemene er imidlertid svært komplekse og består av flere organisatoriske nivåer som har noe å si for om konseptet kan anvendes i praksis. For å måle effekten av denne type opplæring, må opplæringen kunne gjennomføres i praksis og den må kunne testes over en lenger tidsperiode. Det er først da en kan måle om effekten er som ønsket. Det betyr at prosessen er lang og effekten ikke kan måles på grunnlag av tidsrammene som er satt for dette masterprosjektet. Dette kan imidlertid utføres i videre arbeid.

Kapittel 6

Resultat

Dette kapittelet presenterer de ulike resultatene fra casestudien. Først vil identifisert dokumentasjon fremlegges, etterfulgt av deskriptive resultater og til slutt den sosio-tekniske analysen.

6.1 Innhenting av prosedyrer

For å kartlegge eksisterende prosedyrer, var det et ønske å innhente en rekke prosedyrer og rutiner knyttet til opplæring informasjonssikkerhet og pasientsikkerhet. Det viser seg at det finnes minimalt med dokumentasjon for prosedyrer og rutiner for opplæring i informasjonssikkerhet. Det foreligger dokumentasjon for ett strategisk dokument med langsiktige mål, ett obligatorisk nyansattkurs som må gjennomføres for å få tilganger og nøkkelkort, og dokumentasjon for aktiviteter for sikkerhetsmåneden. Ingen andre prosedyrer annet enn disse finnes da det argumenteres for at sykehusavdelingene selv skal utvikle sine prosedyrer. Det betyr at Ahus ikke har konkret opplæring for ansatte og har heller ingen prosedyrer for å måle effekt av opplæring eller evaluerer opplæringen som gis. Det var heller ikke mulig å innhente informasjon om opplæringsprogrammer som gis innen pasientsikkerhet da dette styres internt i avdelingene avhengig av hva sykehusavdelingen er spesialisert i. Nedenfor presenteres kort den informasjonen som er identifisert.

6.1.1 Strategi for personvern og informasjonssikkerhet 2022-2025

I denne strategien har Ahus en klar visjon: «Ahus kal skape en digital sikkerhetskultur til det beste for pasienter, ansatte og samfunnet». I perioden 2022-2025 har Ahus innenfor informasjonssikkerhet et fokus på organisering, kultur og bevisstgjøring, systemeierskap, innovasjon og nye arbeidsmetoder, risikohåndtering, og styring og forbedring. Relatatert til kompetanseheving i informasjonsikkehet skal Ahus utvikle organisasjonen ved å styrke samarbeidet mellom informasjonssikkerhetseksperter og klinikker, staber og prosjektdeltakere. Sikkerhetskulturen skal styrkes ved å utføre dedikerte bevistgjøringskampanjer. Sikkerhetsmåneden er et eksempel på dette. I tillegg skal det gis opplæring til nyansatte og ledere,

samt tilbys veiledning og kurs. Hver avdeling skal sette seg egne mål de har til informasjonssikkerhet.

6.1.2 Grunnkurs i informasjonssikkerhet

Ahus tilbyr et nyansattkurs til alle nyansatte, vikarer, hospitanter og studenter som trenger tilgang til sykehusets ressurser. Kurset er produsert av Ahus sammen med avdeling for kompentanse og utdanning i 2018. Det gjennomføres som et e-læringskurs i læringsportalen, som er en plattform som inneholder alle kurs som tilbys til personell i helseforetaket. Kurset tar cirka 15 minutter å gjennomføre og tilbys også på engelsk. Innholdet er sammensatt og består av forklaring av begrepet personvern og informasjonssikkerhet. Det gis en innføring i nødvendigheten av å beskytte data som er lagret i sykehusets digitale systemer og å hindre spredning av pasientsensitiv data på sosiale medier. Kurset inneholder også informasjon om taushetsplikt og en avtale den ansatte må signere. Det gis informasjon om konsekvensene av å bryte taushetsplikten eller misbruk av pasientinformasjon og teknisk utstyr. En omfattende sikkerhetsinnstruks på ni sider belyser en rekke retningslinjer innenfor spesifike kategorier som er essensielle for å ivareta informasjonssikkerheten i foretaket. Figuren nedenfor viser antall retningslinjer for hver kategori av tema.

Figur 6.1: Figuren viser kategorier for retningslinjer som er gitt i sikkerhetsinnstruksen, samt antall retningslinjer gitt for hver kategori.

Kurset avsluttes med å gi informasjon om at det er en enkel innføring i informa-

sjonssikkerhet og at det på ingen måte er dekkende for alt helsepersonell ved Ahus bør vite om temaet. Det belyses at helsepersonell selv bør sette seg inn i lover og regler som berører ens eget arbeid. I dette kurset var det fokus på hva helsepersonell har lov til og ikke, men ikke bakgrunn for hvorfor de ulike punktene utgjør en cyberrisiko.

6.1.3 Informasjonssikkerhetskurs for ledere

Ahus har et eget program som heter Ahus lederskole. Hensikten med dette lederkurset er å gi opplæring til avdelingsledere om den fagkunnskapen de trenger for å utføre sitt arbeid. Det holdes da et kurs der personvern og informasjonssikkerhet slås sammen. Kurset holdes fysisk i et audotorium over tre timer og holdes av informasjonssikkerhetslederen på sykehuset. Det foregår en gang i året og presenteres temaer som omhandler digitalisering, hjemmebasert behandlinger, risikovurderinger, hvordan bevisstgjøre ansatte ved å gi tips og triks. HR avdelingen registrerer hvor mange som tar kurset, men det er ikke obligatorisk så det er ikke pålagt med ny gjennomføring dersom den ansatte ikke kunne delta.

6.1.4 Program for sikkerhetsmåneden

Hver oktober gjennomføres sikkerhetsmåneden på Ahus. Det lages et eget program som skal rette søkelyset mot informasjonssikkerhet i helseforetaket. Aktivitetene er tilpasset alle nivåene i organisasjonen og skal bidra til kompetanseheving. Det tilbys et e-læringskurs kalt «En trygg hverdag» under hele sikkerhetsmåneden. Formålet med kurset var å styrke den ansattes digitale sikkerhetskultur. Kurset tok 15 minutter å gjennomføre og var valgfritt å ta.

Figur 6.2: Figuren viser hvor mange som gjennomførte e-læringskurs i sikkerhetsmåneden fordelt på ulike år.

Dette kurset var en revidert utgave av kurset som ble utviklet i 2021. Figuren viser en markant nedgang i antall personer som fullførte mellom 2021 til 2022. Årsaken til denne nedgangen mener Ahus henger sammen med at kurset var uforandret og at det var krevende å markedsføre. Det var i tillegg en travel høst på sykehuset som gjorde det utfordrende for helsepersonell å gjennomføre. En annen faktor var at det kun var påkrevd det første året, men ikke det andre. Kurven er foreløpig nullet i 2023 fordi at sikkerhetsmåneden ikke er før i oktober.

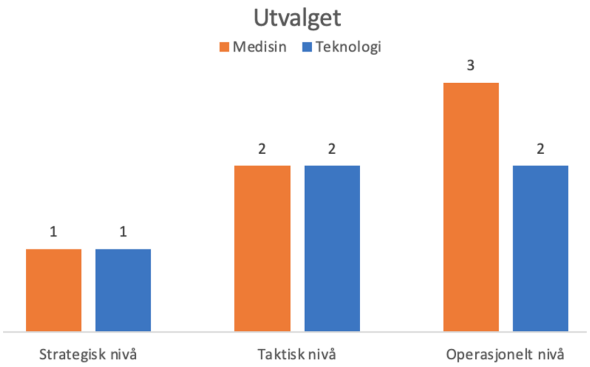
Andre aktiviteter i sikkerhetsmåneden bestod av følgende:

- Sykehusledelsen deltok på en beredksapsøvelse på Norwegian Cyber Range over to dager.
- Refleksjonsspørsmål ble sendt til avdelingsledere hver mandag i hele sikkerhetsmåneden. Der det ble belyst et tema som avdelingen kunne reflektere over på divisjonsledermøter, avdelingsmøter og seksjonsmøter. Totalt fire temaer ble inkludert; to om taushetsplikt, et om bilder og filmopptak av helsepersonell, og ett om personell som har tilgang til store mengder data.
- Avdelingsledere fikk utdelt en quiz på 10 spørsmål som skulle gjennomføres på avdelingsmøter eller seksjonsmøter. Vinneren av quizen mottok en premie
- En fagdag ble arrangert for å belyse internt arbeid med informasjonssikkerhet. Det ble fokusert på behov helseforetaket har innen informasjonssikkerhet og utfordringer i dette arbeidet.
- Fagrelatert innhold ble delt gjennom sosiale medier og informasjonstavler lokalt på sykehuset for å spre kunnskaper.
- Klinikkene ble anbefalt å publisere innlegg i nyhetsbrev der helsepersonell diskuterer sikkerhetsrelaterte dilemmaer og hvordan de ble løst. I tillegg ble avdelingsledere bedt om å stille krav om at ansatte gjennomfører e-læringskurset.

6.2 Deskriptiv statistikk

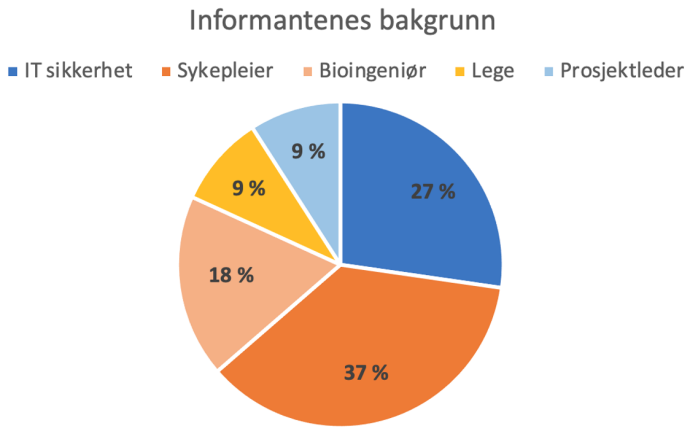
Gjennom de kvalitative intervjuene er det innhentet omfattende informasjon fra alle nivåer i organisasjonen. Nedenfor presenteres først et utvalg av de deskriptive resultatene som er nødvendig for å kartlegge rutiner for opplæring og mulighetene for å anvende det nye opplæringskonseptet. Resten av resultatene vil inkluderes i den sosio–tekniske analysen som presenteres senere i kapittelet.

6.2.1 Utvalget



Figur 6.3: Figuren viser det totale utvalget i studien.

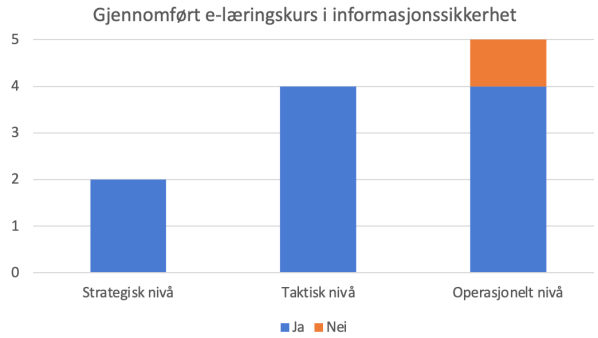
Figuren viser at totalt 11 informanter deltok under de kvalitative intervjuene. Det strategiske nivået består av informanter som har sentrale roller i arbeidet med informasjonssikkerhet og pasientsikkerhet. Informantene på det taktiske nivået representeres av rådgivere innenfor tilsvarende fagfelt. På operativt nivå inkluderes informanter som arbeider på døgnseksjoner, poliklinikk og med e-helse. Totalt 10 av 11 informanter arbeider med fagutvikling og utforming av prosedyrer og regnes å være nøkkelpersonell for denne undersøkelsen. Figuren nedenfor viser en fordeling over hvilke ekspertise informantene har.



Figur 6.4: Figuren viser de ulike yrkesgruppene som ble inkludert i undersøkelsen.

Fem av informantene tilhører kategorien teknologi, mens de resterende seks tilhører medisin.

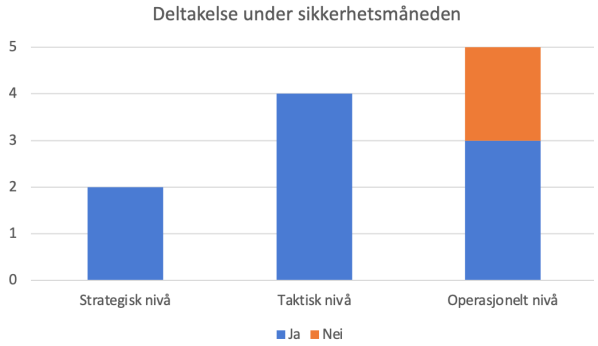
6.2.2 Nyansattkurs i informasjonssikkerhet



Figur 6.5: Antall informanter som har gjennomført nyansattkurs i informasjonssikkerhet

Figuren viser at totalt 10 av 11 personer har gjennomført nyansattkurset til tross for at det er obligatorisk. Bakgrunn for det var at vedkommende ikke hadde fått informasjon om at det måtte gjennomføres.

6.2.3 Deltagelse under sikkerhetsmåneden



Figur 6.6: Figuren viser hvor mange som deltok under sikkerhetsmåneden.

Totalt 9 av 11 deltok under sikkerhetsmåneden i form av deltakelse på fagdag og/eller møter knyttet til informasjonssikkerhet. To informanter kunne ikke delta som følge av at de ikke kunne forlate avdelingen grunnet behandlingsansvar for pasienter.

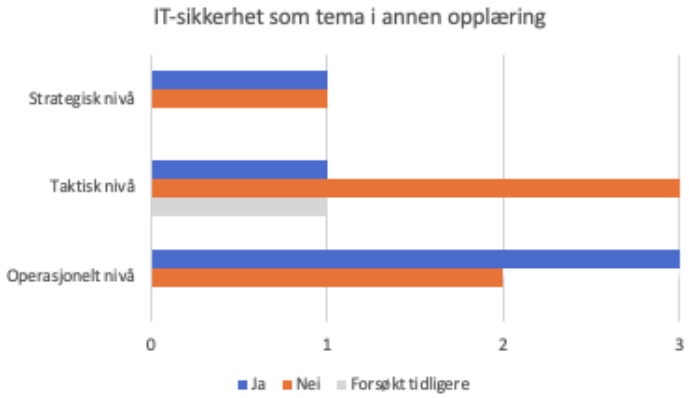
6.2.4 Tilbud om innføring i Informasjonssikkerhet

Figur 6.7: Figuren viser hvor mange som har fått innføring i informasjonssikkerhet.

På strategisk nivå utføres det kontinuerlig tiltak for kompetanseheving i informasjonssikkerhet. Det gis innføring i kunnskaper om risikobildet, trusselvurderinger og nødvendige sikkerhetstiltak. På taktisk nivå er det kun informanter som arbeider med teknologi som oppgir at de har deltatt på foredrag om sikkerhet. På operativt nivå derimot har to informanter fått en innføring der den ene deltok på to møter arrangert av sikkerhetsrådgivere, mens den andre fikk muntlige råd av en kollega.

6.2.5 Inkludering av IT-sikkerhet i andre prosedyrer

Flere av informantene har hatt ansvar for å utvikle opplæringsprogrammer knyttet til sin fagekspertise. Siden fåtallet har fått grundig opplæring i informasjonssikkerhet, ble det spurt om de selv har inkludert slik teori i prosedyrene de har utformet.



Figur 6.8: Figuren viser hvor mange som har inkludert IT-sikkerhet som tema i annen opplæring.

