# Informasjonssikkerhetsledelse og klinisk arbeidsflyt i helsesektoren

En case-studie ved Sørlandet sykehus HF (SSHF)

JØRGEN BJØRNSTAD OG RICKY LØTOFT OMLAND

VEILEDERE
Devendra Bahadur Thapa & Margunn Aanestad

**Universitetet i Agder, 2019**
Fakultet for Samfunnsvitenskap
Institutt for Informasjonssystemer

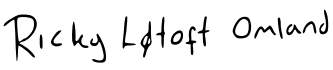
# Forord

Vi ønsker med denne rapporten å fremheve viktigheten av informasjonssikkerhet og flyt i arbeidsprosesser blant klinisk ansatte i norsk helsesektor. Bakgrunn og motivasjon for oppgaven omhandler viktigheten av å fremme informasjonssikkerhet som praksis i en av våre viktigste og mest kritiske offentlige organ; helsesektoren. Vi mener det er viktig å utforske dette temaet fordi det er høyst dagsaktuelt og et kritisk samfunnsbehov at informasjonssikkerheten ivaretas for å beskytte individets rettigheter og personvern. Vi har hatt et ønske om å danne oss innsikt i hvorvidt det finnes nok kunnskap om informasjonssikkerhet ved sykehus i norsk helsesektor og hva slags forhold ansatte har til informasjonssikkerhet og hvordan deres arbeidshverdag påvirkes. Motivasjon ligger således i å synliggjøre og fremme bevissthet rundt informasjonssikkerhet blant ansatte i denne sektoren. Vårt mål med denne rapporten har vært å – gjennom undersøkelse i en enkelt case-studie – bidra til økt bevissthet rundt konflikter mellom informasjonssikkerhetsledelse og klinisk arbeidsflyt. Vi mener det foreligger en mangel i litteraturen spesifikt for informasjonssikkerhet i norsk helsesektor og bevissthet rundt informasjonssikkerhet generelt i organisasjoner. Masteroppgaven begrenses til empirisk forskning og datainnsamling ved Sørlandet sykehus Helseforetak (SSHF) i tillegg til tidligere forskningslitteratur som omhandler informasjonssikkerhet rettet mot helsesektoren.

Vi ønsker å rette en stor takk til institutt for informasjonssystemer ved Universitetet i Agder og de ansatte – våre forelesere og ansatte ved senter for e-helse som har bidratt med støtte, veiledning og råd underveis. Vi retter også en stor takk til våre ytterst hjelpsomme og kunnskapsrike veiledere Devinder og Margunn, og en spesielt stor takk til våre respondenter ved SSHF som har deltatt i denne studien. Til slutt vil vi takke våre kolleger og medstudenter ved Universitetet i Agder for alle de gode minnene.

Jørgen Bjørnstad

Ricky Løtoft Omland



Kristiansand, 03. juni 2019

# Sammendrag

Masteroppgaven omhandler informasjonssikkerhet og informasjonssikkerhetsledelse (ISM) i en kontekst av helsesektoren, med problemstilling: "Konflikter mellom informasjonssikkerhetsledelse og arbeidsflyt i norsk helsesektor". Bakgrunn og motivasjon for oppgaven var innledningsvis basert på interesse for feltet informasjonssikkerhet. Det ønsket vi å forske på gjennom helsesektoren, ettersom dette er en åpenbar samfunnskritisk funksjon med svært sensitive persondata som må beskyttes. Dette førte videre til at vi kontaktet Sørlandet sykehus Helseforetak (SSHF) med forespørsel om å foreta datainnsamling. Denne masterutredningen omtales derfor som en case-studie ved SSHF.
Denne studien avgrenses til informasjonssikkerhetsledelse i norsk offentlig helsesektor hvor vi utelukkende samler data ved SSHF som instans. Innenfor instansen har vi igjen avgrenset oss til å samle data ved to avdelinger, henholdsvis avdeling for teknologi og e-helse (TEH), samt intensiv enhet (IE). I sammenheng med kvalitativt intervju består respondentene av sentrale ledere ved TEH og et utvalg helsepersonell fra IE v/ Kristiansand.

Forskningsstrategien vår har bestått av det vi kaller kombinerte metoder; i en kombinasjon av kvalitativ og kvantitativ forskningsmetodikk. Vi har vurdert det som hensiktsmessig å først legge et empirisk grunnlag gjennom kvalitativ datainnsamling under intervjuer og dokumentasjon, for så å deretter kunne samle inn mer beviselige kvantitative data gjennom et anonymt spørreskjema. Til utforming av spørreundersøkelse og distribuering av spørreskjema har vi brukt SurveyXact.

Under datainnsamling for forskningslitteratur har vi utarbeidet en egen litteraturstudie som har som en del av innledende forskning til masteroppgaven. I denne litteraturstudien fokuserte vi på å innhente teori fra empiriske studier, fagfellevurderte forskningsartikler og anerkjente tidsskrifter innen fagfeltet informasjonssystemer, med fokus på informasjonssikkerhetsledelse i helsesektor.

Vi utarbeidet en konseptmatrise med fokus på arbeidsflyt, samt hvilke praksiser for informasjonssikkerhet organisasjoner følger, med fokus på formell, uformell og teknisk sikkerhetspraksis. Herunder var opplæring av ansatte, formelle retningslinjer, kultur, tillit, EPJ-systemer og tilgangsstyring de underliggende konseptene vi valgte å fokusere på i litteraturen.

Vi fikk tidlige indikasjoner gjennom forskningslitteratur og forstudier på at blant annet tilgangsstyring og autentisering kan være en viktig faktor, som deriblant kan føre til interessekonflikter mellom hensyn til informasjonssikkerheten og arbeidsflyten til de ansatte. Som artikkelen «The authentication dilemma» av Wiercioch, Teufel & Teufel (2018) påpeker: «*Several studies have shown that users consciously refrain from using security measures because they rate practicability higher than security [...] From a user's perspective, the cost of strong passwords outweighs the potential benefits or protection from potential attack»* (Wiercioch, Teufel & Teufel, 2018, s. 278).

Et av våre hovedfunn bygger på at det foreligger 96 % enighet om at det er mer positivt enn negativt med elektronisk rapportering, både for behandling av pasient og sikring av pasientdata. På grunnlag av dette kan vi med høy sannsynlighet konkludere at EPJ-systemet er kommet for å bli i organisasjonen, og at «DIPS» gjør en god jobb med å understøtte klinikernes arbeidsprosesser. Videre viser resultater fra undersøkelsen til 78 % enighet om at responstiden for arbeidsstasjoner i mer eller mindre grad er

dårlig. Respons fra intervjuer med klinikere indikerer at arbeidsstasjonene med dårlig responstid opptar store deler av arbeidsdagen for enkelte. Resultatene fra spørreundersøkelsen viser at 65 % av respondentene opplever at de må logge ut andre fra EPJ-systemene flere ganger i uken, mens 85 % av respondentene opplever å måtte logge ut andre fra arbeidsstasjoner flere ganger i uken. Majoriteten av klinikere i undersøkelsen er fornøyd med kvaliteten på opplæringen innen informasjonssikkerhet.

Utredningen har som formål å bidra med å fylle et tomrom innen forskingslitteraturen når det kommer til forvaltning av teknologi og sikring av informasjon i helsesektor.

# Innholdsfortegnelse

## Figurliste

## Tabelliste

# 1. Innledning

I dette kapittelet tar vi for oss en introduksjon av tema for oppgaven og oppsummerer tidligere forskning som er relevant for temaet vi har valgt oss. Videre presenterer vi formål med prosjektet og studiens problemstilling med forskningsspørsmål og avgrensninger. Etterfølgende gir vi et kort sammendrag av vår forskningsstrategi, som vi utdyper mer om i detalj i tredje kapittel. Til slutt tar vi for oss sentrale begreper som brukes i utredningen og en oppsummering av hovedfunn vi har gjort oss av den.

## 1.1 Introduksjon

Denne utredningen tar for seg temaet «**Information Security Management»** (ISM), eller informasjonssikkerhetsledelse.

For å gi god helsehjelp er det nødvendig å håndtere store mengder opplysninger om enkeltindivider. Disse opplysningene omhandler ofte personlige og sensitive forhold og er avgjørende for helsehjelpens kvalitet. Det er derfor i både virksomhetens og brukernes interesse å få tilgang til og å beskytte opplysningene. Å behandle opplysninger om pasienter og brukere på en betryggende måte, er avgjørende for å sikre tillit. Helsetjenesten er avhengig av tillit fra både pasienter, brukere, helsepersonell og befolkningen for øvrig. Pasienter og brukere må ha tillit for å våge å gi helsetjenesten sine opplysninger, av og til svært intim og personlig informasjon. Uten disse opplysningene kan vi ikke gi helsehjelp av god kvalitet. Helsepersonell må ha tillit til at opplysningene er korrekte og fullstendige for å kunne gi helsehjelpen. Sektoren trenger tillit for å kunne digitalisere og tilby helsehjelp på nye måter. Informasjonssikkerhet er en forutsetning for digitalisering. Dette betyr at opplysninger må være korrekte, oppdaterte, fullstendige og tilgjengelige. Teknologien og behandlingen av opplysninger som brukes i helsetjenesten kan bli utsatt for både utilsiktede og tilsiktede hendelser. Sektoren må bygge og forvalte robust teknologi, organisasjon og sikkerhetskultur og ha gode tiltak for å sikre at dette fungerer og samtidig håndtere og lære av tilfeller der den ikke fungerer (Direktoratet for e-helse, 2018d).