Totalt 5 av 11 nevner å ha inkludert aspekter av informasjonssikkerhet i andre opplæringsprogram. På strategisk og taktisk nivå har det blitt innlemmet i lederkurs. På operativt nivå derimot har det blitt inkludert i opplæringer for kvalitetssystemer og interne kurs for nyansatte både på medisinske og tekniske avdelinger.

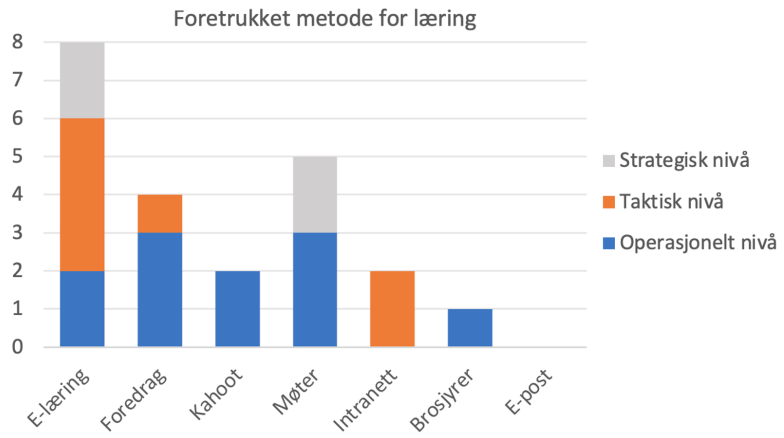
6.2.6 Obligatorisk opplæring i IT-sikkerhet

En metode for å sikre kontinuerlig progresjon av opplæring i informasjonssikkerhet kunne vært at ledelsen stiller krav til obligatorisk gjennomførelse. Det er imidlertid svært delte meninger om dette tiltaket.

Figur 6.9: Figuren viser hvor mange som synes at opplæring i IT-sikkerhet burde vært obligatorisk.

På strategisk nivå mener en informant at det ikke er behov for obligatorisk opplæring grunnet kostnad-nytte effekten. Det argumenteres med at kurset må gi stor nok gevinst at de tjener på å tilby det. Det påpekes at dataangrep ikke skyldes mangel på kunnskaper, men heller tekniske sårbarheter i systemkomponenter. En annen informant mener det ikke er hensiktsmessig å stille strenge krav til kliniske avdelinger grunnet økt arbeidsbelastning, men at det burde vært ett årlig kurs som var pålagt. På taktisk nivå er det delte meninger om behovet for å stille strenge krav. 50 prosent mener det er ugunstig grunnet økt arbeidsbelastning, mangel på tid, og behovet for å fokusere på pasientsikkerhet. Den andre halvdelen observerer stadig betydelige avvik i informasjonssikkerhet, og mener derfor det er nødvendig med obligatorisk opplæring. Det nevnes at klinikere ofte bortprioriterer valgfrie tiltak og at det må pålegges for at det skal bli gjennomført. På operativt nivå derimot, er det kun en person som mener at det stilles for mange krav fra før av. Resten av informantene, inkludert de som arbeider på døgnseksjoner, nevner at det er nødvendig for at kliniske avdelinger skal prioritere det.

6.2.7 Foretrukket metode for opplæring



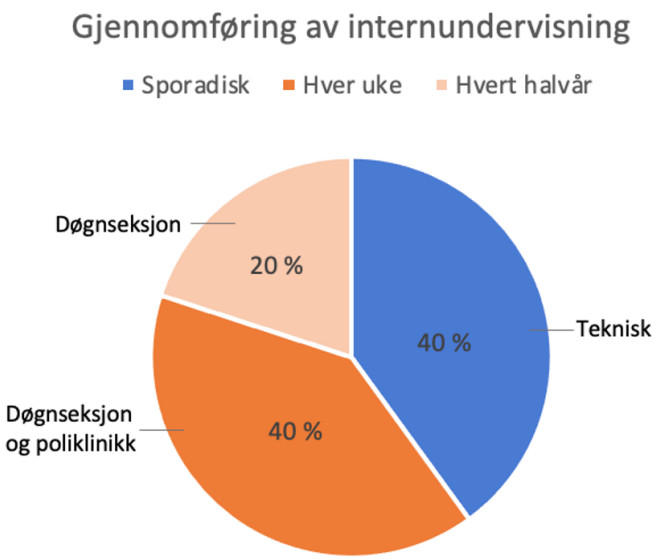
Figur 6.10: Figuren viser hvilke metoder som er foretrukket for kunnskapsheving.

Figuren viser en variasjon i hva informantene foretrekker av opplæring. Informantene hadde mulighet til å velge flere metoder av interesse. På strategisk nivå foretrekkes e-læringskurs eller gjennom møtevirksomhet. På taktisk nivå foretrekker majoriteten e-læring da helsepersonell kan utføre kurset når de selv har tid fremfor å tilby fysiske kurs som ingen dukker opp på. Informantene antar at klinikere ikke har ressurser til å delta på fysisk klasseromsundervisning eller presentasjoner, men at det kunne vært en idé å publisere innlegg på intranett. Kun en på dette nivået mener likevel det er mulig å gjennomføre fysisk undervisning. På operativt nivå derimot, er det kun to som foretrekker e-læring grunnet tidsbegrensninger i hverdagen. Flertallet nevner spesifikt at e-læring ikke er å foretrekke da det virker uinteressant og ofte blir sett på som «enda en ting å gjøre». Utdeling av brosjyrer i papirform foretrekkes av en informant da helsepersonell ofte leser slikt materiell på vaktrommet. Flere nevner at foredrag virker spennende da det legger til rette for interaksjon, refleksjon og diskusjon. Det er også behov for å benytte metoder som skaper konkurranse, er gøy og som samtidig gir læring. Disse informantene hadde erfaring med Kahoot og synes dette er et godt verktøy egnet for å skape engasjement. Det nevnes spesifikt at innlegg på intranett og e-poster med vedlegg ikke er effektivt da helsepersonell sjeldent sjekker disse kanalene, og at kortere møter som i vaktskiftet er mer aktuelt.

6.2.8 Kartlegging av internundervisning på operasjonelt nivå

En forutsetning for å kunne realisere opplæringskonseptet, er at det kan utføres i praksis. Det er derfor vesentlig å innhente rutiner for gjennomføring av internundervisning for å kartlegge om dette er en arena som kan benyttes i arbeidet med opplæring i informasjonssikkerhet.

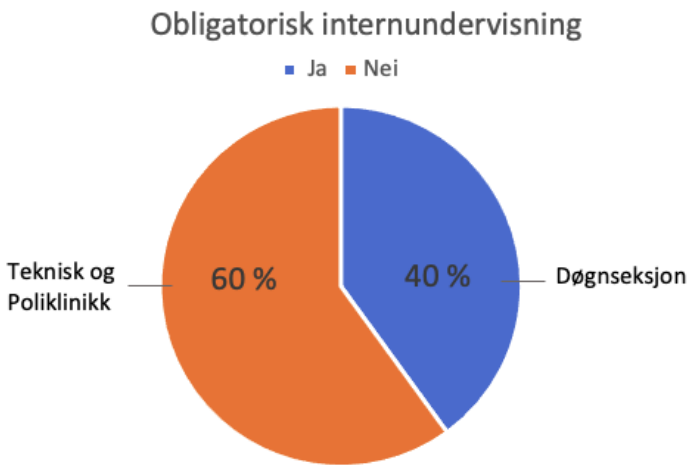
Frekvens for gjennomføring



Figur 6.11: Figuren viser hvor ofte de operasjonelle avdelingene gjennomfører internundervnisning.

Informantene fra de tekniske avdelingene utgjør 40 prosent. De gjennomfører sporadisk internundervisning basert på tilgjengelige ressurser og ved behov. Agendaen styres blant annet av personell som melder interesse for et tema, men også av fagansvarlig som har et eget opplegg. Arenaen benyttes ofte for å gjennomgå avtaler, programvarer og pasientsikkerhet. 40 prosent av informantene fra de medisinske avdelingene har ukentlige internundervisninger. På poliklinikken planlegges innholdet av en komité som arbeider med å sette sammen en agenda. På døgnseksjonen har helsepersonell faste fagdager hver tirsdag, en time før kveldsvakt. Denne undervisningen holdes av leger, og er et samarbeid av fagutviklingssykepleiere på flere medisinske avdelinger. Arenaen benyttes for å belyse problemstillinger, dele erfaringer, samt skape diskusjon og refleksjon. Avdelingen har i tillegg egne fagdager som gjennomføres opptil fire ganger i året. Av de resterende informantene som tilhører døgnseksjon nevner 20 prosent at det settes av fire til seks dager hvert halvår med lik internundervisning for alle på avdelingen. Det velges opptil fire temaer der en kan komme med ønsker til hva en vil lære mer om. Andre ganger styres innholdet av registrerte avvik og observasjoner av hva avdelingen har behov for. I tillegg til denne internundervisningen arrangeres det hvert år en større akuttmedisinsk øvelse som inkluderer fem stasjoner med ulike caseøvelser. På alle døgnseksjonene styres innholdet av ønsker fra helsepersonell eller fagansvarlige.

Obligatorisk internundervisning



Figur 6.12: Figuren viser hvor mange som har obligatorisk internundervisning

Informantene fra tekniske avdelinger oppgir at internundervisningen ikke er obligatorisk. I poliklinikken er heller ikke internundervisningen obligatorisk til tross for at den holdes ukentlig. Ansatte deltar ettersom hva de har tid til, og møter opp dersom de synes innholdet høres spennende ut. På døgnseksjonene er internundervisningen obligatorisk og nøye planlagt seks måneder i forveien. Det legges inn i turnusen slik at alle vet de skal møte opp, noe som også er nødvendig for at alle skal få muligheten til å delta. Siden personell tas ut puljevis, vil det alltid være ressurser på avdelingen. Informantene hevder det ikke er særlig utfordrende å gjennomføre fysisk undervisning på døgnseksjoner grunnet god organisering og koordinering av ressurser.

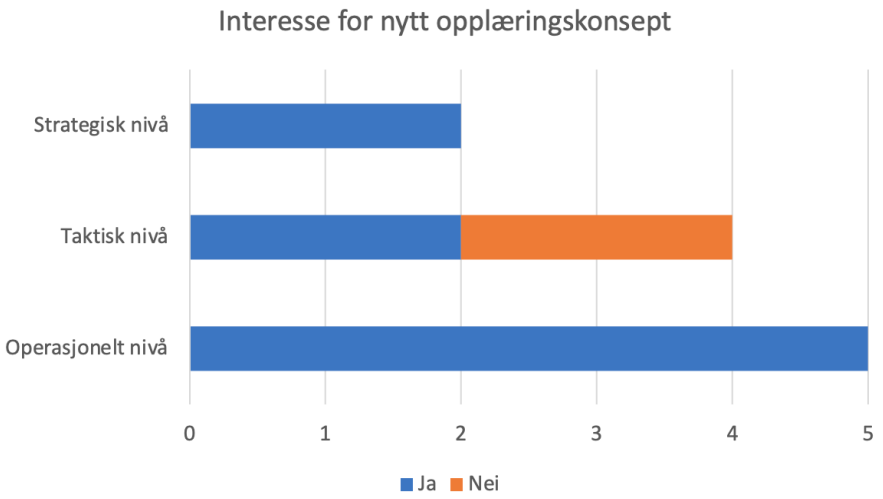
Motivasjon for opplæring og inkluderering av informasjonssikkerhet

Alle informantene på operativ avdeling oppgir at det er god kultur for internundervisning og at ansatte generelt er motiverte for å delta. Internundervisningen er også betalt, noe som bidrar til å skape motivasjon. En informant mener tiden som er satt av for undervisningen er en faktor for om det virker motiverende. Siden internundervisningen på deres avdeling kun varer en time før ens opprinnelige vakt, utgjør det ikke stor forskjell og dermed er det svært overkommelig. Andre svarer det er god kultur for å lære om nye fagområder så lenge det fremstilles på en spennende måte i forveien. Alle informantene mener det er gode muligheter for å inkludere informasjonssikkerhet som tema på internundervisninger. I tillegg er det flere som mener dette er mulig å gjennomføre flere ganger i året utenom aktivitetene i sikkerhetsmåneden. En forutsetning for at dette skal bli vellykket er imidlertid at opplæringen skreddesys informantenes arbeidsoppgaver og at de får bistand av eksterne ressurser. To informanter kunne allerede på dette tidspunk-

tet tenke seg å invitere ressurser fra HR avdelingen for å holde et foredrag om informasjonssikkerhet.

6.2.9 Interesse for nytt opplæringskonsept

Til nå har resultatene presentert karteleggende data om rutiner relatert til opplæring, internundervisning og interesse for informasjonssikkerhet. I de neste delkapitlene presenteres konkrete synspunkter om et nytt opplæringskonsept.



Figur 6.13: Figuren viser hvor mange som er interessert i et nytt opplæringskonsept

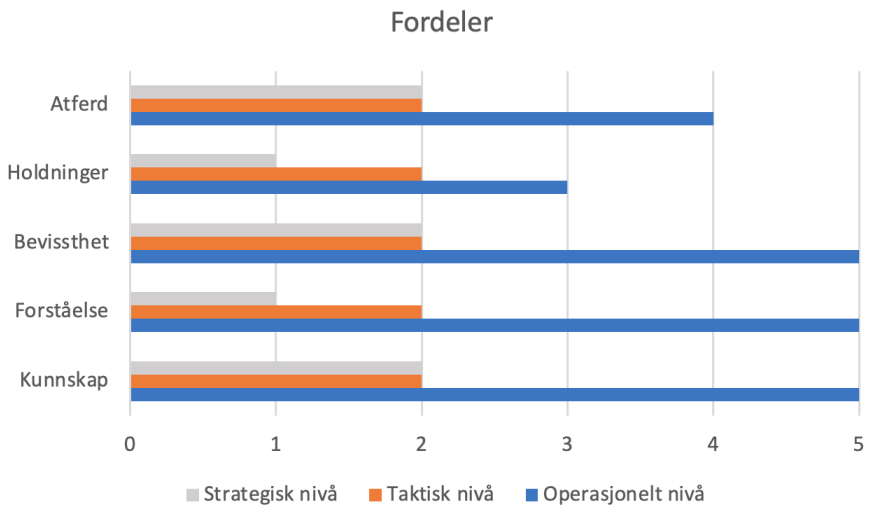
På strategisk nivå hevder informantene at det kunne vært hensiktsmessig iverksette opplæringskonsept som både inkluderer informasjonssikkerhet og pasientsikkerhet. Det påpekes imidlertid at det handler om klinikkens viljestyrke til å tilrettelegge for disse endringene, men at det potensielt kan ha en god effekt dersom konseptet aksepteres på operativt nivå. En av informantene belyser at muligheten for å inkludere informasjonssikkerhet i pasientsikkerhet ble diskutert i sykehusledelsen under sikkerhetsmåneden, uten at ytterligere konklusjon ble fremlagt. Det har lenge vært et ønske med bedre koordinering mellom begge fagområdene grunnet økt digitalisering.

På taktisk nivå er det imidlertid svært ulike meninger. Informantene som til daglig arbeider med informasjonssikkerhet tror dette kan være en effektiv metode for kunnskapsheving blant klinikere. Det legges vekt på at det er vesentlig å skreddersy opplæringen til hver avdeling basert på deres arbeidsoppgaver og systemene som håndteres. Det er først da en kan få økt forståelse og utbytte av et slikt program. Informantene som arbeider med pasientsikkerhet mener imidlertid at konseptet ikke er anvendbart i praksis. Det er sterke meninger om at fagfeltene ikke kan slås sammen i én opplæring og at tiltakene i sikkerhetsmåneden bør være

tilstrekkelig. En annen informant mener opplæringskonseptet blir faglig ukorrekt da helsepersonell må fokusere på pasientbehandling, men at det kan være aktuelt å tilby et valgfritt kurs som klinikere kan utføre dersom de ser behovet for å øke kunnskaper i sikkerhet. Det begrunnes med at brudd på informasjonssikkerhet ikke forekommer så ofte, og at det er Sykehuspartner som har ansvar for å ivareta dette. Et sitat fra en informant lyder som følge: «Å inkludere informasjonssikkerhet i pasientsikkerhet, er som om vi skulle ha inkludert brannsikkerhet i pasientsikkerheten, og det gjør vi ikke».

På operativt nivå er utelukkende alle positive til metoden for opplæring. For avdelinger som ikke har obligatorisk internundervisning, påpekes det at å skape engasjement vil bli essensielt. Andre hevder konseptet er anvendbart i praksis og at det er et nødvendig tiltak grunnet dagens trusselbilde. Det legges vekt på at informasjonssikkerhet er komplekst, og at det er vanskelig å forstå teoretiske konsepter. Teorien må derfor kunne skreddersys til hver enkelt avdeling dersom opplæringen skal være suksessfull.

6.2.10 Fordeler ved nytt opplæringskonsept

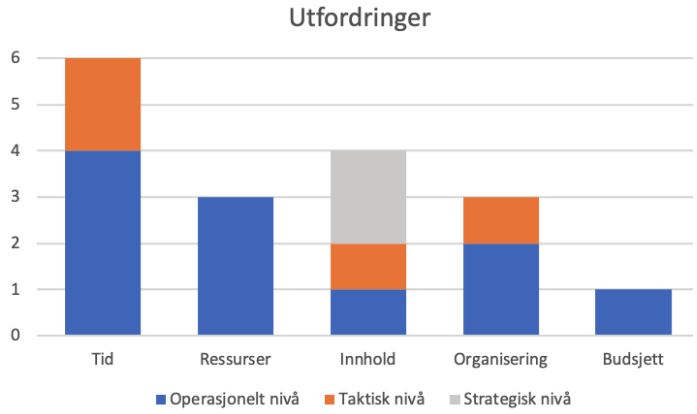


Figur 6.14: Figuren viser hvilke fordeler informantene synes det er ved ny opplæringsmetode

På bakgrunn av at to informanter ikke foretrekker opplæringskonseptet, er det kun 9 av 11 som svarte på spørsmålet. Undersøkelsen viser dog at informantene ser flere fordeler ved opplæringskonseptet. Majoriteten hevder at metoden skaper rom for diskusjon og refleksjon når fagkunnskaper kombineres, særlig dersom det gjennomføres på internundervisninger. En informant påpekte også at fagkunnskapen mest sannsynlig huskes bedre når informasjonssikkerhet ses i sammenheng med profesjonsrelatert arbeid. En annen informant påpeker at ordet vil spre seg

dersom oppleget er bra, noe som potensielt kan øke sannsynligheten for at flere ønsker å delta. Alle nevner at opplæringen kan bidra til å øke forståelse og kunnskaper om på dagens trussel- og risikobilde, noe som over tid kan bidra til å endre sikkerhetsatferd og holdninger. De nevner også at det kan være enklere å ta mer bevisste valg dersom informasjon formidles på en enkel måte.

6.2.11 Utfordringer ved konseptet



Figur 6.15: Figuren viser hvilke utfordringer som kan oppstå ved ny opplæringsmetode

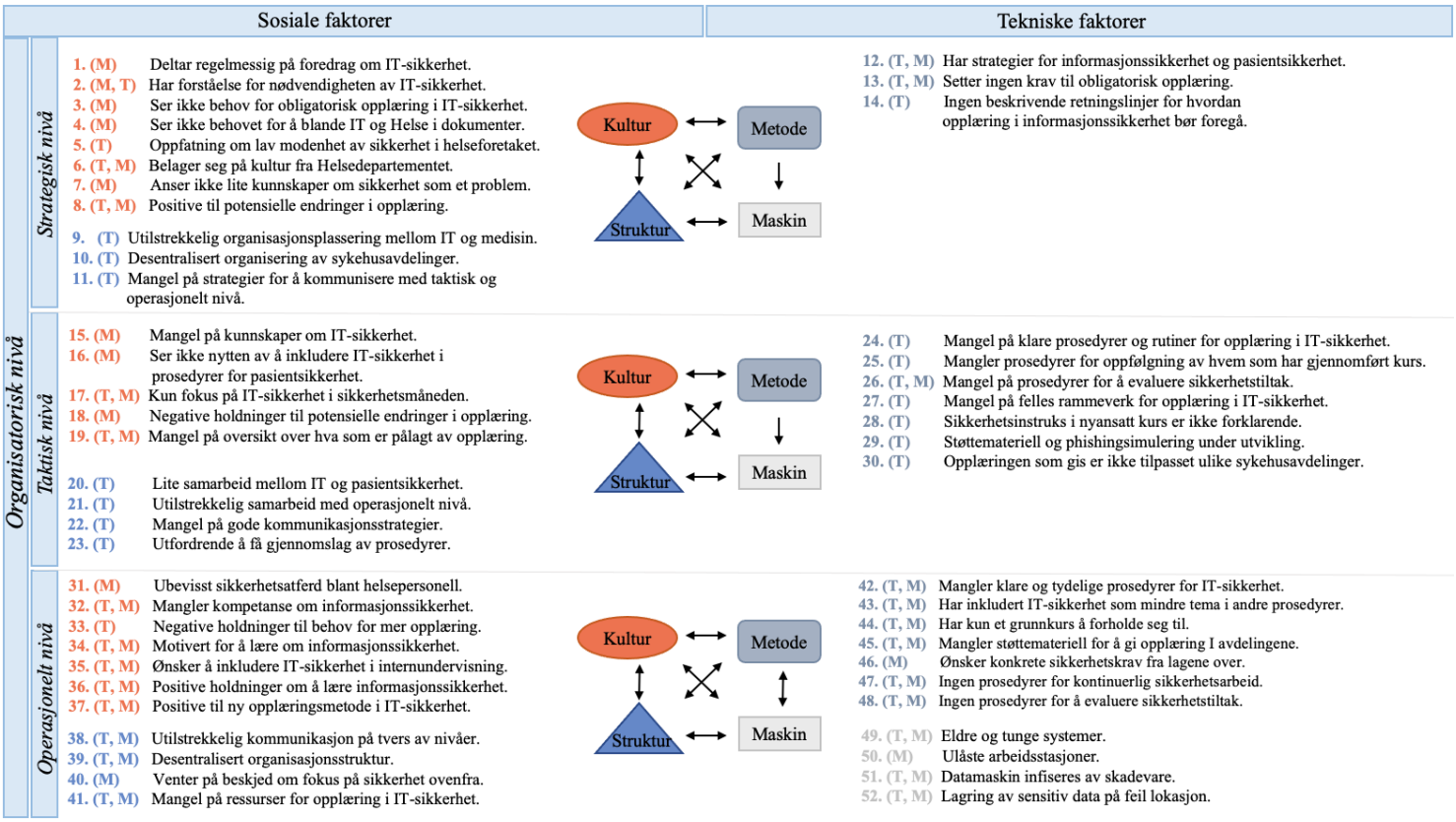
For å identifisere potensielle utfordringer ble informantene bedt om å liste alle situasjoner som kan påvirke gjennomførbarheten i praksis. På taktisk og strategisk nivå uttrykkes det utfordringer relatert til å tilpasse innholdet da omfanget kan bli for omfattende. Det følges nasjonale programmer for opplæring i pasientsikkerhet, og det å finne en innfallsvinkel for informasjonssikkerhet i allerede innarbeidede planer kan være utfordrende. Hadde Helsedepartementet hatt mer fokus på informasjonssikkerhet kunne det vært enklere å kombinere fagområdene i praksis. Flere nevner at det kan være krevende å tilpasse innholdet til hver enkelt sykehusavdeling. Innhold som passer en avdeling trenger ikke nødvendigvis å passe en annen, basert på hva avdelingen tilbyr av helsetjenester. Ikke fordi det ikke er gjennomførbart, men fordi det vil kreve ekstra samarbeid med ressurspersoner fra ulike avdelinger. Uten et samarbeid vil en kun anta hva som trengs i praksis, og det er ikke sikkert det stemmer overens med realiteten.

På operativt nivå nevner særlig helsepersonell at utfordringen kan være dersom det planlegges opplæring og ingen kommer som følge av mangel på tid eller sykefravær. Dersom det ikke er pålagt og tilpasset turnus kan det hende det blir bortprioritert. Dersom det arrangeres i arbeidstiden er det også en risiko for at personell ikke dukker opp da dagene er uforutsigbare med tanke på arbeidsbelastning. To informanter påpeker at det er veldig enkelt å løse dersom det tilpasses turnu-

sen, men at det vil kreve budsjett. Informantene som arbeider på døgnseksjon ser imidlertid ikke på dette som en utfordring, men påpeker at det kan være slik for andre. Det nevnes i tillegg at det kan være en utfordring om avdelingsledere og fagutviklere ikke prioriterer sikkerhet da det ofte er dem som planlegger og organiserer opplæringer. Andre utfordringer relateres til mangel på eksterne ressurser som kan bistå med materiell og innhold. Dersom innholdet blir for generelt og ikke tilpasses avdelingene, kan helsepersonell fort miste interessen og motivasjon.

6.3 Sosio-teknisk analyse

Dette kapittelet presenterer en sosio-teknisk analyse som skal bidra å skape et beslutningsgrunnlag for en potensiell gjennomførbarhet i helseforetaket. Til tross for at majoritet av informantene var positive til det nye opplæringskonseptet, er det nødvendig å utføre en samlet vurdering basert på organisatoriske styrker og svakheter som ble identifisert under de kvalitative intervjuene. Figuren nedenfor viser den første sosio-tekniske analysen der alle identifiserte styrker og svakheter fremlegges.



Figur 6.16: Sosio-teknisk analyse av de tre organisatoriske nivåene i helseforetaket før vekting.

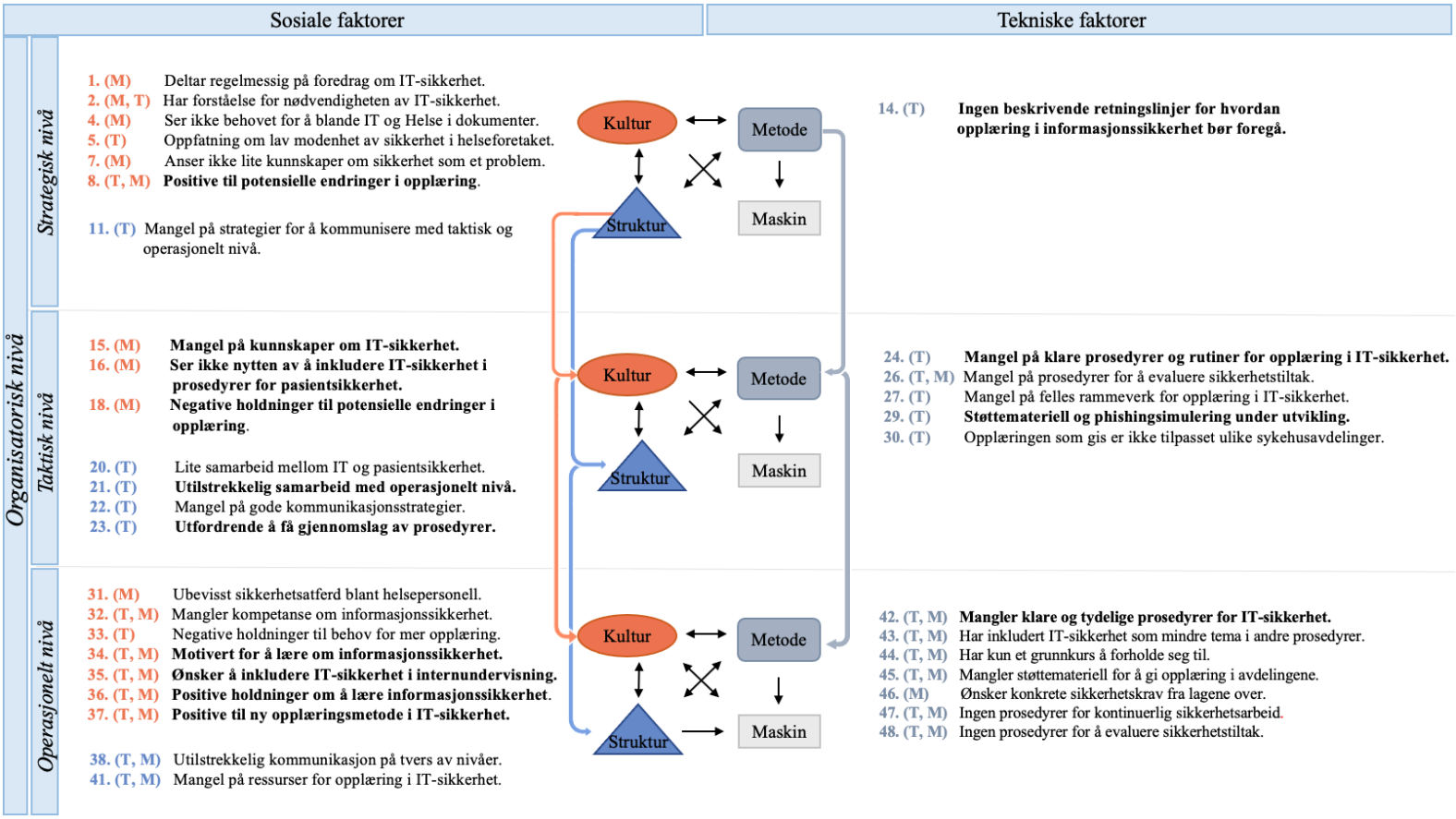
Som figuren viser, er analysen svært omfattende. Totalt 52 ulike sosio-tekniske faktorer er identifisert fordelt på de tre organisatoriske nivåene i helseforetaket. Pilene mellom de fire submodulene illustrerer hvordan domenene påvirker hverandre. Analysen benytter også kategoriene for pseudonymisering for å tydeliggjøre faktorenes opphav, der *T* står for teknologi og *M* står for medisin. For å fremheve de faktorene som er av størst betydning for beslutningsgrunnlaget, ble hver av de vektet basert på høy, middels og lav påvirkning som beskrevet i kapittel 3. Tabellen under viser hvilken vekt de ulike faktorene fikk tildelt.

Vekten av de identifiserte faktorene					
Sosiale faktorer					
Strategisk nivå	**Skår**	**Taktisk nivå**	**Skår**	**Operasjonelt nivå**	**Skår**
1.	2	15.	3	31.	2
2.	2	16.	3	32.	2
3.	1	17.	2	33.	2
4.	2	18.	3	34.	3
5.	2	19.	1	35.	3
6	1	20.	2	36.	3
7.	2	21.	3	37.	3
8.	3	22.	2	38.	2
9.	1	23	3	39.	1
10.	1			40.	1
11.	2			41.	2
Tekniske faktorer					
Strategisk nivå	**Skår**	**Taktisk nivå**	**Skår**	**Operasjonelt nivå**	**Skår**
12.	1	24.	3	42.	3
13.	1	25.	1	43.	2
14.	3	26.	2	44.	2
		27.	2	45.	2
		28.	1	46.	2
		29.	3	47.	2
		30.	1	48.	2
				49.	1
				50.	1
				51.	1
				52.	1
Total vekt av 31 sosiale faktorer = 63.7 %					
Total vekt av 21 tekniske faktorer = 36.3 %					

Figur 6.17: Vekting av identifiserte faktorer

Figuren viser totalt 31 sosiale faktorer og 21 tekniske. De sosiale faktorene utgjør 63.7 prosent av den totale vekten, mens de tekniske utgjør 36.3 prosent. Distribusjonen viser allerede her en overvekt av sosiale faktorer som spiller størst rolle for realiseringen av opplæringskonseptet. Basert på disse resultatene, presenteres en ny analyse i figur 6.18. Analysen inkluderer kun faktorer med skår to eller mer da det er de som er av størst betydning. Det betyr likevel ikke at faktorer med skår

en er ubetydelig i den store sammenhengen, men de er eliminert for å rette fokus mot de faktorene som anses å ha størst betydning når det skal tas en beslutning.