Historisk sett har helsesektoren vært gjenstand for angrep, eksempelvis *WannaCry*-angrepet i 2017 (Norsk Helsenett, i.d.-b). Det vil utvilsomt skje liknende hendelser igjen, og derfor er det viktig å ha en proaktiv tilnærming til informasjonssikkerheten for å begrense skadeomfang.

Vårt mål i utredelsen er å – gjennom utforskende/eksplorative intervjuer – gjøre funn på spesifikke aspekter innenfor informasjonssikkerhet som kan påvirke klinikernes flyt i arbeidsprosesser (arbeidsflyt). Videre ønsker vi å innta en kvantitativ tilnærming for å undersøke graden av påvirkning.

## 1.2 Tidligere forskning

I helsesektoren finner vi gode eksempler på organisasjoner hvor det i høyeste grad holdes på sensitive personopplysninger, som er en kritisk del av ISM: *«Det er åpenbart at dersom sensitiv helseinformasjon – som eksempelvis mental helsehistorikk – blir aksessert av uvedkommende, vil etterfølgende overtredelse kunne ha alvorlige konsekvenser for det gjeldende individ»* (Hou, Gao & Nicholson, 2018, s. 64). Basert på funn som ble gjort i artikkelen av Hou et al., (2018) peker bevisene på at mesteparten av feilene som blir begått innen informasjonssikkerhet, og spesielt i helsesektoren (Hou et al., 2018;

Rahimli & Masrom, 2015), oppstår som følge av menneskelige og organisatoriske faktorer (Chang & Ho, 2006; Hou et al., 2018). Problemer oppstår grunnet dårlig ledelse, og ignoranse fra toppledelse og mellomledelse, (Hou et al., 2018; Straub & Welke, 1998) misbruk av informasjonssystemer, manglende overholdelse av retningslinjer i henhold til informasjonssikkerhet, (Hou et al., 2018; Stanton, Stam, Mastrangelo & Jolton, 2005) og mangel på organisatorisk informasjonssikkerhetsstrategi (Bakari, Tarimo, Yngström, Magnusson & Kowalski, 2007; Hou et al., 2018; Rahimli & Masrom, 2015). Dette er faktorer som har vist å direkte eller indirekte bidra til svikt i informasjonssikkerheten. ISM tilbyr prosedyrer og standarder for å beskytte informasjonssystemer fra uautorisert tilgang og beskytter informasjon fra avsløring, forstyrrelse, modifikasjon eller ødeleggelse (Hou et al., 2018).

Det vises til klare utfordringer relatert til praksiser for informasjonssikkerhet. Av disse er utfordringer knyttet til kultur og bevissthet rundt sikkerhet mest forekommende i forskningslitteraturen, mens opplæring og organisatorisk samarbeid på tvers av hierarkiske nivåer er de to videst diskuterte typer initiativ (Bekkevik, Holm, Vassilakopoulou & Hustad, 2018).

Postdoktor ved Universitetet i Agder, Berglind F. Smaradottir, publiserte tidligere inneværende år en litteraturstudie som presenterer en gjennomgang av sikkerhetsledelse i helsesektorens informasjonssystemer. I artikkelen etterlyser hun videre forskning på innvirkningene av retningslinjer for sikkerhet på klinisk arbeidsflyt, som vi har ønsket å vektlegge i særlig grad i oppgaven vår (Smaradottir, 2018).

Vi har i tidligere litteraturstudie belyst flere ulike problemstillinger som har blitt adressert av tidligere forskning innen ISM og helsesektoren. Deriblant retningslinjer, kultur, kunnskap, problemstillinger innen helseinformasjonsystemer som elektroniske pasientjournaler (EPJ), tilgangsstyring og underliggende faktorer som brukbarhet. Vi har satt disse faktorene i en sammenheng som ikke nødvendigvis har blitt gjort på samme måte tidligere; holdninger blant klinisk ansatte til ISM, faktorer som opplæring/kursing og hvordan det kan bidra til å skape bevissthet rundt sikkerhet, innvirkningen av organisasjonskultur/informasjonssikkerhetskultur på sikkerhet, og at forbedring av informasjonssikkerhetskultur starter med opplæring og kunnskapsheving.

Vi har fremhevet at bevissthet rundt retningslinjer kan gjøre ansatte bedre forberedt på å håndtere sikkerhetsbrudd og risikoer, mens dersom bevissthet rundt retningslinjer ikke fremheves kan ansatte bryte de og ikke engang være klar over det. Ansatte bør dermed inkluderes i utforming av retningslinjer, og eksempelvis retningslinjer for tilgangsstyring med utgangspunkt i helsepersonellets behov og arbeidsflyt (Ferreira, Antunes, Chadwick & Correia, 2010). Vi ønsker med dette å formidle at feilene som blir begått innen informasjonssikkerhet, spesielt i helsesektoren (Hou et al., 2018; Rahimli & Masrom, 2015) oppstår som følge av menneskelige og organisatoriske faktorer (Chang & Ho, 2006; Hou et al., 2018). Dermed er ISM i en kontekst av helsesektoren en problemstilling med svært mange faktorer å ta hensyn til.Vi har fremhevet at bevissthet rundt retningslinjer kan gjøre ansatte bedre forberedt på å håndtere sikkerhetsbrudd og risikoer, mens dersom bevissthet rundt retningslinjer ikke fremheves kan ansatte bryte de og ikke engang være klar over det. Ansatte bør dermed inkluderes i utforming av retningslinjer, og eksempelvis retningslinjer for tilgangsstyring med utgangspunkt i helsepersonellets behov og arbeidsflyt (Ferreira et al., 2010). Vi ønsker med dette å formidle at feilene som blir begått innen informasjonssikkerhet, spesielt i helsesektoren (Hou et al., 2018; Rahimli & Masrom, 2015) oppstår som følge av menneskelige og organisatoriske faktorer (Chang & Ho, 2006; Hou

et al., 2018). Dermed er ISM i en kontekst av helsesektoren en problemstilling med svært mange faktorer å ta hensyn til.

Vi mener at det mangler forskning omkring konflikter mellom informasjonssikkerhetsledelse og arbeidsflyt i norsk helsesektor mellom informasjonssikkerhetsledelse og hvilke av disse aspektene som er viktige og tilstede i norsk sammenheng.

## 1.3 Formål og motivasjon

Formålet med prosjektet har vært å undersøke sammenhengen mellom informasjonssikkerhetsledelse og arbeidsflyt hos klinikere og om det oppstår konflikter mellom disse samt underliggende faktorer. Utredningen har som formål å bidra med å fylle et tomrom innen forskingslitteraturen når det kommer til forvaltning av teknologi og sikring av informasjon i helsesektoren, og videre gi indikasjoner på hvordan dette påvirker klinikernes flyt i arbeidsprosesser. På denne måten vil studien belyse hvorvidt det foreligger behov for å gjennomføre tiltak for å forbedre kompetansen og satsningen på informasjonssikkerhet i offentlig helsesektor, og eventuelt hvilke tiltak som kan innføres eller hva som kan gjøres annerledes. For helsevesen kan en slik studie forhåpentligvis føre til mer bevissthet og engasjement rundt ISM, samtidig som at viktigheten av ISM blir belyst. Kunnskapen vil forhåpentligvis kunne bidra til å øke bevisstheten rundt informasjonssikkerhet innen helsesektoren.

Det har også vært viktig for oss å kunne produsere en rapport som kunne være til nytte for Sørlandet sykehus som vi har samarbeidet med, og derfor har vi hatt jevn dialog mellom IT ledere og kontaktpersoner i organisasjonen. For å kunne undersøke informasjonssikkerhetsledelse og informasjonssikkerhet i denne konteksten har det vært viktig å undersøke hvordan de ansatte faktisk jobber, hvordan deres arbeidshverdag er og deres synspunkter/holdninger relatert til helseinformasjonsystemene, arbeidsstasjoner og annet utstyr.

Vår personlige motivasjon til å undersøke dette temaet er at vi deler en felles interesse for temaet informasjonssikkerhet, og vi har ønsket å forske på helsesektoren ettersom vi anser den som et samfunnsmessig kritisk område innenfor temaet. Det er av ytterste viktighet at uvedkommende ikke har tilgang på sensitive helsedata, og konsekvensene kan bli enorme dersom sikkerheten i denne sektoren svikter. Vi mener det er viktig å utforske dette temaet fordi det er høyst dagsaktuelt og et kritisk samfunnsbehov at informasjonssikkerheten ivaretas for å beskytte individets rettigheter. Vi har et personlig ønske om å danne oss en innsikt i hvorvidt det finnes nok kunnskap om informasjonssikkerhet i norsk helsevesen, hva slags forhold de ansatte har til informasjonssikkerhet, og om det blir gjort nok for å forebygge og å forhindre dataangrep fra et teknisk ståsted, eksempelvis fra *HelseCERT* sin side. HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet (Norsk Helsenett, i.d.-a).