Figur 6.18: Resultatet av den sosio-tekniske analysen etter vekting

Figuren viser en endring i pilene mellom domenene og de ulike strategiske lagene. Svakheter eller styrker i ett lag kan påvirke laget under eller over seg. Hovedfunn fra analysen presenteres her, men diskuteres i neste kapittel.

6.3.1 Kulturelle faktorer

På strategisk nivå får informantene jevnlig opplæring i informasjonsikkerhet i form av foredrag og på møter. De har god forståelse for hvordan sikkerhetsbrudd kan påvirke helseforetaket på ulike nivå, men mener at menneskelige faktor ikke utgjør den største årsaken for at helseforetak blir utsatt for angrep. Fokuset på opplæring i informasjonssikkerhet er derfor størst i sikkerhetsmåneden og det gis minimalt med retningslinjer til taktiske og operative nivåer utover dette. På taktisk nivå hevder informantene at det er utfordrende å nå helsepersonell på operativt nivå når de forsøker å rette fokus mot informasjonssikkerhet. De har tidligere forsøkt å publisere innhold på intranet, sykehusbloggen og e-post, men opplever at

informasjonen ikke når ut til målgruppen. Innenfor medisin ser ikke informantene behovet for ytterlig opplæring da helsepersonell allerede gjennomfører nyansattkurs og deltar under sikkerhetsmåneden. I tillegg anses det ikke som relevant å inkludere aspekter av informasjonssikkerhet i opplæring for pasientsikkerhet. Et direkte sitat av en informant lyder som følgende: «Å inkludere informasjonssikkerhet i pasientsikkerhet ville vært som å inkludere brannsikkerhet. Vi vet at det kan brenne, men det skjer nesten aldri». Ringvirkningen av disse momentene resulterer i at fokuset på sikkerhet blir mindre og at denne kulturen videreføres nedover i helseforetaket. Informanter på operativt nivå hevder på sin side at de får minimalt med informasjon om sikkerhet, og at det derfor er utfordrende å prioritere slik opplæring. Alle informanter har imidlertid nevnt at de er åpne for opplæring dersom de får mer informasjon fra øvre hold. Flere har selv nevnt et ønske om å øke kunnskaper om hvordan et dataangrep kan påvirke ens egen avdeling, og hvordan en selv kan mitigere dataangrep.

6.3.2 Strukturelle faktorer

Informantene uttrykker at en desentralisert organisasjonsstruktur medfører at avdelinger opererer individuelt og at de former egne prosedyrer istedenfor å arbeide sammen. Dette igjen fører til utilstrekkelig kommunikasjon og mer rom for misoppfatninger i helseforetaket. Divisjonene for pasientsikkerhet og informasjonssikkerhet er adskilt på strategisk nivå, og organisasjonsplasseringen gjør det utfordrende å arbeide tverrfaglig. Denne organisatoriske strukturen er gjennomgående i hele helseforetaket. På taktisk nivå medfører dette at det skapes antakelser om at helsepersonell er for opptatt med pasientbehandling og at det er ekstremt utfordrende for de som arbeider på døgnseksjon å prioritere opplæring i informasjonssikkerhet. I tillegg nevnes det at de ikke har kompetanse til å vurdere viktigheten av informasjonssikkerhetsopplæring. Når helsepersonell på døgnseksjonen får spørsmål om dette nevnes det at de ikke har fått beskjed om at det skal gjøres. Flere har svart at det aldri har vært en utfordring å lære om nye temaer da internundervisningen ligger i turnusen og er planlagt nøye seks måneder frem i tid. Dette viser at både medisinsk og teknologisk personell på høyere nivå har en feiloppfatning om hva som er mulig i praksis. På operativt nivå er det en tydelig usikkerhet om hvilke prosedyrer som skal følges og hvem som skal kontaktes for ekstern bistand. Informanter på taktisk nivå i informasjonssikkerhet nevner at personell på deres avdeling tar på seg slike oppdrag, men nevner at ingen har sendt en slik bestilling til i dag. Dette viser at det er utilstrekkelig kommunikasjon på tvers av lagene, noe som påvirker det totale sikkerhetsarbeidet betraktelig.

6.3.3 Metodiske faktorer

På strategisk nivå mangler det retningslinjer for hvordan helseforetaket kan tilby kontinuerlig opplæring i informasjonssikkerhet. Det stilles kun krav til at hver operative avdeling skal lære sine ansatte om informasjonssikkerhet, men ikke hvordan

opplæringen skal gjennomføres. Dette påvirker de underliggende nivåene i arbeidet med å utvikle prosedyrer for opplæring. På taktisk nivå har det blitt nevnt at det er utfordrende å få gjennomslag av e-læringskurs etter at de er utviklet. Det refereres til et eksempel der Helse Sør-Øst forsøkte å lage opplæringsmateriell, men fikk avslag som følge av at det ble for mye innhold og tok lang tid å gjennomføre. I slike tilfeller oppstår det en intern uenighet mellom taktisk og strategisk nivå som igjen påvirker hvordan opplæringen til operativt nivå er. Når taktisk nivå på sin side har laget opplæringsprogram for det de mener er anvendbart for sykehusavdelinger, men får avslag fordi sykehusledelsen mener det ikke er anvendbart i praksis, ender det opp med at de ikke får laget et kurs som gir den verdien de ønsker fordi de må komprimere innhold. Det nevnes imidlertid at Ahus holder på å utvikle nytt støttemateriell til kliniske avdelingsledere som de kan benytte for å gi opplæring i informasjonssikkerhet lokalt på avdelingene. Senere dette året skal også Sykehuspartner starte phishingsimulering for å trene ansatte på å identifisere falske e-poster. Det viser imidlertid at tiltak er på vei til å bli iverksatt.

6.3.4 Forutsetninger for et suksessfult resultat

På taktisk nivå påpekes det at det kreves et tverrfaglig team som kan bistå med dette prosjektet. Identifisering av behov for opplæring er vesentlig, samt å tilby materiell skreddersydd hver avdeling. Det anses imidlertid å være enkelt å iverksette en tilsvarende prosjektgruppe da det er god kultur for det på Ahus. Ofte samles fageksperter fra ulike felt og arbeider mot et felles mål. Det påpekes at det ikke er hensikt i å utvikle et opplæringsprogram som ikke er anvendbart i praksis og at det derfor kreves et godt samarbeid mellom klinikere og taktiske avdelinger. Informanter på operativt nivå legger til at det uansett vil være behov for bistand fra eksterne ressurser slik at de kan presentere faglig innhold uavhengig om det opprettes et prosjekt. På bakgrunn av at internundervisning gjerne foregår over flere dager, vil det være behov for at ressurspersonen er tilgjengelig i en lenger periode. Strategisk nivå legger til at avdelingsledere snart får informativt støttemateriell de kan benytte dersom det er utfordrende å innhente eksterne ressurser innenfor ønsket tidsrom. Flertallet mener avdelingsledere og fagutviklere må skape et fokus på sikkerhet og lokalt engasjement for å sikre at helsepersonell ønsker å delta. Eksempelvis kan det utføres ved å gi små drypp av sikkerhet på seksjonsmøter, statusmøter, i vaktskiftet og lignende. Det legges vekt på at en må bruke arenaer der en kan nå ut til flere samtidig, og at internundervisninger ofte er en god arena. Tre informanter mener det også er behov for at personell på strategisk og taktisk nivå bidrar å skape fokus på informasjonssikkerhet da det er enklere å prioritere det dersom det kommer ovenfra. Fra kliniske avdelingsledere vil det kreve nøye planlegging og koordinering av ressurser da ansatte må tas ut i puljer for å delta. Til tross for behovene mener likevel 9 av 11 informanter at opplæringskonseptet er anvendbart med god organisering.

Kapittel 7

Diskusjon

Forrige kapittel presenterte hovedfunnene fra casestudiet og den sosio-tekniske analysen. Dette kapittelet diskuterer hvilken betydning disse resultatene har for opplæringskonseptet og drøfter det opp mot litteratursøket som ble gjennomført.

7.1 Deskriptive resultater

De deskriptive resultatene viser at majoriteten er positive til et nytt opplæringskonsept, og at helsepersonell er motivert til å lære om informasjonssikkerhet. Til tross for at de operative avdelingene utfører internundervisning ulikt i henhold til undervisningsmetode og frekvens, påpeker alle at det er rom for å inkludere informasjonssikkerhet på disse dagene. For å fange interesse er det dog essensielt å skreddersy innholdet til hver enkelt avdeling basert på deres arbeidsoppgaver, systemer som benyttes og informasjon som skal beskyttes. Det faktum at kliniske informanter er interessert i å lære mer om informasjonssikkerhet gir overraskende resultater. Sammenlignet med litteratur presentert av Conventry et al., (2020), Branley-Bell et al., (2021) og Warner (2022), nevner ikke informantene i denne studien at stressfaktor, arbeidsbelastning eller mangel på tid hinder gjennomførelsen for en slik type opplæring. Enkelte nevner likevel at det kan ha en påvirkning dersom opplæringen foregår i arbeidstiden eller i perioder med stor pågang i sykehusavdelingene. Noen eksempler som ble dratt opp var under COVID-19 pandemien, da helsepersonell var overarbeidet og hadde lite ressurser. I slike situasjoner vil det naturligvis bli mer utfordrende å gjennomføre opplæring. Til tross for positive resultater er det likevel nødvendig å analysere helseforetaket på et dypere nivå da organisatoriske faktorer kan påvirke suksessen ved innføring av en ny arbeidsprosess.

7.2 Perspektiver ved den sosio-teknisk analysen

Som de sosiale og tekniske faktorene illustrerte, er spesialisthelsejentesten svært kompleks. Helseforetaket består av mange nøkkelspillere som er med i beslut-

ningsprosessen og det må i tillegg tas høyde for etablerte rutiner og prosedyrer. For å besvare forskningsspørsmålet: « Hvilke forutsetninger bør oppfylles for at norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet?», er det nødvendig å analysere sammenhengen mellom de sosiale og tekniske faktorene for å identifisere de konkrete behovene som må tilfredsstilles.

Den sosio-tekniske analysen viser at distribusjonen gir en overvekt av sosiale faktorer. Det vil si at de sosiale faktorene har større betydning for om opplæringskonseptet er anvendbart i praksis, sammenlignet med de tekniske. Det betyr likevel ikke at de tekniske faktorene er ubetydelig, men at de ikke er overrepresentert i denne analysen. Resultatene i forrige kapittel illustrerer hvordan faktorene i de ulike domenene påvirker hverandre. For at informasjonssikkerhet skal kunne innlemmes i opplæring for pasientsikkerhet, er det essensielt at det skapes et fokus på informasjonssikkerhet på alle nivåer i helseforetaket. Det henger sammen med at helsepersonell sjeldent fokuserer på informasjonssikkerhet med mindre det gis beskjed fra øvre ledelse. Et tiltak for å sikre deltagelse på opplæringer, kunne vært å kreve at det blir obligatorisk. Informantene har imidlertid ulike synspunkt for en slik tilnærming. Flertallet på operativ avdeling påpeker at det er nødvendig for at helsepersonell skal prioritere det, mens på strategisk nivå hevder enkelte at kostnaden er høyere enn nytteeffekten. I tillegg er det flere andre kurs som står i kø for å bli obligatorisk og terskelen for å få gjennomslag på et slikt tiltak er derfor høy. Riksrevisjonen (2021) avdekket i sin undersøkelse at helsepersonell i Norge ikke bestandig gjennomfører opplæring til tross for at det er obligatorisk. Dette viser at det ikke alltid er en løsning med påkrevde tiltak, samtidig som det fremhever viktigheten av behovet for å etablere god sikkerhetskultur.

Resultatene fra forrige kapittel viser også at det å skape engasjement for tematikken er en forutsetning for at helsepersonell ønsker å delta. Gjennom intervju påpeker operativt personell at de ikke inkluderes tilstrekkelig i arbeidet med informasjonssikkerhet, og at de kun får retningslinjer for hva de har lov til og ikke. Det fører til at de ikke forstår bakgrunn for hvorfor sikkerhetstiltakene iverksettes. Ringvirkningen av dette er at fagfeltet oppleves tungt og at sikkerhetsatferden ikke nødvendigvis forbedres. For å skape interesse, er det derfor essensielt å anvende eksempler fra deres arbeidshverdag slik at klinikere enklere kan relatere fagkunnskapene til egne erfaringer og praksis.

Til tross for behovet for økt fokus på sikkerhet, identifiserer analysen også utilstrekkelige kommunikasjonsstrategier på tvers av helseforetaket. Slike strukturelle faktorer påvirker sikkerhetskulturen direkte da personell på taktisk nivå ikke når frem til klinikere, og at klinikere på sin side hevder de ikke får nok informasjon. Medisinsk personell på taktiske avdelinger hevder imidlertid at det er enkelt å nå frem til helsepersonell på morgenmøter, seksjonsmøter og i vaktskiftet. Slike arenaer kan benyttes for å videreformidle kunnskaper. Dette viser at det

både er utfordringer med kommunikasjon med livået under i organisasjonsnivået, men også på samme nivå. Uheldig organisasjonsplassering holder personell adskilt, noe som fører til at det interne samarbeidet svekkes. Resultatet blir at fageksperter ikke finner relevante metoder for å nå ut til målgruppen. Gode kommunikasjonsstrategier er en nøkkelfaktor for suksess i arbeidet med opplæring i informasjonssikkerhet i spesialisthelsetjenesten. I likhet med forskning utført av Branley-Bell et al. (2021), viser analysen at personell på taktisk nivå opplever helsepersonell som svært opptatt og at de ikke har tid til opplæring i informasjonssikkerhet da det er mye å gjøre på avdelingen. Resultatene fra intervjuene i denne casestudien, viser derimot at flere avdelinger, selv travle døgnseksjoner evner å organisere, koordinere og planlegge kurs. En sykepleier må nødvendigvis ikke velge mellom internundervisning eller direkte pasientbehandling da det løses ved at det tilbys fagdager utenfor planlagt arbeidstid slik at ansatte tas ut puljevis. En kliniker nevnte at utfordringen ikke var stressnivå og arbeidsmengde, men lite fokus på sikkerhet fra ledelsen. To av informantene var allerede etter intervju villig til å kartlegge muligheten for å inkludere informasjonssikkerhet på sine internundervisninger. Det viser at det er behovet for å styrke kommunikasjonsstrategiene på tvers av nivåene er vesentlig for om sikkerhetsarbeidet skal lykkes. Schneider Wirth (2021) påpeker også viktigheten av dette samarbeidet i sin studie.

Utilstrekkelig kommunikasjon og fokus på sikkerhet kan også påvirke utforming av prosedyrer da det oppstår en risiko for at prosedyrer ikke utvikles eller at de ikke er anvendbare i praksis. Når det er sagt, viser forskning utført av Pollini et al. (2022) at utforming av tekniske prosedyrer i seg selv heller ikke er tilstrekkelig for opplæring. Dersom det ikke foreligger en god kultur med fokus på sikkerhet, vil prosedyrene miste verdi på grunnlag av at den ikke blir formidlet til målgruppen. Dette viser hvordan kultur, struktur og metode påvirker hverandre, og ikke minst nødvendigheten av samspillet mellom disse faktorene.