## 1.4 Problemstilling og forskningsspørsmål

Denne studien tar for seg følgende problemstilling: «**Konflikter mellom informasjonssikkerhetsledelse og arbeidsflyt i norsk helsesektor**». Vi har hatt som mål å utrede problemstillingen ved å besvare to forskningsspørsmål:

**RQ1**: *Hvilke aspekter for informasjonssikkerhetsledelse er viktige i organisasjonen?*
**RQ2**: *I hvilken grad er aspektene tilstede i organisasjonen?*

Forskningsspørsmålene tar for seg problemstillingen i hver sine metodiske tilnærminger, henholdsvis kvalitativ og kvantitativ, noe vi kommer tilbake til i neste underkapittel (*kap. 1.5: Forskningsstrategi*).

Denne studien avgrenses til informasjonssikkerhetsledelse i norsk offentlig helsesektor hvor vi utelukkende samler data ved en instans; Sørlandet sykehus HF (SSHF). Innenfor instansen har vi igjen avgrenset oss til å samle data ved to avdelinger, henholdsvis avdeling for teknologi og e-helse (TEH), samt intensiv enhet (IE). I sammenheng med kvalitativt intervju består respondentene av sentrale ledere ved TEH og et utvalg helsepersonell fra IE v/ Kristiansand. Dette er klinisk ansatte, både ordinære sykepleiere og spesialutdannede intensivsykepleiere. Utvalget til spørreundersøkelsen er alle ansatte i IE v/ Kristiansand. Vi rapporterer om alt dette i detalj i tredje kapittel *(kap. 3.1.2: Populasjon og utvalg)*. Vi beskriver hvordan vi har avgrenset innledende litteraturstudie i andre kapittel *(kap. 2.1: Avgrensninger i litteraturen)*.

## 1.5 Forskningsstrategi

Forskningsstrategien vår har bestått av det vi kaller kombinerte metoder; en kombinasjon av kvalitativ og kvantitativ forskningsmetodikk. Vi har vurdert det som hensiktsmessig å først legge et empirisk grunnlag gjennom kvalitativ datainnsamling under intervjuer og dokumentasjon, for så å deretter kunne samle inn mer beviselige kvantitative data gjennom et anonymt spørreskjema. Til utforming av spørreundersøkelse og distribuering av spørreskjema har vi brukt SurveyXact, som er standardverktøyet for spørreundersøkelser på SSHF og Universitetet i Agder. Vi kommer nærmere inn på dette i *kap. 3.4.3 (SurveyXact)*.

Studien er gjennomført ved Sørlandet sykehus HF (SSHF) hvor vi har innsamlet data og avholdt møter, samt hatt korrespondanse via mail med ansatte ved sykehuset. Vi har gjennom åpne individuelle intervjuer både med ansatte i tekniske lederroller og kliniske roller undersøkt hvilke aspekter for informasjonssikkerhet som er viktige for organisasjonen, satt i et perspektiv av påvirkning på flyt i arbeidsprosesser. Basert på dette har vi utformet og sendt ut spørreskjema til et utvalg klinikere, henholdsvis ansatte ved intensiv enhet under avd. for somatikk i Kristiansand for å undersøke i hvilken grad disse aspektene er tilstede i organisasjonen. Vi bestemte oss for å foreta semi-strukturerte dybdeintervjuer med ansatte i en deduktiv tilnærming for å kunne avgrense problemområdet vårt ytterligere. Et av disse områdene vi har avgrenset studien til og fokusert på i større grad er tilgangsstyring. Dermed har vi vektlagt dette under utformingen av spørreundersøkelsen. Vi kommer nærmere inn på forskningens tilnærming og kontekst i *kap. 3 (Forskningstilnærming og -kontekst*).

## 1.6 Sentrale begreper

**ISM** – «*Information security management*»: Omhandler ledelsens håndtering av informasjonssikkerhet. Retningslinjer, operasjonelle prosesser og relaterte ressurser som beskytter informasjon (McLaughlin & Gogan, 2018, s. 239).

**Informasjonssikkerhet** – Omhandler konfidensialitet, integritet og tilgjengelighet for digitale informasjonsressurser (data, informasjon, kunnskap, dokumenter) og andre relevante IT-ressurser (maskinvare, programvare, nettverk) (McLaughlin & Gogan, 2018, s. 239).

**Tilgangsstyring** – Vi har tidligere under forstudien brukt begrepet adgangskontroll og adgangskontrollmekanismer som en oversettelse av de engelske begrepene «access control» og «access control mechanism» i relasjon til kontroller og mekanismer for autorisering og autentisering av tilgang. Vi velger å bruke begrepet tilgangsstyring, ettersom vi har erfart under kvalitativ datainnsamling at dette begrepet er dekkende og kanskje mest brukt i denne sammenhengen.

**Autentisering** – Tilgangsstyringsmekanismen som validerer brukerens identitet (Whitman & Mattord, 2018, s. 694).

**Autorisering** – Tilgangsstyringsmekanismen som sjekker en autentisert entitet opp mot en liste med ressurser og tilhørende tilgangsnivåer (Whitman & Mattord, 2018, s. 694).

**Principle of least privilege** (POLP) – Et sikkerhetsprinsipp som begrenser tilgangsprivilegier til autorisert personell (eksempelvis privilegier for programeksekusjon eller modifikasjon av filer) til et minimum av det som er nødvendig for å kunne utføre en jobb (Barker, Barker, Burr, Polk & Smid, 2019, s. 17).

**Session lock** – Forhindrer videre tilgang til et system ved å låse økten etter en definert tidsperiode ved inaktivitet (NIST, i.d.-b).

**Information flow control** – Regulerer hvor informasjon har lov til å bevege seg rundt i et informasjonssystem og mellom informasjonssystemer. Det kan eksempelvis være å begrense flyt av informasjon over det åpne internett eller å blokkere trafikk utenfra som tilsynelatende kommer innenfra organisasjonen (NIST, i.d.-a).

**Session termination** – En logisk økt initieres når en bruker aksesserer et organisatorisk informasjonssystem. Disse øktene og derav tilgangen, og tilhørende prosesser kan termineres, kan eksempelvis skje på bakgrunn av perioder med inaktivitet eller som en respons til spesifikke hendelser (NIST, i.d.-c).

## 1.7 Viktigste resultater

Et av våre hovedfunn bygger på at det foreligger 96 % enighet om at det er mer positivt enn negativt med elektronisk rapportering, både for behandling av pasient og sikring av pasientdata. På grunnlag av dette kan vi med høy sannsynlighet konkludere at EPJ-systemet er kommet for å bli i organisasjonen, og at «DIPS» gjør en god jobb med å understøtte klinikernes arbeidsprosesser. Videre viser resultater fra undersøkelsen til 78 % enighet om at responstiden for arbeidsstasjoner i mer eller mindre grad er dårlig. Respons fra intervjuer med klinikere indikerer at arbeidsstasjonene med dårlig responstid opptar store deler av arbeidsdagen for enkelte. Resultatene fra spørreundersøkelsen viser at 65 % av respondentene opplever at de må logge ut andre fra EPJ-systemene flere ganger i uken, mens 85 % av respondentene opplever å måtte logge ut andre fra arbeidsstasjoner flere ganger i uken. Majoriteten av klinikere i undersøkelsen virker å være fornøyd med kvaliteten på opplæringen innen

informasjonssikkerhet. Kvalitative resultater har avdekket at organisasjonens utfordringer relatert til opplæring og håndtering av kunnskap bygger på oppfølging og mangel på avsatte ressurser.

# 2. Teori

I dette kapittelet beskriver vi teori fra forskningslitteratur der vi bruker egen litteraturstudie som har vært utarbeidet som innledende forskning til masteroppgaven. I denne litteraturstudien fokuserte vi på å innhente teori fra empiriske studier, fagfellevurderte forskningsartikler og anerkjente tidsskrifter innen informasjonssystemer fagfeltet. Vi mener at det å se mot studerte case-studier er mest hensiktsmessig for vår problemstilling. Fokuset vårt ble dermed avgrenset til studier som omhandler informasjonssystemer/informasjonssikkerhet/ISM og helseinformatikk i sammenheng med helsesektor. Konseptene vi anså som aktuelle og relevante å utforske omhandlet **arbeidsflyt**, samt hvilke praksiser for informasjonssikkerhet organisasjoner følger, med fokus på **formell**, **uformell** og **teknisk sikkerhetspraksis.** Herunder var opplæring av ansatte, formelle retningslinjer, kultur, tillit, EPJ-systemer og tilgangsstyring de underliggende konseptene vi valgte å fokusere på i litteraturen. Til slutt ønsket vi å skape et innblikk i hvordan innføring og oppfølging av denne typen sikkerhetstiltak påvirker klinikernes flyt i arbeidsprosesser (*klinisk arbeidsflyt*). Litteraturstudien har blitt gjennomført med systematisk gjennomgang av litteratur via databaser for fagfellevurdert forskning (e.g.: Scopus). Videre i kapittelet presenterer vi et konseptuelt rammeverk hentet fra litteraturen, før vi avslutter kapittelet med å presentere vår egen skreddersydde forskningsmodell for studien.