På grunnlag av fleksibiliteten som kommer med opplæringskonseptet, er det i utgangspunktet vesentlig at det foreligger noe faglig materiale om informasjonssikkerhet. De fleste kliniske avdelingslederne er utdannet helsepersonell og det kan derfor være krevende dersom de ikke har innhold å inkludere i opplæringen. Fleksibiliteten gjør at avdelingene selv kan velge den formen for informasjonsdeling de vil. Det betyr at opplæringen både kan gjennomføres som en fysisk presentasjon, gjennom quiz eller refleksjonsspørsmål. Mangel på støttemateriell kan imidlertid gjøre det krevende å komme i gang med opplæringen da det ikke er noe fagstoff å formidle. En kan miste motivasjon for å prioritere informasjonssikkerhet, noe som igjen kan påvirke sikkerhetsatferd og utsette maskinene for sårbarheter. Etablering av prosedyrer er derfor en teknisk faktor av stor betydning for gjennomførbarheten av opplæringskonseptet. Konseptet legger kun til rette for at informasjonssikkerhet skal komme på agendaen, men presenterer ikke konkret innhold som skal inkluderes. Det er fordi at trussel- og risikobildet endrer seg, og at avdelingene

kan ha ulikt behov for opplæring. Å ha en fast agenda som alle må følge kan derfor bli for bindende, noe som igjen kan påvirke deres motivasjon for gjennomførelse. Det at informasjonsmateriale er under utvikling er imidlertid en positiv faktor som kan bidra å veie opp for gjennomførbarheten. Informativt støttemateriell er under produksjon og vil snart overleveres til operative avdelingsledere. I løpet av året vil det også tas i bruk simuleringsverktøy for å trene helsepersonell på å bli teknisk motstandsdyktig for dataangrep. Dette gir gode forutsetninger for at avdelingene selv kan legge til rette for relevant opplæring i fremtiden.

Manglende prosedyrer og rutiner for opplæring av informasjonssikkerhet, og mangel på kompetanse om sikkerhet generelt gjør at helsepersonellets sikkerhetsatferd i stor grad påvirker datamaskinene på avdelingene. Det fører til at helsepersonell lar datamaskinen stå ulåst, noe som kan påvirke både konfidensialitet, integritet og tilgjengelighet dersom en uautorisert aktør får aksess til denne datamaskinen. Ubevist sikkerhethetsatferd fører også til store avvik som observeres av personell på taktisk nivå. Eksempelvis lagrer mange sensitiv forskningsdata på fellesområder fremfor lokalt på sin egen datamaskin. Dette fører til at annet helsepersonell som ikke skal ha tilgang til denne dataen få innsyn. Manglende opplæring kan også føre til at helsepersonell klikker på lenker eller vedlegg på e-poster og laster ned skadevare. Selv om det på strategisk nivå påpekes at det finnes sterke mekanismer som filtrerer og blokkerer slik aktivitet, er det gjennom forskning vist at trusselaktører benytter avanserte teknikker for å snike seg forbi disse sikkerhetsbarrierene (Rizzoni et al., 2022).

På bakgrunn av de presenterte faktorene, kan en si at forutsetninger som det å tilrettelegge for god kommunikasjon, øke fokus på sikkerhet, skreddersydd opplæring og etablere et godt samarbeid på tvers av nivåene er vesentlig for om norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet. Flere av funnene i denne masteroppgaven er støttet av internasjonal forskning. Det kan tyde på at utfordringene knyttet til opplæring i spesialisthelsetjenesten er et globalt problem. Som litteratursøket presenterte, foreligger det minimal forskning om en kombinasjon av opplæring i pasientsikkerhet og informasjonssikkerhet. En sentral informant har imidlertid nevnt at det er gode muligheter for å etablere et tverrfaglig samarbeid gjennom en prosjektgruppe som kan arbeide med disse problemstillingene. I tillegg har helsepersonell vist åpenhet for å teste et nytt opplæringsforløp. Ahus har dedikerte informasjonssikkerhetsrådivere som tilbyr bistand til opplæring. Det foreligger derfor gode forutsetninger for at opplæringskonseptet kan testes i praksis. Selv om intensjonen med denne arbeidsmetoden er å forbedre dagens tiltak, betyr det ikke at alle endringer er effektive. Det er først etter en lenger testperiode at en kan konkludere om effektiviteten står til forventningene.

7.3 Generalisering av resultater

Til tross for at 9 av 11 var positive til å inkludere informasjonssikkerhet i opplæring av pasientsikkerhet, er det svært essensielt å påpeke at resultatene per nå ikke kan generaliseres. De fleste informantene som ble inkludert regnes å være nøkkelpersonell for oppgavens formål. Det var kun en informant som ikke hadde erfaring med utvikling av opplæringsprosedyrer på operativt nivå. På strategisk og taktisk nivå kan en argumentere med at utvalget var representativt på grunnlag av at antall personer med ansvar er langt mindre sammenlignet med operativt nivå. I tillegg har de sentrale arbeidsoppgaver innenfor kvalitet – og forbedringsarbeid i både informasjonssikkerhet og pasientsikkerhet for hele helseforetaket. Slik organisasjonskartet presenterer i figur 2.2, består sykehusledelsen av personell som arbeider innen finans, HR og lignende. Å inkludere slike informanter var ikke aktuelt da de verken arbeider med pasientsikkerhet eller informasjonssikkerhet. Resultatet av å ikke inkludere dem fører dog til at det oppstår en skeivhet i utvalget når en sammenligner de organisatoriske nivåene. Likevel gjøres det en antagelse om at det mer hensiktsmessig å ha en skjevhet sammenlignet med å inkludere utvalg som ikke faller innunder riktig målgruppe. På operativt nivå derimot, kan ikke en si at utvalget er representativt. Det henger sammen med at Ahus har om lag 12000 ansatte og 5 operative klinikere er derfor ikke nok til å representere hele helseregionen eller Ahus lokalt. Samtidig er dette en casestudie der det blir gjennomført kvalitative intervjuer. En slik forskningsmetode skaper begrensninger på hvor mange informanter en kan inkludere på en kort prosjektperiode.

Om resultatene er pålitelige og valide, kan imidlertid diskuteres. Det faktum at flere av de identifiserte faktorene støttes av forskningslitteratur er med på å øke påliteligheten og validiteten av resultatene. Det er fordi at flere forskere har kommet frem til de samme resultatene når det gjelder utfordringer og hva det er behov for på tvers av de organisatoriske nivåene i helseforetaket, i arbeidet med informasjonssikkerhet. Det som imidlertid kan være med på å redusere påliteligheten og validiteten av resultatene, er at selve konseptet for opplæringen ikke er identifisert gjennom litteratur. Det betyr likevel ikke at en kan konkludere med at det aldri er gjort, men siden det ikke ble identifisert under litteraturstudien kan det tyde på at det mangler forskning på feltet. På den andre siden kan det være svakheter i søkeordene som gjorde at relevant litteratur ikke ble identifisert. En tredje faktor kan henge sammen med at det kan være utfordrende å få nøyaktige resultater av kvalitative intervjuer da svarene til informantene kan endre seg over tid eller at andre informanter med andre perspektiver skaper helt ulike resultater. Basert på eksisterende litteratur er det imidlertid gode holdepunkter for å konkludere med at det trengs ytterligere forskning på feltet for å innhente pålitelige og valide resultater som kan bidra til generalisering.

7.4 Svakheter i casestudien

På grunnlag av at utvalget ikke kan generaliseres på nåværende tidspunkt, ville det vært vesentlig å inkludere flere informanter. På den andre siden var dette utfordrende å få til da operativt personell måtte delta under arbeidstiden sin eller ulønnet på fritiden. Tre informanter endret tidspunkt grunnet akutte situasjoner i avdelingen. To av informantene fant et nytt tidspunkt, mens den tredje ikke hadde muligheten likevel. På den ene siden gjenspeiler dette også utfordringer som er identifisert i resultatene. Det kreves planlegging og organisering for at det skal være mulig å inkludere flest mulig. Samtidig var det flere som sa seg villige til å delta på starten av prosjektperioden, men merket at det var mer travelt på sykehuset enn forventet gjennom våren.

En annen svakhet kan relateres til oppgavens omfang og innhentede resultater. Til tross for at det besvares på problemstillingen, var det flere faktorer som kunne vært verdt å diskutere. Eksempelvis gjelder dette at enkelte informanter viste uttrykte dårlige holdninger til sikkerhetskultur. Siden det var fåtallet, og at holdningene ikke gjentok seg på andre nivåer, veiet ikke det nok for å inkludere i diskusjonen. Det er likevel verdt å nevne at slike holdninger også påvirker om tiltak kan settes i verk.

Kapittel 8

Konklusjon

Økt digitalisering har bidratt til å effektivisere helsetjenester, men bruk av teknologi har også åpnet for sikkerhetsrelaterte utfordringer. Undersøkelser viser at helsepersonell mangler kunnskaper om informasjonssikkerhet og at menneskelige sårbarheter stadig utnyttes av trusselaktører under dataangrep. Behovet for kompetanseheving i hvordan helsepersonell kan beskytte informasjonsverdier er derfor stort. Forskning viser imidlertid at opplæringen som gis i dag ofte blir bortprioritert som følge av at pasientsikkerheten er i fokus. Utilstrekkelig sikkerhetskultur gjør det i tillegg utfordrende å holde fokuset på informasjonssikkerhet i klinikken.

Dette masterprosjektet presenterte derfor et nytt opplæringskonsept som kan bidra til å rette fokuset på informasjonssikkerhet og sikre en mer kontinuerlig opplæring sammenlignet med dagens tiltak. Gjennom kvalitative intervju og en sosioteknisk analyse av opplæringskonseptet, har dette casestudiet besvart hvilke forutsetninger som bør oppfylles for at norske sykehus kan inkludere informasjonssikkerhet som en del av opplæringen i pasientsikkerhet. Faktorer som manglende fokus på sikkerhet, utilstrekkelig kommunikasjon og samarbeid, samt mangel på prosedyrer kan gjøre det utfordrende å gjennomføre opplæring i dag. Likevel viser resultatet at Ahus har gode forutsetninger for å styrke sikkerhetskulturen på grunnlag av prosedyrer som er under utvikling og motivasjon blant helsepersonell. Det trengs imidlertid et samspill mellom alle nivåer i helseforetaket for å sikre fremgang og suksessfulle resultater. Selv om undersøkelsen også har gitt lovende resultater, foreligger det ingen grunnlag for generalisering på nåværende tidspunkt. I likhet med internasjonale studier, viser også denne undersøkelsen at det er behov for ytterligere forskning for å sikre pålitelige og valide resultater. Denne studien danner imidlertid grunnlag for videre arbeid med muligheter for gjennomføring av et pilotprosjekt.

8.1 Videre arbeid

De presenterte resultatene danner grunnlag for videre arbeid og det er mulig å videreføre dette prosjektet på flere måter. Eksempelvis kan det gjøres ytterlige-

re forskning ved å inkludere et representativt utvalg med informanter fra både strategiske, taktiske og operative divisjoner. I masteroppgaven var det et fokus på å inkludere nøkkelpersonell som på et vis arbeidet med fagutvikling og som har erfaringer med å utarbeide prosedyrer. Selv om flere også arbeidet klinisk, kunne det ha vært en idé å inkludere flere klinikere. Det vil si helsepersonell som aktivt arbeider med direkte pasientbehandling for å innhente deres perspektiver og vurderinger. Det er også mulig å inkludere flere helseforetak i Helse Sør-Øst for å innhente mer pålitelige og valide resultater, samt danne et større grunnlag for generalisering.

En annen måte å videreføre prosjektet på kan være å starte et pilotprosjekt for å teste konseptet i praksis. Ved å inkludere noen av de operative avdelingene som var med i casestudien, kan en raskere innhente erfaringer som kan bidra til kvalitetsforbedringer. Disse avdelingene bestod både av døgnseksjoner, poliklinikk og digitale seksjoner, noe som kan gi en god variasjon i testmiljøet. Innføring av den nye opplæringsmetoden vil kreve endringer i nåværende arbeidsprosesser. I hvor stor grad en avdeling er i stand til å takle endringer avhenger både av ressurser de har til rådighet, deres kompetanse om temaer, ansvarsfordeling, hvilke teknologier de bruker i sitt daglige arbeid og lignende. Ved å gjennomføre et praktiske eksperimenter, kan en imidlertid innhente raske resultater (Itryggehender, 2023). Et forslag kan være å benytte aksjonsforskning der forskeren tett arbeider med de ulike avdelingene for å studere utfordringer, aktivt identifisere og iverksette løsninger, og ikke minst å evaluere effekten av opplæringen. Det er først da en kan konkludere med om konseptet bidrar til økt effektivisering av opplæring i informasjonssikkerhet. Resultatet av prosjektet kan eksempelvis presenteres under sikkerhetsmåneden på Ahus. Dette kan bidra til å skape åpenhet rundt erfaringer, belysning av utfordringer og ikke minst rom for diskusjon og refleksjon.

En tredje måte å videreføre prosjektet på, kan være å utforske problemstillinger på nasjonalt nivå. Både internasjonal forskning og resultater fra denne undersøkelsen viser at helsemyndigheter ofte må inkluderes for å etablere den helhetlige sikkerhetskulturen i helsesektoren. Personell som arbeider på strategisk nivå i et helseforetak belager seg ofte på føringer utarbeidet av høyere myndigheter. Kulturen på det nivået videreføres og forplantes på nivåene lenger ned i helseforetaket. Når helsemyndighetene ikke har stort fokus på å formidle opplæring informasjonssikkerhet, er det enkelt for de som arbeider med pasientsikkerhet å vurdere det som mindre relevant. Sett i lys av innhentede resultater, er det flere som nevner at dette kan være en medvirkende faktor til hvorfor sykehusledelsen ikke legger et større press på opplæring i informasjonssikkerhet. På operasjonelt nivå har det imidlertid vist seg at det er ønskelig at det stilles krav ovenfra for at endringer skal skje i praksis. I fremtiden kunne det derfor vært svært interessant å involvere helsedirektoratet og andre myndigheter som legger føringer for hvordan pasientsikkerheten kan ivaretas ved å fokusere inkludere informasjonssikkerhet for å styrke sikkerhetskulturen i hele Helse-Norge.

Referanseliste

Agboola, S. O., Bates, D. W., & Kvedar, J. C. (2016). Digital Health and Patient Safety. JAMA, 315(16), 1697–1698. https://doi.org/10.1001/jama.2016.2402

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in human behavior, 49, 567-575.

Ali, K. A., & Alyounis, S. (2021). CyberSecurity in Healthcare Industry. International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 695-701, doi: 10.1109/ICIT52682.2021.9491669.

Akershus Universitetssykehus. (2022a). Forskning og innovasjon.
Hentet fra https://www.ahus.no/fag-og-forskning/forskning-og-innovasjon

Akershus Universitetssykehus. (2022b). Instruks for administrerende direktør – Helse Sør-Øst RHF 2022 – 2024. Hentet fra https://helse-sorost.no/Documents /Ledelse/Instruks%20for%20administrerende %20direkt%C3%B8r.pdf

Akershus Universitetssykehus. (2023a). Om oss: Menneskelig nær – Faglig sterk. Hentet fra https://www.ahus.no/om-oss

Akershus Universitetssykehus. (2023b). Organisasjonskart – Ahus. Hentet fra https://www.ahus.no/Documents/Om-oss/Organisasjonskart-Ahus.pdf

Alder, S. (2022). The Hipaa journal – Editorial: Why do criminals target medical records? Hentet fra https://www.hipaajournal.com/why-do-criminals-target-medical-records/

Berntsen, H. (2022). Nasjonalt senter for e-helseforskning. Hvor trygge er egentlig våre helsedata? Hentet fra https://ehealthresearch.no/nyheter/2022/hvor-trygge-er-egentlig-vare-helsedata

Bruvoll, J.A., Thuv, A., Enemo, G. (2020).Håndtering av IKT-sikkerhetshendelsene i Helse Sør-Øst og fylkesmannsembetene - en vurdering. Hentet fra https://ffi-

publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2719/20-01560.pdf

Branley-Bell, D., Coventry, L., & Sillence, E. (2021, June). Promoting cybersecurity culture change in healthcare. In The 14th PErvasive Technologies Related to Assistive Environments Conference (pp. 544-549).

Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43, 1-12.

Chinthapalli, K. (2017). The hackers holding hospitals to ransom. BMJ, 357.

Chua, J., PMP, CAP, CISSP & 40S(D) task group. (2021). Cybersecurity in the Healthcare Industry. Hentet fra https://podiatrym.com/pdf/2021/7/Chua821web.pdf.

Cohen, G. (2021). Throwback Attack: A ransomware attack shuts down the Parkview Medical Center IT networks at the worst time. Hentet fra www.industrialcybersecuritypulse.com/facilities/throwback-attack-a-ransomware-attack-shuts-down-the-parkview-medical-center-it-networks-at-the-worst-time/

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Coventry, L., Branley-Bell, D., Sillence, E., Magalini, S., Mari, P., Magkanaraki, A., & Anastasopoulou, K. (2020). Cyber-risk in healthcare: Exploring facilitators and barriers to secure behaviour. In HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings (pp. 105-122). Cham: Springer International Publishing.

Cowan, E. (2023). Australia ECU University. Search Engines and Library Databases Google Scholar. Hentet fra https://ecu.au.libguides.com/search-engines/google-scholar

Dameff, C. J., Selzer, J. A., Fisher, J., Killeen, J. P., & Tully, J. L. (2019). Clinical Cybersecurity Training Through Novel High-Fidelity Simulations. The Journal of emergency medicine, 56(2), 233–238. https://doi.org/10.1016/j.jemermed.2018.10.029

Datatilsynet. (2015). Anonymisering av personopplysninger Hentet fra https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/anonymisering-veileder-041115.pdf

Datatilsynet. (2019). Hva er personopplysning? Hentet fra

https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/

Direktoratet for e-Helse. (2020) Strategi for digital sikkerhet i helse- og omsorgssektoren Vurdering av behov og innretning (IE-1064). Oslo: Directorate of e-health. Hentet fra https://www.ehelse.no/publikasjoner/strategi-for-digital-sikkerhet-i-helse-og-omsorgssektoren-vurdering-av-behov-og-innretning

Direktoratet for eHelse. (2022) – Normen. Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren – Versjon 6.1. Hentet fra https://www.ehelse.no /normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren/

Direktoratet for eHelse. (2023a) – Normen. Veileder i personvern og informasjonssikkerhet i forskningsprosjekter Versjon 2.1. Hentet fra https://www.ehelse.no//normen /normen-dokumenter/Veileder-i-personvern-og-informasjonssikkerhet-i-forskningsprosjekter/

Direktoratet for eHelse. (2023b). Plan for realisering av Nasjonal e-helsestrategi versjon 0.95. Hentet fra https://www.ehelse.no/strategi/nasjonal-e-helsestrategi-for-helse-og-omsorgssektoren/Plan%20for%20realisering%20av%20Nasjonal%20e-helsestrategi.pdf

Erasmus University Library. (2023). Doing the literature review: Using a database thesaurus. Hentet fra https://libguides.eur.nl/informationskillslitreview/thesaurus

Etterretningstjenesten. (2023). Fokus 2023 – Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer. Hentet fra https://www.etterretningstjenesten.no/ //publikasjoner/fokus/fokus-norsk/Fokus2023%20-%20NO%20-%20Weboppslag%20v3.pdf/

Flott, K., Maguire, J., and Phillips, N. (2021). Digital safety: the next frontier for patient safety. Future Healthcare Journal, 8(3), e598.

Finklea K. (2017). Congressional Research Service. Dark Web. Hentet fra https://a51.nl/sites/default/files/pdf/R44101%20(1).pdf

Frich, J. (2011). Kvalitet, kvalitetsforbedring og pasientsikkerhet. Hentet fra Universitetet i Oslo – Det medisinske fakultet //https://www.med.uio.no/studier/ressurser /fagsider/klok/info-fagplanutvalg/kvalitet-og-pasientsikkerhet.html

Gerring, J. (2004). What is a case study and what is it good for?. American political science review, 98(2), 341-354.

Ghaljaie, F., Goli, H., Naderifar, M. (2017). Snowball Sampling: A purposeful methos of sampling in qualitative research. Hentet fra https://sdme.kmu.ac.ir/ article_90598_3632edfb2e97c38d73c0bdea8753195c.pdf

Greenhalgh, T., Peacock, R. (2023). Information in practice. Effectiveness and efficiency of search methods in systematic reviews of complex evidence: audit of primary sources. Hentet fra https://www.bmj.com/content/bmj/331/7524/1064.full.pdf

Helsedirektoratet. (2018). Definisjoner. Hentet fra https://www.helsedirektoratet.no/rundskriv/pasient-og-brukerrettighetsloven-med-kommentarer/alminnelige-bestemmelser/definisjoner#7be9628e-6b9b-4cd3-97f2-dd2bf1f880ff

Helsedirektoratet. (2019). Nasjonal handlingsplan for pasientsikkerhet og kvalitetsforbedring 2019 – 2023. Hentet fra https://www.helsedirektoratet.no/veiledere/ledelse-og-kvalitetsforbedring-i-helse-og-omsorgstjenesten/Nasjonal%20handlingsplan%20for%20pasientsikkerhet%20og%20kvalitetsforbedring%202019-2023.pdf

Helsedirektoratet. (2023). Pasientsikkerhet og kvalitetsforbedring. Hentet fra https://www.helsedirektoratet.no/tema/pasientsikkerhet-og-kvalitetsforbedring

Helse Sør-Øst. (2023). Om Helse Sør-Øst RHF. Hentet fra https://helse-sorost.no/om-oss#om-helse-sor-ost-rhf

Helse Sør-Øst. (2022). Om Helse Sør-Øst RHF. Hentet fra https://www.helsesorost.no/siteassets/documents/Organisasjonskart/Organisasjonskart.pdf

Helse Sør-Øst. (2023). Organisering av personvern- og informasjonssikkerhetsarbeidet. Hentet fra https://helse-sorost.no/Documents/Informasjonssikkerhet%20og%20personvern/Styringssystem%20for%20informasjonssikkerhet/Regionalt%20styrende%20dokumenter/Styrende/NO-04%20-%20Organisering%20av%20personvern-%20og%20informasjonssikkerhetsarbeidet.pdf

Helsetilsynet. (2020). Kartlegging ved fem virksomheter Hvordan er sykehusene forberedt på IKT-bortfall? Hentet fra: https://www.helsetilsynet.no/globalassets/opplastinger/publikasjoner/rapporter2020/helsetilsynetrapport3_2020.pdf

Hofmann, B. (2013). Ethical challenges with welfare technology: a review of the literature. Science and engineering ethics, 19(2), 389-406.

IEEE. (2023). IEEE Thesaurus Version 1.01. Advancing Technology for Humanity. Hentet fra https://www.ieee.org/content/dam/ieee-org/ieee/web/org/pubs/ieee-thesaurus.pdf

Itryggehender. (2021). Om pasientsikkerhet. Hentet fra i trygge hender 24-7 https://www.itryggehender24-7.no/om-pasientsikkerhet

Itryggehender (2023). Pasientsikkerhetsvisitter. Hentet fra https://www.itryggehender24-7.no/reduser-pasientskader/pasientsikkerhetsvisitter

Itryggehender. (2017). Ledelse av pasientsikkerhet – Hva innebærer det? Hentet fra https://www.itryggehender24-7.no/ledelse-og-kultur/ledelse-av-pasientsikkerhet-hva-innebaerer-det

Kaspersky. (2023). What is Hacking? Hentet fra https://www.kaspersky.no/resource-center/definitions/what-is-hacking

Khiralla, F. A. M. (2020). Statistics of cybercrime from 2016 to the first half of 2020. Int. J. Comput. Sci. Netw., 9(5), 252-261.

Kowalski, S. (1993, August). The SBC model as a conceptual framework for reporting it crimes. In Proceedings of the IFIP TC9/WG9. 6 Working Conference on Security and Control of Information Technology in Society on board M/S Illich and ashore (pp. 207-226).

Kowalski, S. (1994). IT insecurity: A multi-disciplinary inquiry.

Kristensen, M., Muhaisen, S., Pettersen, J., Johansen, E. N. & Sviggum (2023). Norske sykehus trues av russiske hackergrupper. Hentet fra https://www.nrk.no/norge/norske-sykehus-trues-av-russiske-hackergrupper-1.16275175

Pasientjournalforskriften. (2021). Forskrift om pasientjournal (pasientjournalforskriften). Hentet fra https://lovdata.no/dokument/SF/forskrift/2019-03-01-168

Helsepersonelloven. (2022). Lov om helsepersonell m.v. (helsepersonelloven). Hentet fra https://lovdata.no/dokument/NL/lov/1999-07-02-64

Sikkerhetsloven. (2019). Lov om nasjonal sikkerhet (sikkerhetsloven). Hentet fra https://lovdata.no/dokument/NL/lov/2018-06-01-24
Martinsen, H. (2023) – Telenor. Hackere – Slik jobber de. Hentet fra https://www.telenor.no/bedrift/blogg/sikkerhet/hacker/

Martin, G., Martin, P., Hankin, C., Darzi, A., & Kinross, J. (2017). Cybersecurity and healthcare: how safe are we?. Bmj, 358.

McNiff, J. (2013). Action research: Principles and practice. Routledge.

Meld. st. 47 (2009) Samhandlingsreformen, Rett behandling – på rett sted – til rett tid. Hentet fra Hentet fra https://www.regjeringen.no/contentassets/d4f0e16ad32e4bbd8d8ab5c21445a5dc/no/pdfs/stm200820090047000dddpdfs.pdf

Meld. St. 7 (2019-2020)(2019) Nasjonal helse- og sykehusplan 2020 – 2023. Oslo: Det Kongelige Helse – og Omsorgsdepartementet. Hentet fra: https://www.regjeringen.no/contentassets/95eec808f0434acf942fca449ca35386/no/pdfs/stm201920200007000dddpdfs.pdf

NIST (2023). Cyber Attack. Hentet fra https://csrc.nist.gov/glossary/term/Cyber_Attack

NISO. (2021). ANSI/NISO Z39.4-2021 – Criteria for Indexes. Hentet fra https://www.niso.org/publications/z394-2021-indexes

Norsk helsenett (2022) Situasjonsbilde 2022. Hentet fra https://www.nhn.no/om-oss/Personvern- og-informasjonssikkerhet/helsecert/publikasjoner/situasjonsbilde-2022.

NSM. (2023a). Risiko 2023 – Økt uforutsigbarhet krever høyere beredskap. Hentet fra https://nsm.no/getfile.php/1312547-1676548301/NSM/Filer/Dokumenter/Rapporter/Risiko%202023%20-%20Nasjonal%20sikkerhetsmyndighet.pdf

NSM. (2023b). Nasjonal Sikkerhetsmyndighet. Hva er sikkerhetsstyring? Hentet fra https://nsm.no/fagomrader/sikkerhetsstyring/hva-er-sikkerhetsstyring/

NSM. (2023c). Nasjonal Sikkerhetsmyndighet. Sikkerhetskultur. Hentet fra https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/

NTNU. (2023a). Norges tekniske naturvitenskapelige universitet. Søk og finn – Oria. Hentet fra https://i.ntnu.no/oppgaveskriving/sok-og-finn

NTNU. (2023b). Norges tekniske naturvitenskapelige universitet. Computer science (IT). Hentet fra https://www.ntnu.no/blogger/ub-teknologi/en/subject-resources/computer-science-it/

NTNU. (2023c). Norges tekniske naturvitenskapelige universitet. PubMed – En oversikt. Hentet fra https://folk.ntnu.no/janove/medbib/pdf_filer/PubMed%20brukerveiledning.pdf

NTNU. (2023d). Norges tekniske naturvitenskapelige universitet. Avanserte litteratursøk. Hentet fra https://i.ntnu.no/wiki/-/wiki/Norsk/Avanserte+litteraturs%C3%B8k

O'Brien, N., Ghafur, S., & Durkin, M. (2021). Cybersecurity in health is an urgent patient safety concern: we can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management, 26(1), 5-10.

Oftebro, I. (2021). www.digi.no. Sykehus rammet av løspengevirus må avvise pasienter. Hentet fra https://www.digi.no/artikler/sykehus-rammet-av-losepengevirus-

ma-avvise-pasienter/512658

Paloalto Networks. (2023). What are Ransomware Attacks? Hentet fra https://www.paloaltonetworks.com/cyberpedia/ransomware-common-attack-methods

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology Work, 24(2), 371-390.

Politiets Sikkerhetstjeneste. (2023) – PST. Nasjonal trusselvurdering 2023. Hentet fra https://www.pst.no/globalassets/ntv/2023/ntv_2023_nor_web.pdf

Rajamäki, J., Nevmerzhitskaya, J., & . Virág, C. (2018). Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF), 2018 IEEE Global Engineering Education Conference (EDUCON), Santa Cruz de Tenerife, Spain, 2018, pp. 2042-2046, doi: 10.1109/EDUCON.2018.8363488.

Riksrevisjonen. (2021). Riksrevisjonens undersøkelse av helseforetakenes forebygging av angrep mot sine IKT-systemer. Hentet fra https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/undersokelse-av-helseforetakenes-forebygging-av-angrep-mot-sine-ikt-systemer.pdf

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. Digital Health, 8, 20552076221081716.

SIKT. (2023). Hva er personopplysning? Hentet fra https://sikt.no/hva-er-personopplysninger

Schneider, J., & Wirth, A. (2021). Balancing Patient Safety, Clinical Efficacy, and Cybersecurity with Clinician Partners. Biomedical instrumentation & technology, 55(1), 21–28. https://doi.org/10.2345/0899-8205-55.1.21

Sheikh, A., Anderson, M., Albala, S., Casadei, B., Franklin, B. D., Richards, M., Taylor, D., Tibble, H., & Mossialos, E. (2021). Health information technology and digital innovation for national learning health and care systems. The Lancet. Digital health, 3(6), e383–e396. https://doi.org/10.1016/S2589-7500(21)00005-4

Skjelvik, A., & Yang, B. (2022). Information Security Risk for Welfare Technology and Personal Healthcare Devices. pHealth 2022, 165-170.

Spence, N., Bhardwaj,N. M. B. B. S., & Paul III, D. P. (2018). Ransomware in healthcare facilities: a harbinger of the future?. Perspectives in Health Information Management, 1-22.

Sykehuspartner HF. (2022). Årlig melding 2021 til Helse Sør-Øst RHF, Oslo 1. mars. 2022. Hentet fra https://sykehuspartner.no/Documents/Styrem%C3%B8ter/022022/007-2022-1%20-%20%C3%85rlig%20melding%202021%20-%20Sykehuspartner%20HF.pdf

Sykehuspartner. (2022). Økonomisk langtidsplan 2022 – 2025 Sykehuspartner HF Versjon 1.0. Hentet fra https://sykehuspartner.no/Styremter/032021/021-2021-1%20-%20%C38konomisk%20langtidsplan%20Sykehuspartner%20HF%202022%20-%202025.pdf
Swann, C. (2002). Action research and the practice of design. Design issues, 18(1), 49-61.