## 2.1 Avgrensninger i litteraturen

For å avgrense søkene våre har vi utarbeidet en oversikt over journaler som tar for seg hver enkelt journals unike ISSN-kode. Ved å legge til ISSN-kodene i søkestrengen kan vi avgrense søket vårt til å gjelde kun for de journalene som vi ønsker å lete i.

Vi har satt sammen to lister med journaler innenfor IS. Listene tar henholdsvis for seg det vi vurderer som hovedjournalene innen IS *(Tabell 1)* og for øvrig noen gode kvalitetsjournaler innen IS *(Tabell 2)*.

| Journal | ISSN |
|---|---|
| European Journal of Information Systems (EJIS) | 1476-9344 |
| Information Systems Journal (ISJ) | 1365-2575 |
| Information Systems Research (ISR) | 1526-5536 |
| Journal of AIS (JAIS) | 1536-9323 |
| Journal of Information Technology (JIT) | 1466-4437 |
| Journal of MIS (JMIS) | 0742-1222 |
| Journal of Strategic Information Systems (JSIS) | 0963-8687 |
| MIS Quarterly (MISQ) | 2162-9730 |

*Tabell 1: Åtte hovedjournaler innen IS*

| Journal | ISSN |
|---|---|
| Communications of the Association for Information Systems (CAIS) | 1529-3181 |
| Information and Organization (IO) | 1471-7727 |
| Information Technology and People (ITP) | 0959-3845 |

| | |
|---|---|
| International Journal of Information Management (IJIM) | 0268-4012 |
| Scandinavian Journal of Information Systems (SJIS) | 1901-0990 |
| MIS Quarterly Executive (MISQE) | 1540-1960 |
| Computer Supported Cooperative Work (CSCW) | 1573-7551 |

*Tabell 2: Syv høykvalitetsjournaler i IS*

Vi har i tillegg satt sammen en liste for medisinske journaler *(Tabell 3)*. Listen er basert på journaler brukt av forskere som i eksisterende litteratur har bidratt innenfor samme fagområde.

| Journal | ISSN |
|---|---|
| International Journal of Medical Informatics (IJMI) | 1386-5056 |
| BMC Medical Informatics and Decision Making (BMCMIDM) | 1472-6947 |
| Journal of Advanced Nursing (JAN) | 1365-2648 |
| Journal of the American Medical Informatics Association (JAMIA) | 1067-5027 |
| Health Informatics Journal (HIJ) | 1741-2811 |
| Journal of Medical Internet Research (JMIR) | 1438-8871 |

*Tabell 3: Seks håndplukkede medisinske/helsebaserte journaler*

### 2.1.1 Søkekriterier

Vi har vært bevisst på å bruke artikler fra det siste tiår da informasjonssikkerhet er et tema som i stor grad har blitt et større fokusområde i nyere tid. Dette har en naturlig sammenheng med økt fokus på digitalisering i offentlig sektor og helsesektor hvor det holdes på sensitive pasientdata.

Andre kriterier har vært å gjennomsøke artikler for konsepter som vi mente var relevant for studien og konseptmatrisen basert på andre litteraturstudier og forskning vi har gjennomgått (kultur, retningslinjer, arbeidsflyt, opplæring, EPJ, osv.). Artikler har enten blitt inkludert som følge av at de oppfyller en rekke kriterier i henhold til tema og problemstilling, samt at de utgjør et breddegrunnlag som danner en forståelse av ulike problemstillinger som er knyttet til ISM og helsesektor. Utenom dette har inkludering/ekskluderingskriterier stort sett basert seg på å gjennomgå sammendrag/introduksjon og titler, samt søkeord for å identifisere de mest relevante artiklene.

I tidlig fase av arbeidet vårt utviklet vi en tabell for å holde styr på litteratursøkene vi tok for oss. Vi har dessverre ikke satt av ressurser til å dokumentere alle søk for hele prosjektet, men velger allikevel å presentere våre fem første søk som viser vårt utgangspunkt (*Tabell 4: Grafisk presentasjon av søkestrenger*).

| # | Primær-søkeord | Sekundær-søkeord | Data-base | Journal/konferanse | Treff |
|---|---|---|---|---|---|
| 1 | Information Security Management | ISM | ORIA | | 16 166 |
| 2 | Information Security | Healthcare / Health Care | Scopus | ICIS, ECIS, AMCIS, PACIS, MCIS, SCIS, HICSS | 55 |

| | | | | | |
|---|---|---|---|---|---|
| 3 | Information Security | Healthcare / Norway | Scopus | | 4 |
| 4 | Information Security Management | Healthcare / Health Care | Scopus | | 57 |
| 5 | Information Security | Health Care / Healthcare | AURA | | 3 797 |

*Tabell 4: Grafisk presentasjon av søkestrenger*

Tabellen viser en grafisk presentasjon av søkestrengene vi tok for oss oppstykket i primær- og sekundærsøkeord. I tillegg viser den hvilken database vi har utført søket i, eventuelle avgrensninger i form av filtrering til spesifikke journaler og konferanser, og hvor mange treff det ga. Det er primært sett disse databasene som er presentert i tabellen vi har hentet relevant litteratur fra gjennom hele prosjektet. Etterhvert som vi begynte å få kontroll på å metodene for å hente relevant litteratur og bestemme hvilke søkeord vi burde bruke, utviklet vi søkestrenger som tar for seg hver sin liste av journaler (*Tabell 5: Søkestrenger ut fra journaler*).

| # | Streng |
|---|---|
| 1 | ( TITLE-ABS-KEY ( "information security" AND "health care" OR "healthcare" ) AND ISSN ( 14769344 OR 13652575 OR 15265536 OR 15369323 OR 14664437 OR 07421222 OR 09638687 OR 21629730 ) ) |
| 2 | ( TITLE-ABS-KEY ( "information security" AND "health care" OR "healthcare" ) AND ISSN ( 15293181 OR 14717727 OR 09593845 OR 02684012 OR 19010990 OR 15401960 OR 15737551 ) ) |
| 3 | ( TITLE-ABS-KEY ( "information security" AND "health care" OR "healthcare" ) AND ISSN ( 13865056 OR 14726947 OR 13652648 OR 10675027 OR 17412811 OR 14388871 ) ) |

*Tabell 5: Søkestrenger ut fra journaler*

Disse strengene tar for seg «information security» som primærsøkeord og «health care/healthcare» som sekundærsøkeord. I tillegg filtrerer den søket til å kun vise journalene med de oppgitte ISSN-kodene. Hver enkelt streng er tildelt en fargekode lik den i tabellene fra forrige delkapittel (*kap. 2.1.1: Avgrensninger*). Dette gjør vi for å illustrere hvilken liste av journaler strengen tar for seg i et eventuelt litteratursøk.

## 2.2 **Tema**: Informasjonssikkerhet

Informasjonssikkerhet defineres av NIST (National Institute of Standards and Technologies) som beskyttelse av informasjon og systemer fra uautorisert tilgang, bruk, avsløring, forstyrrelse, modifikasjon eller ødeleggelse for å gi *konfidensialitet*, *integritet* og *tilgjengelighet (CIA)* (Nieles, Dempsey & Pillitteri, 2017, s. 7). The Committee on National Security Systems (CNSS) definerer informasjonssikkerhet som beskyttelse av informasjon og kritiske elementer, inkludert systemer og maskinvare som bruker, lagrer og overfører informasjonen (Whitman & Mattord, 2018, s. 11).

«CIA-triangelen» har blitt brukt som standarden for datasikkerhet både i privat og offentlig sektor siden utviklingen av stormaskiner. «CIA» baserer seg på de tre karakteristikkene som gir informasjon verdi for en organisasjon; konfidensialitet, integritet og tilgjengelighet. Den regnes forøvrig som en modell som ikke lenger er tilstrekkelig for å kunne adressere det stadig endrede sikkerhetsbildet som organisasjoner står ovenfor. Sikkerhetsbildet har endret seg mye med tiden, og har utviklet seg til å bestå av en rekke hendelser: som utilsiktet eller forsettlig skade, ødeleggelse, tyveri, utilsiktet eller

uautorisert endring, eller annen misbruk både fra menneskelig og ikke menneskelige faktorer (Whitman & Mattord, 2018, s. 11). Selv om CIA triangelen ikke lenger regnes som helt tilstrekkelig så kan den likevel være hensiktsmessig å gjøre rede for. Verdien av informasjon kommer fra karakteristikkene, når karakteristikken endres så endres verdien til informasjonen enten ved at den øker eller i de fleste tilfeller minsker. Karakteristikker endres under visse omstendigheter, som dermed påvirker verdien. Det kan for eksempel være når kritisk informasjon blir overført for sent, dermed mister informasjon verdi og hensikt (Whitman & Mattord, 2018, s. 16):