Suri, H. (2011). Purposeful sampling in qualitative research synthesis. Qualitative research journal, 11(2), 63-75.

The Hipaa Guide. (2023). Examples of phishing attacks in healthcare. Hentet fra https://www.hipaaguide.net/examples-of-phishing-attacks/

Trost, J. E. (1986). Statistically nonrepresentative stratified sampling: A sampling technique for qualitative studies. Qualitative sociology, 9(1), 54-57.

Vinningland, P., NTB. (2023). www.rb.no Russisk hackergruppe truer AHus. Hentet fra https://www.rb.no/russisk-hackergruppe-truer-ahus/s/5-43-1953456

Warner, R. M. (2022). Policy options in the health care sector. Cybersecurity is Patient Safety. Hentet fra https://www.warner.senate.gov/public/_cache/files/f/5/f5020e27-d20f-49d1-b8f0-bac298f5da0b/0320658680B8F1D29C9A94895044DA31.cips-report.pdf

Wasserman, L., & Wasserman, Y. (2022). Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Frontiers in digital health, 4, 862221. https://doi.org/10.3389/fdgth.2022.862221

Whitman, M. E. & Mattford, H. J. (2017). Principles of information security (6. Utg.). Cengage Learning.

White, G. (2009). Strategic, tactical, operational management security model. Journal of Computer Information Systems, 49(3), 71-75.
WHO. (2021). World Health Organization. Globak Patient Safety Action Plan 2021-2030. Hentet fra https://www.who.int/publications/i/item/9789240032705

Witts, J. (2023). Expert Insights. Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know. Hentet fra https://expertinsights.com/insights/healthcare-cyber-attack-statistics/

Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into Phishing

Risk Behaviour among Healthcare Staff. Information, 13(8), 392.

Young, F. W. (1981). Quantitative analysis of qualitative data. Psychometrika, 46, 357-388.

Vedlegg A

Intervjuguide

Dette vedlegget inneholder intervjuspørsmålene som ble brukt som grunnlag for de kvalitative intervjuene. Noen spørsmål var felles for alle mens andre var tilpasset organisatoriske nivå. Først presenteres de spørsmålene som var felles for alle etterfulgt av de spørsmålene som var spesifikke for hvert organisatoriske nivå. For hver av spørsmålene som uttrykker utfordringer spørres det om hvilken påvirkning det har for gjennomføring av det nye opplæringskonseptet. Formålet med det er å danne grunnlag for vektingen i den sosio-tekniske analysen.

Om informanten

- Hvilken avdeling jobber du i?
- Hvilken rolle har du på arbeidsplassen?

Om deres opplæring innen informasjonssikkerhet

- Har du gjennomført nyansattkurs i informasjonssikkerhet?
- Har du tatt noen andre kurs innen informasjonssikkerhet? Hvis ja, hvilke og hvor mange?
- Har du tatt noen andre kurs innen informasjonssikkerhet? Hvis ja, hvilke og hvor mange?
- Deltok du under sikkerhetsmåneden? Hvis ja, hva deltok du på? Hvis nei, hvorfor ikke?
- Hvordan tilbyr deres avdeling opplæring om informasjonssikkerhet til de ansatte? Hvis det ikke gjøres, hva er det som gjør det utfordrende å gi opplæring innen informasjonssikkerhet?
- Hvor ofte gir dere opplæring i informasjonssikkerhet?
- Er det enkelt å gjennomføre i praksis eller ser du noen spesifikke utfordringer?
- Hva trengs av ressurser for at dere kan drive opplæring innen informasjonssikkerhet?
- Har du eller noen på avdelingen inkludert aspekter i informasjonssikkerhet i en annen opplæring?
- Hvordan måler dere effekten av opplæring?
- Hvordan evaluerer dere gjennomgåtte kurs?
- Synes du opplæring i informasjonssikkerhet burde være obligatorisk?
- Det finnes mange måter å øke kunnskaper innen informasjonssikkerhet. Eksempelvis kan en bruke e-læring, delta på foredrag og møter, gjennomføre quiz, lese brosjyrer, følge med på bloggposter, lese innlegg på e-post eller intranett. List de alternativene du tror er mest foretrukket for deres avdeling. Det kan også være alternativer som ikke er på listen.
- En utfordring som nevnes i litteraturen er å gi opplæring til helsepersonell på døgnseksjoner. Hvilken metode tror du egner seg best for helsepersonell med lite tid, ressurser og økt arbeidsbelastning?
- Hvilken metode tror du kunne skapt engasjement generelt?
- Hvilke metoder er ikke foretrukket og hvorfor?

Om det nye opplæringskonseptet

Det undersøkes om et nytt opplæringskonsept kunne bidratt til å øke hyppigheten for opplæring i informasjonssikkerhet. Konseptet går ut på å lage et felles opplæringsprogram som både inkluderer temaer for informasjonssikkerhet og pasientsikkerhet. Helsepersonell har fra før av opplæringsprogrammer som eksempelvis kan inkludere tema som hjerte- og lungeredning, håndtering av epileptiske anfall, behandling ved hjernerystelse og lignende. Flere tema står ofte på agendaen og avdelinger kan ofte velge de selv. I informasjonssikkerhet vil en avdelingsleder selv kunne tilpasse innholdet, men hovedpoenget er at minimum et tema i informasjonssikkerhet må inkluderes.

- Hva tenker du om et slikt opplæringskonsept?
- Hvilke fordeler tror du et slikt konsept kan ha?
- Hvilke ulemper tror du et slikt konsept kan ha?
- ror du det ville vært mulighet til å gjennomføre i praksis, eventuelt hva gjør det utfordrende å realisere?
- Hva trengs av ressurser for å eventuelt realisere et slikt konsept?

Strategisk nivå

- Hvilken rolle har du når det skal tas en beslutning i en beslutningsprosess?
- Hvilke vurderinger gjør dere når dere beslutter om et tiltak skal settes i verk, særlig innen opplæring i informasjonssikkerhet/pasientsikkerhet?
- Er informasjonssikkerhet en del av strategien i pasientsikkerhet? Hvis nei, hvorfor ikke?
- Hvordan arbeider dere med å utforme strategier som skal bidra til å gi opplæring i pasientsikkerhet/informasjonssikkerhet?

Taktisk nivå

- Hvordan arbeider dere med å tilby opplæring basert på strategier?
- Hvordan ser handlings – og delplanene deres ut for opplæring i informasjonssikkerhet?
- Hvilke oppgaver bidrar din avdeling med for å sikre opplæring til de som arbeider på operativt nivå?
- Hvilke utfordringer ser du i arbeidet med informasjonssikkerhet?
- Hva tror du kliniske avdelingsledere trenger for at de kan drive opplæring innen informasjonssikkerhet?

Operasjonelt nivå
• Gjennomfører dere internundervisning og hvor ofte? • Er internundervisning obligatorisk? • Hvordan planlegges internundervisning? • Hvordan velges de ulike temaene? • Hvordan gjennomfører dere opplæring? • Hvilken motivasjon har ansatte for å gjennomføre internundervisning? • Kunne informasjonssikkerhet vært en del av internundervisningen?

Vedlegg B

Informasjonsskriv om prosjektet

Vedlegg C

Godkjenning for behandling av personoplysninger

Sikt

Vurdering av behandling av personopplysninger

Referansenummer
407549

Vurderingstype
Automatisk

Dato
15.04.2023

Prosjekttittel
Masteroppgave i informasjonssikkerhet

Behandlingsansvarlig institusjon
Norges teknisk-naturvitenskapelige universitet / Fakultet for informasjonsteknologi og elektroteknikk (IE) / Institutt for informasjonssikkerhet og kommunikasjonsteknologi

Prosjektansvarlig
Stewart James Kowalski

Student
sarita sunder

Prosjektperiode
04.01.2023 - 01.06.2023

Kategorier personopplysninger
Alminnelige

Lovlig grunnlag
Samtykke (Personvernforordningen art. 6 nr. 1 bokstav a)

Behandlingen av personopplysningene er lovlig så fremt den gjennomføres som oppgitt i meldeskjemaet. Det lovlige grunnlaget gjelder til 01.06.2023.

Meldeskjema

Grunnlag for automatisk vurdering
Meldeskjemaet har fått en automatisk vurdering. Det vil si at vurderingen er foretatt maskinelt, basert på informasjonen som er fylt inn i meldeskjemaet. Kun behandling av personopplysninger med lav personvernulempe og risiko får automatisk vurdering. Sentrale kriterier er:

- De registrerte er over 15 år
- Behandlingen omfatter ikke særlige kategorier personopplysninger;
  - Rasemessig eller etnisk opprinnelse
  - Politisk, religiøs eller filosofisk overbevisning
  - Fagforeningsmedlemskap
  - Genetiske data
  - Biometriske data for å entydig identifisere et individ
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Behandlingen omfatter ikke opplysninger om straffedommer og lovovertredelser
- Personopplysningene skal ikke behandles utenfor EU/EØS-området, og ingen som befinner seg utenfor EU/EØS skal ha tilgang til personopplysningene
- De registrerte mottar informasjon på forhånd om behandlingen av personopplysningene.

Informasjon til de registrerte (utvalgene) om behandlingen må inneholde

- Den behandlingsansvarliges identitet og kontaktopplysninger
- Kontaktopplysninger til personvernombudet (hvis relevant)
- Formålet med behandlingen av personopplysningene
- Det vitenskapelige formålet (formålet med studien)
- Det lovlige grunnlaget for behandlingen av personopplysningene
- Hvilke personopplysninger som vil bli behandlet, og hvordan de samles inn, eller hvor de hentes fra
- Hvem som vil få tilgang til personopplysningene (kategorier mottakere)

- Hvor lenge personopplysningene vil bli behandlet
- Retten til å trekke samtykket tilbake og øvrige rettigheter

Vi anbefaler å bruke vår mal til informasjonsskriv.

Informasjonssikkerhet
Du må behandle personopplysningene i tråd med retningslinjene for informasjonssikkerhet og lagringsguider ved behandlingsansvarlig institusjon. Institusjonen er ansvarlig for at vilkårene for personvernforordningen artikkel 5.1. d) riktighet, 5. 1. f) integritet og konfidensialitet, og 32 sikkerhet er oppfylt.

Vedlegg D

Masteravtale og kontrakt for samarbeid med ekstern organisasjon

Masteravtale/hovedoppgaveavtale

Fastsatt av prorektor for utdanning 10.12.2020

Fakultet	**Fakultet for informasjonsteknologi og elektroteknikk**
Institutt	**Institutt for informasjonssikkerhet og kommunikasjonsteknologi**
Studieprogram	**Information security (MIS)**
Emnekode	**MIS4900 Masteroppgave informasjonssikkerhet**

Studenten

Etternavn, fornavn	**Sunder, Sarita**
Fødselsdato	**24.12.1994**
E-postadresse ved NTNU	**saritas@stud.ntnu.no**

Tilknyttede ressurser

Veileder	**Stewart James Kowalski**
Eventuelle medveiledere	
Eventuelle medstudenter	

Oppgaven

Oppstartsdato	**04.01.2023**
Leveringsfrist	**01.06.2023**
Oppgavens arbeidstittel	**Can cyber security training be integrated into patient safety education in Norway?**

Problembeskrivelse

Healthcare professionals lack knowledge about IT security. Many healthcare professionals report that they are not offered training, which makes it difficult for them to detect malicious activity. One common challenge in today's training programs at the hospital is that they separate information security training from patient safety training. The problem arises when they do not prioritize conducting security awareness training due to a lack of time and capacity. Therefore a part of this master thesis will assess if cyber security training can be integrated into patient safety education in Norway. Other research questions are: What methods can make employees in the health sector aware of risks and vulnerabilities related to ICT security? How can healthcare professionals avoid phishing?

Risikovurdering og datahåndtering

Skal det gjennomføres risikovurdering? **Dersom «ja», har det blitt gjennomført?**	**Nei** **Nei**
Skal det søkes om godkjenninger? (REK*, NSD)**	**Ja**
Skal det skrives en konfidensialitetsavtale i forbindelse med oppgaven? **Hvis «ja», har det blitt gjort?**	**Ja** **Nei**

* Regionale komiteer for medisinsk og helsefaglig forskningsetikk (https://rekportalen.no)

** Norsk senter for forskningsdata (https://nsd.no/)

Eventuelle emner som skal inngå i mastergraden

The specialization is in information security management IMT4110 Scientific Methodology and Communication IMT4113 Introduction to Cyber and Information Security Technology IMT4114 Introduction to Digital Forensics IMT4115 Introduction to Information Security Management IMT4127 Security Management Metrics IMT4129 Risk Management for Information Security IMT4215 Specialization Project IMT4000 Experts in Teamwork - Co-design and Social Innovation for Health-promoting Local Communities IMT4205 Research Project Planning IMT4128 Socio-technical Enabled Crime IMT4204 Intrusion Detection in Physical and Virtual Network TTM4165 Digital Economics

Retningslinjer - rettigheter og plikter

Formål

Avtale om veiledning av masteroppgaven/hovedoppgaven er en samarbeidsavtale mellom student, veileder og institutt. Avtalen regulerer veiledningsforholdet, omfang, art og ansvarsfordeling.

Studieprogrammet og arbeidet med oppgaven er regulert av Universitets- og høgskoleloven, NTNUs studieforskrift og gjeldende studieplan. Informasjon om emnet, som oppgaven inngår i, finner du i emnebeskrivelsen.

Veiledning

Studenten har ansvar for å

- Avtale veiledningstimer med veileder innenfor rammene master-/hovedoppgaveavtalen gir.
- Utarbeide framdriftsplan for arbeidet i samråd med veileder, inkludert veiledningsplan.
- Holde oversikt over antall brukte veiledningstimer sammen med veileder.
- Gi veileder nødvendig skriftlig materiale i rimelig tid før veiledning.
- Holde instituttet og veileder orientert om eventuelle forsinkelser.
- Inkludere eventuell(e) medstudent(er) i avtalen.

Veileder har ansvar for å

- Avklare forventninger om veiledningsforholdet.
- Sørge for at det søkes om eventuelle nødvendige godkjenninger (etikk, personvernhensyn).
- Gi råd om formulering og avgrensning av tema og problemstilling, slik at arbeidet er gjennomførbart innenfor normert eller avtalt studietid.
- Drøfte og vurdere hypoteser og metoder.
- Gi råd vedrørende faglitteratur, kildemateriale, datagrunnlag, dokumentasjon og eventuelt ressursbehov.
- Drøfte framstillingsform (eksempelvis disposisjon og språklig form).
- Drøfte resultater og tolkninger.
- Holde seg orientert om progresjonen i studentens arbeid i henhold til avtalt tids- og arbeidsplan, og følge opp studenten ved behov.
- Sammen med studenten holde oversikt over antall brukte veiledningstimer.

Instituttet har ansvar for å

- Sørge for at avtalen blir inngått.
- Finne og oppnevne veileder(e).
- Inngå avtale med annet institutt/ fakultet/institusjon dersom det er oppnevnt ekstern medveileder.
- I samarbeid med veileder holde oversikt over studentens framdrift, antall brukte veiledningstimer, og følge opp dersom studenten er forsinket i henhold til avtalen.
- Oppnevne ny veileder og sørge for inngåelse av ny avtale dersom:
    - Veileder blir fraværende på grunn av eksempelvis forskningstermin, sykdom, eller reiser.
    - Student eller veileder ber om å få avslutte avtalen fordi en av partene ikke følger den.
    - Andre forhold gjør at partene finner det hensiktsmessig med ny veileder.
- Gi studenten beskjed når veiledningsforholdet opphører.
- Informere veileder(e) om ansvaret for å ivareta forskningsetiske forhold, personvernhensyn og veiledningsetiske forhold.
- Ønsker student, eller veileder, å bli løst fra avtalen må det søkes til instituttet. Instituttet må i et slikt tilfelle oppnevne ny veileder.