- **Tilgjengelighet**: Muliggjør at brukere av datasystemer får tilgang til informasjon uten forstyrrelser eller hinder og å få tilgang på informasjon i det nødvendige formatet.
- **Nøyaktighet**: Informasjon er nøyaktig når det er feilfritt og har verdien som brukeren forventer. Blir informasjonen modifisert eller endret så er den ikke lenger nøyaktig.
- **Autentisitet**: Informasjon er autentisk når informasjonen er genuin eller original, og ikke er en uekte kopi eller falsk. Informasjon er derfor autentisk når informasjon er i samme tilstand som når den ble laget, der den ble lagret og evt. hvor den ble overført. Eksempel på dette kan være spoofing av mailadresser (Whitman & Mattord, 2018, s. 15).
- **Konfidensialitet**: Informasjon har konfidensialitet når den beskyttes mot offentliggjøring, eller eksponering til uautoriserte individer eller systemer. Konfidensialitet sikrer at bare brukere med de rettigheter, privilegier og nødvendighet har tilgang til informasjonen. Konfidensialitet er nært beslektet med personvern og har høy verdi i henhold til sensitiv data om ansatte og pasienter, spesielt i organisasjoner som helseinstitusjoner. Brudd på konfidensialitet kan eksempelvis skje om en ansatt sender en mail med konfidensiell informasjon til noen utenfor organisasjonen, eller at sensitive dokumenter ikke holdes skjult og at man f.eks. kaster et sensitivt dokument uten å makulere.
- **Integritet:** Informasjon har integritet når den er komplett og ikke skadet. Korrumpering av data kan skje når informasjon lagres eller overføres, og kan skades av ondsinnet programvare og virus (Whitman & Mattord, 2018, s. 16-17).

### 2.2.1 Informasjonssikkerhet, samfunnsvitenskap og menneskelige faktorer

Samfunnsmessige faktorer påvirker hvordan individer forstår og bruker systemer som igjen påvirker informasjonssikkerheten til systemer og organisasjon. Individer oppfatter, resonnerer og gjør risikobaserte vurderinger forskjellig (Nieles et al., 2017, s. 11).

Boken til Whitman & Mattord (2018) beskriver ulike perspektiver på informasjonssikkerhet, deriblant informasjonssikkerhet som en samfunnsvitenskap. Det samfunnsvitenskapelige perspektivet undersøker menneskelige interaksjoner med informasjonssystemer men også samfunnssystemer. Informasjonssikkerhet begynner og slutter med menneskene i organisasjonen, det er de som interagerer med systemene. Sluttbrukere som trenger tilgang til den informasjonen det jobbes med å sikre vil kunne være det svakeste leddet. Ved å forstå atferdsmessige aspekter i organisasjonssammenheng og endringsledelse kan sikkerhetsadministratorer redusere risikoen assosiert med sluttbrukere og skape mer akseptable sikkerhetsmiljøer. Dette kombinert med hensiktsmessige policyer og opplæring vil bedre ytelsen til sluttbrukere og resultere i mer sikre informasjonssystemer (Whitman & Mattord, 2018, s. 42). Samfunnsmessige normer kan påvirke

informasjonssikkerhet både på en positiv og negativ måte. Eksempelvis vil det at brukere skriver ned passord og lar de ligge ved arbeidsstasjonen påvirke informasjonssikkerheten negativt, mens implementasjon av autentisering med flere faktorer vil påvirke informasjonssikkerheten positivt. Sikkerhet kan forbedre tilgang og flyt av data og informasjon ved å sikre mer nøyaktig og pålitelig informasjon og større grad av tilgjengelighet blant systemene. Sikkerhetsmekanismer kan forbedre individers personvern som for eksempel ved kryptering. Noen mekanismer kan innføre nye svakheter eller utfordringer slik som «single sign-on». Derfor bør det overveies hvorvidt sikkerhetsløsninger optimaliserer overordnede samfunnsmessige mål (Nieles et al., 2017, s. 11). Kultur og sikkerhetsmiljøet i organisasjonen spiller en viktig rolle i de ansattes risikovurdering. Utilstrekkelige sikkerhetsstandarder kan medføre svekkede holdninger informasjonssikkerhet i organisasjonen og ved oppdatert og gjentakende opplæring om akseptabel bruk av organisatoriske systemer bidrar til å beskytte systemets generelle sikkerhet (Nieles et al., 2017, s. 12).

Når mennesker bruker informasjonssystemer oppstår det feil og problemer, uerfarenhet, utilstrekkelig opplæring og feilaktige antakelser er blant faktorer som påvirker og forårsaker menneskelige feil. En av de største truslene for informasjonssikkerheten er de ansatte, fordi det er de som har tilgang til informasjonen. Menneskelige feil kan ofte unngås ved å ta i bruk opplæring, aktiviteter for å øke bevisstheten, og kontroller. Kontrollene kan være at en bruker må bekrefte en handling, skrive inn en kommando flere ganger, eller at man har systemer som overvåker menneskelig aktivitet (Whitman & Mattord, 2018, s. 80-81).

Informasjonssikkerhet bidrar til suksess i organisasjoner ettersom det gir et solid fundament for å øke effektivitet og produktivitet. Mange organisasjoner ser at overholdelse av informasjonssikkerhetsstandarder vil påvirke virksomhetsperspektiver. Å sikre informasjonsressurser mot uautorisert tilgang er viktig, og må dermed forvaltes på riktig og systematisk vis. Informasjonssikkerhet er også et svært komplekst område (Susanto & Almunawar, 2018). Organisasjoners manglende evne til å innføre tilstrekkelige sikkerhetsregler og prosedyrer vil kunne medføre negativ påvirkning på organisasjonens oppdrag, mens velvalgte sikkerhetsregler og prosedyrer som er satt på plass for å beskytte viktige ressurser («assets») understøtter det helhetlige organisatoriske oppdraget (Nieles et al., 2017, s. 7). I dag trues organisasjoner blant annet av ondsinnet programvare, systeminnbrudd og innsidetrusler, og sikkerhetsproblemer kan få alvorlige konsekvenser for lønnsomhet og organisasjonens rykte. Organisasjoner i privat og offentlig sektor forbedrer både lønnsomhet og tjenesteytelse til under når tilstrekkelig sikkerhetsbeskyttelse iverksettes. *«Information security, therefore, is a means to an end and not an end in itself»* (Nieles et al., 2017, s. 7).

### 2.2.2 Informasjonssikkerhetsledelse (ISM)

Organisasjoner bruker kontroller (sikringstiltak) for å forhindre innbrudd og beskytte informasjonseiendeler fra ulike trusler (Niemimaa, 2016; Smith, Winchester, Bunker & Jamieson, 2010). Organisasjoner trenger omfattende informasjonssikkerhetsledelse for å overvåke, velge ut og implementere effektiviteten av disse kontrollene. Ulike rammeverk har vært foreslått, som: ISO/IEC27001 og «System Security Engineering Capability Maturity Model» (Niemimaa, 2016). Forskning har tradisjonelt sett på informasjonssikkerhet som en teknisk problemstilling (Niemimaa, 2016; Siponen & Oinas-Kukkonen, 2007) men på bakgrunn av begrensningene som forekommer så har det i nyere tid blitt viet større fokus til informasjonssikkerhetsledelse (Niemimaa, 2016; Ransbotham &

Mitra, 2009).

Målet med informasjonssikkerhetsledelse er å beskytte konfidensialiteten, integriteten og tilgjengeligheten til informasjon og å begrense risikoer og trusler mot denne informasjonen (Tu & Yuan, 2014, s. 1). Informasjonssikkerhetsledelse kan dermed defineres som en systematisk prosess for å effektivt håndtere trusler og risiko mot informasjonssikkerheten i en organisasjon, gjennom anvendelsen av fysiske, tekniske og operasjonelle sikkerhetskontroller for å beskytte informasjonseiendeler og å oppnå forretningsmål. Informasjonssikkerhetsledelse er primært opptatt av av strategisk, taktisk og operasjonelle spørsmål i henhold til planlegging, analyse, design, implementasjon og vedlikehold av organisasjonens informasjonssikkerhetsprogram (Tu & Yuan, 2014, s. 1).

Det er avgjørende at organisasjoner finner en balanse mellom informasjonssikkerhetskrav og brukervennlighet (Nieles et al., 2017, s. 11). Ansatte foretrekker å utføre arbeidsoppgaver på den enkleste måten. Når ansatte står overfor et valg mellom den «offisielle» måten å utføre en arbeidsoppgave på og en enklere «uoffisiell» måte så vil det «uoffisielle» valget vinne. Den beste måten å løse dette på er å innlemme sikkerhet og brukervennlighet i informasjonssystemene, i sammenheng med opplæring, bevisstgjøring og tilstrekkelige kontroller (Whitman & Mattord, 2018, s. 109). Vil dette bidra til å minske mulige snarveier eller «workarounds».

Når nyansatte blir en del av organisasjonens kultur og arbeidsflyt bør de motta omfattende informasjonssikkerhetsorientering som en del av orienteringsprosessen. Retningslinjer bør forklares, samt prosedyrer for nødvendige sikkerhetsoperasjoner. I tillegg bør nivåene av autorisert tilgang beskrives for nyansatte, og opplæring gis i henhold til sikker bruk av informasjonssystemer. Gjennomgående orientering rundt rettigheter, ansvarsspørsmål og sikkerhetskomponenter anbefales også (Whitman & Mattord, 2018, s. 109). Sikkerhetsbevisstgjøring er blant de minst brukte men mest nyttige i en organisasjon. Bevisstgjøringskampanjer bidrar til at ansatte har en bevisst holdning til sikkerhet og er oppmerksomme på det. Dette kan blant annet bestå av nyhetsbrev, videoer, plakater og oppslagstavler. Spesielt nyhetsbrev er en kostnadseffektiv måte å sikre et bevisst forhold til informasjonssikkerhet (Whitman & Mattord, 2018, s. 213).

## 2.3 **Konsepter**: ISM og klinisk arbeidsflyt

Ut fra tidligere litteratur har vi satt opp en konseptmatrise som bidro til at vi kunne holde kontroll og oversikt over hvilken litteratur som omtaler hvilke av konseptene vi er ute etter. Matrisen tar for seg artikkelnummer hvorav rekkefølgen ble fulgt gjennomgående i arbeidet for å holde oversikt, sammen med forfatteren(e)s navn. Utfylt konseptmatrise med våre 20 utvalgte artikler presenteres senere i kapittelet (*kap. 2.4: Litteraturgjennomgang*).

| | | **Konsepter** | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | **Formell praksis** | | **Uformell praksis** | | **Teknisk praksis** | | *Klinisk arbeidsflyt* |
| **#** | **Forfatter** | *Kunnskap* | *Retningslinjer* | *Kultur* | *Tillit* | *EPJ* | *Tilgangsstyring* | |

*Tabell 6: Konsepter*

Konseptene er definert og valgt ut fra litteraturen som vi finner relevant for vår problemstilling. I denne sammenhengen vurderer vi konseptet **klinisk arbeidsflyt** som et kontrollerende/kontekstuelt konsept. Vi ønsket å påse at litteraturen vi fant for ISM var i tilstrekkelig grad rettet mot det vi ønsket å teste i studien. Ut fra dette har vi kunne sett til litteraturen for å finne hvilke konsepter som har en direkte relasjon til arbeidsflyt i form av at den påvirkes av ulike organisatoriske praksiser for sikring av informasjon. Vi har videre definert relaterte/tilhørende konsepter på bakgrunn av litteraturen, i tillegg til å vurdere konseptets aktualitet, samt relevans i forhold til å fylle et tomrom i arbeidet mot videre forskning innenfor temaet ISM i en kontekst av helsesektoren.

Vi gjør oppmerksom på at mange av konseptene har en større eller mindre grad av tilhørighet til hverandre ved at de utgjør en direkte eller indirekte relasjon eller avhengighet. Vi eksemplifiserer og understreker dette senere i kapittelet hvor vi presenterer resultater fra litteraturstudien.

***ISM**:*

- **Formell praksis**: En kategori for formelle rutiner og praksiser i organisasjoner. For dette konseptet har vi definert følgende underkategorier/-konsepter:
    - **Kunnskap**: En organisasjon er aldri sterkere enn sitt svakeste ledd. Å tilegne de ansatte kunnskap og bevisstgjøre dem rundt sikkerhetsrutiner i sine arbeidsprosesser er fullstendig kritisk for en organisasjon. Kunnskap refererer til opplæring, kursing, taus og eksplisitt kunnskap som besittes av organisasjonen og dens ansatte. Vi mener at organisasjoners håndtering av ansattes kunnskap om sikring av informasjon og bruk av systemer er en faktor som kan ha stor innflytelse på klinisk arbeidsflyt.
    - **Retningslinjer**: Basert på rammeverkets andre punkt (organisatoriske retningslinjer). Noe som ofte defineres fra toppledelsen og ned for å påse at organisasjonen tar for seg standarder som følges på tvers av avdelinger og nivåer i dem. Retningslinjer vil variere i ulike organisasjoner i henhold til viktigheten, og hvor sensitiv data de besitter. Retningslinjer kan eksempelvis være HIPAA (Health Insurance Portability and Accountability Act) eller ISO 27000-standarder. Retningslinjer kan også bestå av andre organisatoriske retningslinjer for hvordan ansatte skal opptre og bruke IT-verktøy på arbeidsplassen, i tillegg til prosedyrer for å sikre informasjon/data.

- **Uformell praksis**: En kategori for uformelle rutiner og praksiser i organisasjoner. For dette konseptet har vi definert følgende underkategorier/-konsepter:
    - **Kultur**: Kultur i arbeidsmiljøet viser til organisasjonskultur blant ansatte i møte med informasjonssikkerhet. Kultur i arbeidsmiljøet påvirker holdninger som igjen kan påvirke informasjonssikkerhet, vi har dermed en teori om at kultur påvirker, ikke bare klinisk arbeidsflyt direkte, men også rutiner for ISM som igjen kan påvirke den kliniske arbeidsflyten. En utslagsgivende faktor for hvordan de ansatte tilegner seg kunnskap og utfører arbeidsprosesser.
    - **Tillit**: I forhold til sikkerhetsaspektet anser vi tillit innad i organisasjonen som en tilleggende viktig faktor. En organisasjon er fullstendig avhengig av at klinisk ansatte, mellomledere og toppledere har tillit til hverandre for at rutiner og tiltak skal kunne oppnå sine formål og hensikter. Vel så viktig er det at de ansatte som systemenes brukere har tillit til systemene.

- **Teknisk praksis**: En kategori for tekniske rutiner i organisasjoner. Den omhandler organisasjonens bruk av teknologi; blant annet helseinformasjonssystemer (HIS) og underliggende systemer, samt funksjoner og programmer for å sikre elektronisk informasjon. For dette konseptet har vi definert følgende underkategorier/-konsepter:
    - **EPJ**: Står for elektronisk pasientjournal (EPJ), i engelskspråklig litteratur ofte omtalt som *Electronic Health Record (EHR)* og *Electronic Medical Record (EMR)*. Et spesifikt HIS som alle klinikere er avhengige av i deres arbeidshverdag. Denne underkategorien viser til selve systemet; dets sikkerhet og effektivitet i forhold til plattformer det kjøres på, utvikling, osv. Vi tenker også at i denne faktoren inngår brukervennlighet og øvrige faktorer som påvirker funksjonaliteten som igjen kan påvirke klinisk arbeidsflyt og effektivitet i arbeidsprosesser.
    - **Tilgangsstyring**: Innloggingsrutiner, autorisering, autentisering og lignende funksjoner som definerer sikkerheten for et HIS (høyst relevant for EPJ-system). Det finnes ulike definerte standarder innen retningslinjer for tilgangsstyring som presentert i *kap. 2.4.2.1 (Retningslinjer))*. Uansett hvilke standarder man følger, er tilgangsstyring en sterkt utslagsgivende faktor for organisasjonens håndtering av sikkerhet (ISM) og klinikernes flyt i arbeidsprosesser (klinisk arbeidsflyt). Man kan argumentere for at konseptet er vel så mye en formell som teknisk sikkerhetspraksis. Vi har lagt det under teknisk for å gjøre konseptmatrisen mest mulig oversiktlig.

***Kontekstuelt konsept**:*

- **Klinisk arbeidsflyt**: Konsept for å kontrollere kontekst for litteraturen – begrepet tar for seg effektivitet i klinikernes arbeidsprosesser, både i henhold til tidsforbruk og produktivitet. Et aspekt som påvirkes av andre aspekter som fremkommer av organisatoriske tilnærminger til ISM som presentert over.

## 2.4 Litteraturgjennomgang

I dette delkapittelet presenterer vi en gjennomgang av sentral forskningslitteratur for konseptene som vi også vil ta i bruk til sammenlikning med våre resultater i det vi kaller testing av eksisterende teori. Dette skriver vi mer om i neste kapittel (*kap. 3.1: Strategi: Case-studie*). Vi fylte inn den tidligere nevnte konseptmatrisen med 20 artikler vi anså som mest relevante for arbeidet mot vår problemstilling (*Tabell 7: Konseptmatrise*). Vi utarbeidet også en liste som tar for seg artiklene sammen med hvilket årstall de er publisert og i hvilken journal/konferanse de presenteres *(kap. 8.2: Liste over artikler med journaler)*.