Avtaleskjemaet skal godkjennes når retningslinjene er gjennomgått.

Godkjent av

Sarita Sunder
Student

25.01.2023
Digitalt godkjent

Stewart James Kowalski
Veileder

25.01.2023
Digitalt godkjent

Hilde Bakke
Institutt

03.03.2023
Digitalt godkjent

Fastsatt av prorektor for utdanning 10.12.2020

STANDARDAVTALE

om utføring av studentoppgave i samarbeid med ekstern virksomhet

Avtalen er ufravikelig for studentoppgaver (heretter oppgave) ved NTNU som utføres i samarbeid med ekstern virksomhet.

Forklaring av begrep

Opphavsrett
Er den rett som den som skaper et åndsverk har til å fremstille eksemplar av åndsverket og gjøre det tilgjengelig for allmennheten. Et åndsverk kan være et litterært, vitenskapelig eller kunstnerisk verk. En studentoppgave vil være et åndsverk.

Eiendomsrett til resultater
Betyr at den som eier resultatene bestemmer over disse. Utgangspunktet er at studenten eier resultatene fra sitt studentarbeid. Studenten kan også overføre eiendomsretten til den eksterne virksomheten.

Bruksrett til resultater
Den som eier resultatene kan gi andre en rett til å bruke resultatene, f.eks. at studenten gir NTNU og den eksterne virksomheten rett til å bruke resultatene fra studentoppgaven i deres virksomhet.

Prosjektbakgrunn
Det partene i avtalen har med seg inn i prosjektet, dvs. som vedkommende eier eller har rettigheter til fra før og som brukes i det videre arbeidet med studentoppgaven. Dette kan også være materiale som tredjepersoner (som ikke er part i avtalen) har rettigheter til.

Utsatt offentliggjøring
Betyr at oppgaven ikke blir tilgjengelig for allmennheten før etter en viss tid, f.eks. før etter tre år. Da vil det kun være veileder ved NTNU, sensorene og den eksterne virksomheten som har tilgang til studentarbeidet de tre første årene etter at studentarbeidet er innlevert.

1. Avtaleparter

Norges teknisk-naturvitenskapelige universitet (NTNU) Institutt: Institutt for informasjonssikkerhet og kommunikasjonsteknologi
Veileder ved NTNU: Stewart James Kowalski e-post og tlf. stewart.kowalski@ntnu.no ["61135236"] / 95434212
Ekstern virksomhet: Akershus universitetssykehus, Oslo Ekstern virksomhet sin kontaktperson, e-post og tlf.: Kåre Magne Stennes and Aleksander Andreassen kare.magne.stennes@ahus.no, aleksander.andreassen@ahus.no Kåre (90083520), Aleksander (91584739)
Student: Sarita Sunder Fødselsdato: 24.12.1994
Ev. flere studenter[1]

Partene har ansvar for å klarere eventuelle immaterielle rettigheter som studenten, NTNU, den eksterne eller tredjeperson (som ikke er part i avtalen) har til prosjektbakgrunn før bruk i forbindelse med utførelse av oppgaven. Eierskap til prosjektbakgrunn skal fremgå av eget vedlegg til avtalen der dette kan ha betydning for utførelse av oppgaven.

2. Utførelse av oppgave

Studenten skal utføre: (sett kryss)

Masteroppgave	X
Bacheloroppgave	-
Prosjektoppgave	-
Annen oppgave	-

Startdato: 04.01.2023
Sluttdato: 01.06.2023

Oppgavens arbeidstittel er: Can cyber security training be integrated into patient safety education in Norway?

Ansvarlig veileder ved NTNU har det overordnede faglige ansvaret for utforming og godkjenning av prosjektbeskrivelse og studentens læring.

3. Ekstern virksomhet sine plikter

[1] Dersom flere studenter skriver oppgave i fellesskap, kan alle føres opp her. Rettigheter ligger da i fellesskap mellom studentene. Dersom ekstern virksomhet i stedet ønsker at det skal inngås egen avtale med hver enkelt student, gjøres dette.

Ekstern virksomhet skal stille med en kontaktperson som har nødvendig faglig kompetanse til å gi studenten tilstrekkelig veiledning i samarbeid med veileder ved NTNU. Ekstern kontaktperson fremgår i punkt 1.

Formålet med oppgaven er studentarbeid. Oppgaven utføres som ledd i studiet. Studenten skal ikke motta lønn eller lignende godtgjørelse fra den eksterne for studentarbeidet. Utgifter knyttet til gjennomføring av oppgaven skal dekkes av den eksterne. Aktuelle utgifter kan for eksempel være reiser, materialer for bygging av prototyp, innkjøp av prøver, tester på lab, kjemikalier. Studenten skal klarere dekning av utgifter med ekstern virksomhet på forhånd.

Ekstern virksomhet skal dekke følgende utgifter til utførelse av oppgaven: Only transport costs related to visiting the hospital

Dekning av utgifter til annet enn det som er oppført her avgjøres av den eksterne underveis i arbeidet.

4. Studentens rettigheter

Studenten har opphavsrett til oppgaven[2]. Alle resultater av oppgaven, skapt av studenten alene gjennom arbeidet med oppgaven, eies av studenten med de begrensninger som følger av punkt 5, 6 og 7 nedenfor. Eiendomsretten til resultatene overføres til ekstern virksomhet hvis punkt 5 b er avkrysset eller for tilfelle som i punkt 6 (overføring ved patenterbare oppfinnelser).

I henhold til lov om opphavsrett til åndsverk beholder alltid studenten de ideelle rettigheter til eget åndsverk, dvs. retten til navngivelse og vern mot krenkende bruk.

Studenten har rett til å inngå egen avtale med NTNU om publisering av sin oppgave i NTNUs institusjonelle arkiv på Internett (NTNU Open). Studenten har også rett til å publisere oppgaven eller deler av den i andre sammenhenger dersom det ikke i denne avtalen er avtalt begrensninger i adgangen til å publisere, jf. punkt 8.

5. Den eksterne virksomheten sine rettigheter

Der oppgaven bygger på, eller videreutvikler materiale og/eller metoder (prosjektbakgrunn) som eies av den eksterne, eies prosjektbakgrunnen fortsatt av den eksterne. Hvis studenten skal utnytte resultater som inkluderer den eksterne sin prosjektbakgrunn, forutsetter dette at det er inngått egen avtale om dette mellom studenten og den eksterne virksomheten.

Alternativ a) (sett kryss) Hovedregel

X	Ekstern virksomhet skal ha bruksrett til resultatene av oppgaven

Dette innebærer at ekstern virksomhet skal ha rett til å benytte resultatene av oppgaven i egen virksomhet. Retten er ikke-eksklusiv.

[2] Jf. Lov om opphavsrett til åndsverk mv. av 15.06.2018 § 1

Alternativ b) (sett kryss) Unntak

	Ekstern virksomhet skal ha eiendomsretten til resultatene av oppgaven og studentens bidrag i ekstern virksomhet sitt prosjekt

Begrunnelse for at ekstern virksomhet har behov for å få overført eiendomsrett til resultatene:

6. Godtgjøring ved patenterbare oppfinnelser

Dersom studenten i forbindelse med utførelsen av oppgaven har nådd frem til en patenterbar oppfinnelse, enten alene eller sammen med andre, kan den eksterne kreve retten til oppfinnelsen overført til seg. Dette forutsetter at utnyttelsen av oppfinnelsen faller inn under den eksterne sitt virksomhetsområde. I så fall har studenten krav på rimelig godtgjøring. Godtgjøringen skal fastsettes i samsvar med arbeidstakeroppfinnelsesloven § 7. Fristbestemmelsene i § 7 gis tilsvarende anvendelse.

7. NTNU sine rettigheter

De innleverte filer av oppgaven med vedlegg, som er nødvendig for sensur og arkivering ved NTNU, tilhører NTNU. NTNU får en vederlagsfri bruksrett til resultatene av oppgaven, inkludert vedlegg til denne, og kan benytte dette til undervisnings- og forskningsformål med de eventuelle begrensninger som fremgår i punkt 8.

8. Utsatt offentliggjøring

Hovedregelen er at studentoppgaver skal være offentlige.

Sett kryss

X	Oppgaven skal være offentlig

I særlige tilfeller kan partene bli enige om at hele eller deler av oppgaven skal være undergitt utsatt offentliggjøring i maksimalt tre år. Hvis oppgaven unntas fra offentliggjøring, vil den kun være tilgjengelig for student, ekstern virksomhet og veileder i denne perioden. Sensurkomiteen vil ha tilgang til oppgaven i forbindelse med sensur. Student, veileder og sensorer har taushetsplikt om innhold som er unntatt offentliggjøring.

Oppgaven skal være underlagt utsatt offentliggjøring i (sett kryss hvis dette er aktuelt):

Sett kryss		Sett dato
	ett år	

	to år	
	tre år	

Behovet for utsatt offentliggjøring er begrunnet ut fra følgende:

Dersom partene, etter at oppgaven er ferdig, blir enig om at det ikke er behov for utsatt offentliggjøring, kan dette endres. I så fall skal dette avtales skriftlig.

Vedlegg til oppgaven kan unntas ut over tre år etter forespørsel fra ekstern virksomhet. NTNU (ved instituttet) og student skal godta dette hvis den eksterne har saklig grunn for å be om at et eller flere vedlegg unntas. Ekstern virksomhet må sende forespørsel før oppgaven leveres.

De delene av oppgaven som ikke er undergitt utsatt offentliggjøring, kan publiseres i NTNUs institusjonelle arkiv, jf. punkt 4, siste avsnitt. Selv om oppgaven er undergitt utsatt offentliggjøring, skal ekstern virksomhet legge til rette for at studenten kan benytte hele eller deler av oppgaven i forbindelse med jobbsøknader samt videreføring i et master- eller doktorgradsarbeid.

9. Generelt

Denne avtalen skal ha gyldighet foran andre avtaler som er eller blir opprettet mellom to av partene som er nevnt ovenfor. Dersom student og ekstern virksomhet skal inngå avtale om konfidensialitet om det som studenten får kjennskap til i eller gjennom den eksterne virksomheten, kan NTNUs standardmal for konfidensialitetsavtale benyttes.

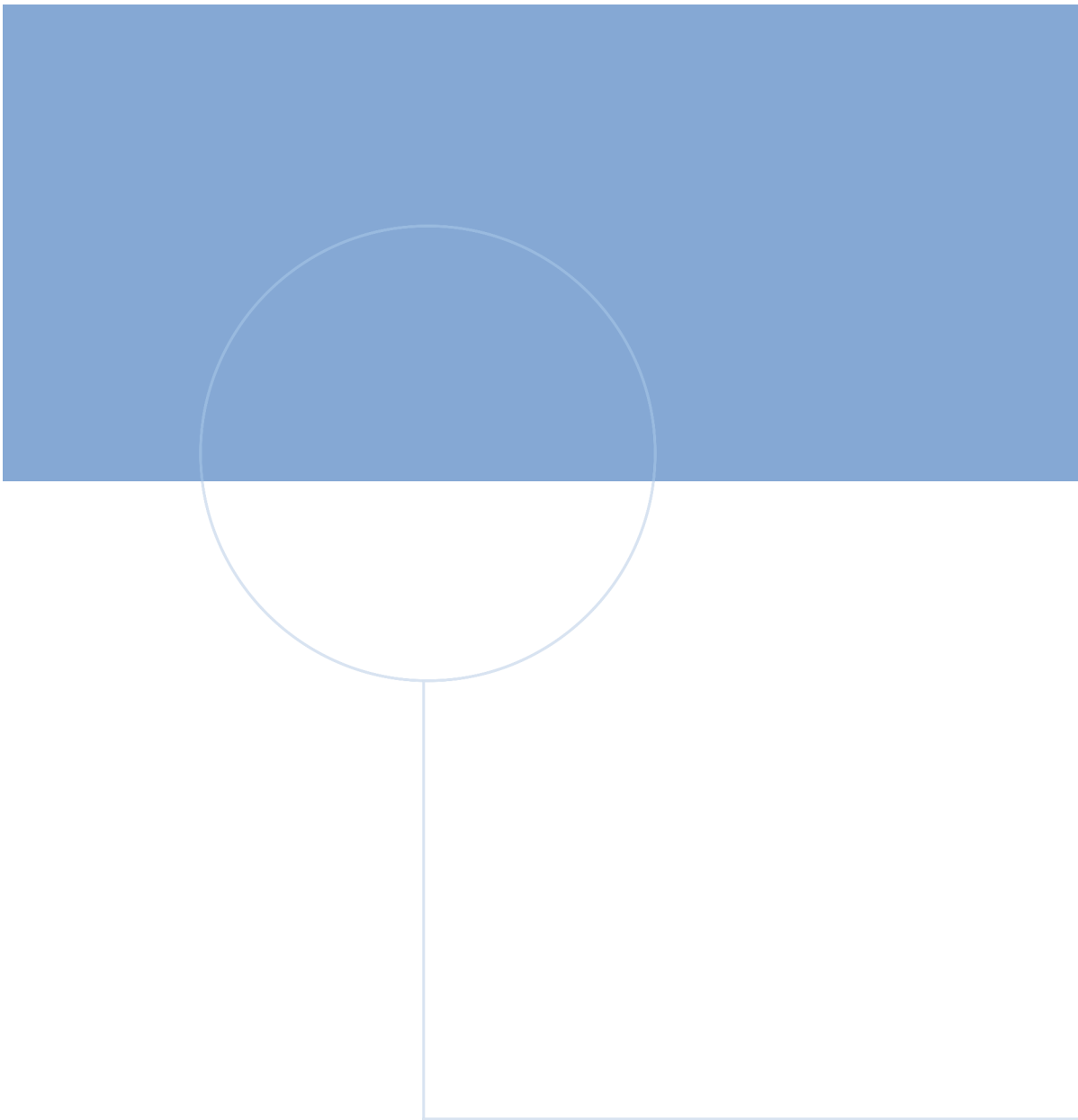
Den eksterne sin egen konfidensialitetsavtale, eventuell konfidensialitetsavtale den eksterne har inngått i samarbeidprosjekter, kan også brukes forutsatt at den ikke inneholder punkter i motstrid med denne avtalen (om rettigheter, offentliggjøring mm). Dersom det likevel viser seg at det er motstrid, skal NTNUs standardavtale om utføring av studentoppgave gå foran. Eventuell avtale om konfidensialitet skal vedlegges denne avtalen.

Eventuell uenighet som følge av denne avtalen skal søkes løst ved forhandlinger. Hvis dette ikke fører frem, er partene enige om at tvisten avgjøres ved voldgift i henhold til norsk lov. Tvisten avgjøres av sorenskriveren ved Sør-Trøndelag tingrett eller den han/hun oppnevner.

Denne avtale er signert i fire eksemplarer hvor partene skal ha hvert sitt eksemplar. Avtalen er gyldig når den er underskrevet av NTNU v/instituttleder.

Signaturer:

Instituttleder: Hilde Bakke Dato: 03.03.2023
Veileder ved NTNU: Stewart James Kowalski Dato: 25.01.2023
Ekstern virksomhet: Ahus, Kåre Magne Stennes Dato: 23.03.2023
Student: Sarita Sunder Dato: 25.01.2023
Ev. flere studenter (Skal ikke signeres av medstudenter. Hver enkelt student oppretter sin egen avtale.)



NTNU

Kunnskap for en bedre verden