| # | Forfatter | Konsepter | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | Formell praksis | | Uformell praksis | | Teknisk praksis | | ***Klinisk arbeidsflyt*** |
| | | *Kunnskap* | *Retningslinjer* | *Kultur* | *Tillit* | *EPJ* | *Tilgangsstyring* | |
| 1. | Hou et al. | X | X | X1 | | | | |
| 2. | Bekkevik et al. | X | X | X | | | | X |
| 3. | McLaughlin et al. | X | X | X1 | X | | X1 | X |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 4. | Tu & Yuan | X | X | X | | | X1 | X |
| 5. | Faxvaag et al. | X2 | X1 | X2 | X2 | X | X | X |
| 6. | Smaradottir | | X | | | X | X | X |
| 7. | Anderson et al. | X | X | X1 | X1 | X1 | X1 | |
| 8. | Huson & Hewitt | X1 | X | | X1 | | X1 | |
| 9. | Hedström et al. | | X | X1 | | | X | |
| 10. | Hassan et al. | X | X | X | X | | | |
| 11. | Stahl et al. | | X | | | | | |
| 12. | Ferreira et al. | X1 | X | | X | X | X | X |
| 13. | Luethi et al. | X | X | | X | X3 | X | X |
| 14. | Sunyaev et al. | X1 | X | | | | | |
| 15. | Van Devender et al. | X1 | | | | X | | |
| 16. | Nemati et al. | X | X | X | | | | |
| 17. | Sedlack | X | X | | | X2 | X1 | |
| 18. | Kisekka et al. | X | X | | | X | | X |
| 19. | Martin et al. | X | X | | | | X2 | |
| 20. | Elmrabit et al. | X | X | X3 | X | | X | |

*Tabell 7: Konseptmatrise*

Matrisen har gjort vår innledende forskning med litteraturstudie mye enklere og mer oversiktlig å håndtere, ettersom vi enkelt kunne se hvilke artikler vi kunne finne stoff for hvert av konseptene. Underveis i gjennomgangen av litteraturen oppdaget vi at det kunne være hensiktsmessig å utvikle noen alternative kategoriske avkrysninger:

- **X1** = blir nevnt i artikkelen, men ikke spesielt vektlagt.
- **X2** = nevnes ikke, men omhandler
- **X3** = ikke spesielt vektlagt, men har gode kilder

Disse har som hensikt å gi oss en mest mulig oversiktlig og forklarende konseptmatrise, i form av at den blir mer presiserende enn kun gjennom enkel avkrysning.

### 2.4.1 Teknisk praksis

Vi kan av konseptmatrisen se at vi har funnet en del litteratur som omhandler teknisk sikkerhetspraksis som også omhandler formell og uformell praksis. På denne måten kan vi se sammenhengen i temaet som utgjør ISM. Tekniske praksiser for organisasjoner er gjerne veldig situasjonsbetinget, og det har vært viktig for oss å kontrollere at emnet snakkes om med hensyn til helsesektoren, noe vårt kontekstuelle konsept har bidratt med. Vi tar i dette delkapittelet for oss relevant litteratur for to konsepter som vi har ansett som representative for kategorien «teknisk praksis».

#### *2.4.1.1 Tilgangsstyring*

Tilgang er muligheten til å benytte seg av hvilken som helst systemressurs. Tilgangsstyring er prosessen med å innvilge eller å nekte spesifikke forespørsler til å: 1) skaffe og bruke informasjon og relaterte informasjonsprosesseringstjenester. 2) Tilgang til fysiske anlegg/bygg, som i militære anlegg eller føderale bygninger. System-basert tilgangsstyring kalles for logisk tilgangsstyring. Logisk tilgangsstyring kan autorisere hvem eller hva som har tilgang til en spesifikk systemressurs, og hvilke typer tilgang som tillates. Disse kontrollene kan være bygd inn i operativsystemer, inkorporert i applikasjonsprogrammer og større systemer som DBMS, eller implementert gjennom tilleggspakker. Logisk tilgangsstyring kan implementeres internt i systemer eller gjennom eksterne enheter. Eksempler på kontroller for tilgangsstyring: kontoadministrasjon, separering av plikter, «principle of least privilege», «session lock», «information flow control» og «session termination». Organisasjoner begrenser dermed: systemtilgang til autoriserte brukere, prosesser som utføres på vegne av autoriserte brukere, enheter og i tillegg andre systemer samt typer hvilke transaksjoner og funksjoner som autoriserte brukere har lov til å utføre (Nieles et al., 2017, s. 59).

Vi fikk tidlige indikasjoner gjennom forskningslitteratur og forstudier på at blant annet tilgangsstyring og autentisering kan være en viktig faktor, som deriblant kan føre til interessekonflikter mellom hensyn til informasjonssikkerheten og arbeidsflyten til de ansatte. Som artikkelen «The authentication dilemma» av Wiercioch, Teufel & Teufel (2018) påpeker: «*Several studies have shown that users consciously refrain from using security measures because they rate practicability higher than security [...] From a user's perspective, the cost of strong passwords outweighs the potential benefits or protection from potential attack»* (Wiercioch et al., 2018, s. 278).

Tilgangsstyring krever opplæring av brukere og påvirker arbeidsflyt og daglige rutiner for helsepersonell. Brukervennligheten til tilgangsstyringsløsninger påvirker akseptansebarrieren (Smaradottir, 2018).

En empirisk studie av Alhaqbani og Fidge (2007) presenterer de tradisjonelle sikkerhetsmodellene for tilgangsstyring. De bruker så en case-studie til å demonstrere at ingen av modellene egenhendig er tilstrekkelige i forente miljøer for helse og omsorg (Alhaqbani & J. Fidge, 2007).

En norsk studie utført ved NTNU (EHR Research Centre og andre avdelinger/fakulteter) undersøkte helsepersonell ved sykehjem og sykehus, samt deres holdninger til og erfaringer ved bruk av tilgangsstyring for systemer som elektroniske pasientjournaler (EPJ). Forfatterne understreker viktigheten av å ha tilgang til oppdatert informasjon om pasienter, men samtidig være beskyttet mot uautorisert tilgang. Det er en balansegang mellom sikkerhet og tilgang (konfidensialitet/tilgjengelighet) som blant annet må kontrolleres gjennom mekanismer for autentisering og autorisering av adgang. *«Many studies have addressed how access control mechanisms should influence on the information working conditions of healthcare professionals, but little is known on how such mechanisms actually influences on the work of healthcare personnel.»* (Faxvaag, Johansen, Heimly, Melby & Grimsmo, 2011, s. 602). Artikkelen av Faxvaag og kolleger (2011) presiserer at mange studier er gjort i forhold til mekanismer for tilgangsstyring og deres påvirkning på arbeidsforholdene innen informasjonshåndtering, men det er lite kunnskap om hvordan dette påvirker helsepersonalets arbeid (Faxvaag et al., 2011, s. 601-604).

Gjennom ti år har forskerne kartlagt helsepersonells bruk av EPJ-systemer, og uformelle observasjoner har indikert at det finnes ulike problemer med tilgangsstyring for EPJ-systemer i forhold til informasjons- og dokumentasjonsarbeid. Det ble således utformet et spørreskjema, der 45 av 430 kommuner ble utvalgt for å representere det nasjonale gjennomsnittet, hvorav 29 sykehjem og 21 sykehus var blant utvalget som mottok spørreskjemaet. Resultatet viste blant annet at majoriteten mente at det tok for lang tid å bruke mekanismer for tilgangsstyring; 60 % av sykehjem og 62 % sykehus' helsepersonell mente at det tok for lang tid å logge inn. Informasjonssikkerhetsreglementet pålegger brukere å logge ut av systemet etter bruk ettersom dette omhandler klinisk dokumentasjon og sensitiv pasientinformasjon. Derimot viser denne undersøkelsen at 36 % av respondentene i sykehjem og 45 % av respondentene på sykehus opplevde at de måtte logge ut andre før de kunne sette i gang med eget arbeid. 46 % av respondentene rapporterte at den langsomme prosessen med innlogging førte til at de ikke alltid rakk å lese pasientjournaler før de skulle se til pasienter, og at dokumentasjonsarbeid ofte ble utsatt til de hadde tid (Faxvaag et al., 2011, s. 603).

Studien viser at selv om det eksisterer formelle krav og reglementer i henhold til informasjonssikkerhet i helsesektor, kan disse bli overstyrt av personalet dersom informasjonssystemene ikke oppleves som funksjonelle og effektive. De opplevde at arbeidet ble ineffektivt og tregere av de etablerte sikkerhetsmekanismene og dermed fungerte mot sin hensikt. Dette medfører blant annet ulike vurderinger som kan betegnes som risikable for pasient- og informasjonssikkerheten ved sykehus/sykehjem (som at en større andel opplevde at andre ikke logget ut av EPJ-systemene). Dette medfører igjen risiko for pasienter fordi deres journaler potensielt kan aksesseres av uvedkommende. I tillegg til at pasientenes journaler potensielt ikke blir gjennomgått skikkelig før de blir behandlet.

#### *2.4.1.2 EPJ*

Helseinformasjonsystemer spiller en viktig rolle innen kommunikasjon og koordineringsprosesser for helse- og omsorgstjenesten og anvendelsen av informasjonsteknologi samt overgangen fra papirbaserte pasientjournaler til elektroniske pasientjournaler påvirker klinisk arbeidsflyt og daglige rutiner i helsetjenester. Implementering og bruk av forskjellige typer EPJ- og informasjonssystemer innfører utfordringer iht. personvern og sikkerhetsledelse i helsevesen. Organisasjoner må derfor innføre strategier for å håndtere sikkerhet og personvern som følge av helseinformasjonsystemer. Informasjon må også være tilgjengelig og lesbar for helsepersonell for å kunne sikre tilstrekkelig pasientbehandling (Smaradottir, 2018).

I en kvantitativ studie undersøkte Kisekka med kolleger (2015) helsepersonells oppfatninger av funksjonene i et EPJ-system og hvorvidt de ulike funksjonene medfører organisatorisk motstandskraft i et scenario hvor man har hatt et sikkerhetsbrudd i EPJ-systemet. Av resultatene fra spørreskjemaet fant forfatterne at helsepersonell anser informasjonsvern som det mest kritiske, vurdert over informasjonstilgang og informasjonssikkerhet (Kisekka, Sharman, Rao, Upadhyaya & Gerber, 2015).

Van Devender og kolleger (2016) presenterer en spådom fra Federal Bureau of Investigation (FBI) om at fristende muligheter til utnyttelse vil kunne skapes i programvare og medisinske enheter når organisasjoner går over til EPJ-miljøer (Van Devender, Campbell, Glisson & Finan, 2016). Ut fra en case-studie med bruk av ulike datamaskiner, oppdaget forfatterne også at Windows XP på maskiner som kjører EPJ-system(er) utgjør en sårbarhet, ettersom Microsoft sluttet å støtte Windows XP helt tilbake i april 2014 (Microsoft, 2014; Van Devender et al., 2016, s. 7). Heller ikke Windows Vista kan lenger

anses som et sikkert operativsystem å drifte EPJ-systemer på, etter at Microsoft også avviklet støtte til dette operativsystemet tilbake i april 2017 (Microsoft, 2017).

### 2.4.2 Formell praksis

Konseptmatrisen (*Tabell 7: Konseptmatrise*) viser at vi sitter på mye litteratur som omhandler formell praksis for sikkerhetsrutiner. Vi mener metodene vi har brukt for innhenting av de ulike artiklene på ingen måte har favorisert denne kategorien, og vi kan på grunnlag av dette konkludere med at tidligere forskning har dekket godt oppunder formell praksis for sikkerhetsrutiner i en kontekst av helsesektoren. Vi tar i dette delkapittelet for oss relevant litteratur for to konsepter (*retningslinjer* og *kunnskap*) som vi har ansett som representative for kategorien «formell praksis».

#### *2.4.2.1 Retningslinjer*

Sikkerhetsretningslinjer definerer hvordan produsere, lagre og bruke sensitive data i en organisasjon. Det finnes 3 ulike varianter av sikkerhetsretningslinjer (Smaradottir, 2018):

1. Verbalt ustrukturert
2. Strukturert
3. Skjemaer eller formelle modeller

Sikkerhetsretningslinjer brukes til å kontrollere tilgang, autentisere for forespurt data og beskytte sensitiv data. Konfidensialitet innen EPJ-systemer utgjør informasjonspersonvern, som betyr at adgang begrenses til autoriserte brukere. Den vanligste autentiseringsmodellen i helsetjenester er en identifikator og passord. Revisjonslogger er også viktig ettersom autoriserte brukere kan få tilgang til rettigheter og forårsake sikkerhetsbrudd (Smaradottir, 2018).

#### *2.4.2.2. Kunnskap*

Organisasjoners informasjonssikkerhetsstrategi bør adressere menneskelige faktorer som bevissthet rundt informasjonssikkerhet og opplæring, for å bli bevisst på sikkerhetstrusler og dermed tilegne ansatte i organisasjonen grunnleggende kunnskap (Culnan, Foxman & W. Ray, 2008; Tu & Yuan, 2014, s. 4). Alle relevante grupper i organisasjonen bør tilbys tilstrekkelig med opplæring slik at de vil være i stand til å kunne identifisere risikoer effektivt samt å beskytte deres informasjon (Straub & Welke, 1998; Tu & Yuan, 2014, s. 8).

Bevisene peker på at det er vanskelig å implementere tilstrekkelige sikkerhetskontroller dersom ikke opplæring tilbys: *"Empirical evidence indicates that it will be difficult to implement security controls if people have insufficient training about best IT security practices"* (S. M. Furnell, Clarke, Werlinger, Hawkey & Beznosov, 2009; Tu & Yuan, 2014, s. 9).

I Bekkevik et al. (2018) foreslås det – basert på litteraturstudien – å legge til rette for "information security awareness" (ISA), noe som direkte eller indirekte kan påvirke holdninger til Informasjonssikkerhet (Bekkevik et al., 2018, s. 7; Bulgurcu, Cavusoglu & Benbasat, 2010). Man bør dermed forsikre at man har rett tankesett og at man således jobber for sikkerhetsrutiner, og ikke mot dem (Bekkevik et al., 2018, s. 7; S. Furnell & Thomson, 2009). For å få mest mulig fordeler og utbytte av sikkerhetsopplæring, bør kursprogrammer og opplæring skreddersys av organisasjonen. I tillegg bør

ikke sikkerhet bli ansett som en byrde, men som en del av daglige arbeidsrutiner, slik at ansatte vil utvikle kompetanse og å få tiltro til deres egne ferdigheter (Bekkevik et al., 2018, s. 7).

Det kan også innføres informasjonssikkerhetssystem som kan lagre og distribuere informasjonssikkerhetsretningslinjer, det kan bør også overveies muligheten for å innføre e-læringsinitiativer som omfatter hele organisasjonens sikkerhetspraksis, tiltakene kan ifølge forfatterne tilby gode opplevelser for opplæringstiltak innen Informasjonssikkerhet, i tillegg til at man har en felles plattform for å gi og motta tilbakemeldinger og å kunne ha tilgang til alle retningslinjer på en plass (Bekkevik et al., 2018, s. 8; J. M. Hagen & Albrechtsen, 2009).

E-læringsprogrammer for sikkerhet kan få ansatte til å ta ansvar for egne læringsprosesser (Bekkevik et al., 2018, s. 8; J. M. Hagen & Albrechtsen, 2009). Implementering av et omfattende e-læringsinitiativ kan bidra til forbedringen av sikkerhetskultur (Bekkevik et al., 2018, s. 8; J. Hagen, Albrechtsen & Ole Johnsen, 2011). Ledelsen kan promotere og støtte grupper eller sub-kulturer som viser størst interesse for informasjonssikkerhet, eksempelvis gjennom å motivere dem til å overtale andre til å være oppmerksomme på sikkerheten i organisasjonen (Bekkevik et al., 2018, s. 8; da Veiga & Martins, 2017).

Litteraturstudien av Bekkevik og kolleger (2017) adresserer 9 forskjellige initiativer for å imøtekomme utfordringer i henhold til informasjonssikkerhetspraksis i organisasjoner (Bekkevik et al., 2018, s. 6):

- Organisatorisk støtte og samarbeid
- Opplæring og bevissthet
- Belønning eller straff
- Tilstrekkelige sett av komponenter for informasjonssikkerhet
- Rammeverk for bevissthet rundt sikkerhet
- Implementering av systemer for informasjonssikkerhet
- Vurdere, måle og forbedre tiltak
- Individuelle kurs og opplæringsprogrammer

### 2.4.3 Uformell praksis

Vi kan av konseptmatrisen (*Tabell 7: Konseptmatrise*) se tendenser av et større gap i tidligere forskning hva gjelder uformell praksis, kontra formell praksis. Deler av dette kan trolig forklares ved at formell praksis utgjør en mer direkte relasjon til ISM og klinisk arbeidsflyt enn uformell praksis, og at publiseringene innen forskningstemaet først fikk et oppsving for omlag 15 år siden. Vi mener allikevel at uformell praksis har en avgjørende samhørighet med formell praksis ved at deler av praksisene er avhengige av hverandre (e.g.: generert kunnskap gjennom kursing og opplæring bygger kultur. Evt.: tillit blant de ansatte bygger kunnskap og gode retningslinjer). Vi tar i dette delkapittelet for oss relevant litteratur for to konsepter (*kultur* og *tillit*) som vi har ansett som representative for kategorien «uformell praksis».

#### *2.4.3.1 Kultur*

I en kvalitativ studie av Hassan og kolleger (2017) som tok for seg aspektet kultur innen miljøer for helseinformatikk, konkluderte forfatterne med at bevissthet, kunnskap og oppførsel er de tre viktigste faktorene innen kultur for informasjonssikkerhet. Forfatterne understreker viktigheten av å engasjere

toppledelsen for å forsikre at kulturen er dyrket blant helsepersonalet (Hassan, Maarop, Ismail & Abidin, 2017).

Litteraturstudien til Bekkevik, Holm, Vassilakopoulou og Hustad (2017) beskriver hvorfor det kan være utfordrende å etablere en sikkerhetskultur:

> *Not all employees understand organizational security as part of their daily work practice. Security managers fail to implement a security culture in the organization because of different understandings about security issues among organizational groups, as well as the distance between the management and the hierarchical levels.*

Litteraturstudien viser til at sikkerhetsbrudd kan skje på bakgrunn av dårlig sikkerhetskultur ettersom ansatte kan bryte reglene uten å vite om det. Dette vil kunne utsette organisasjonen for risiko, eksempler på dårlig sikkerhetskultur er: man lar være å låse/logge ut PC'er etter bruk eller når man forlater kontoret, skriver ned passord, og deler kontoinformasjon med andre ved forespørsel. Grunnen til at slike scenarier skjer er ofte at tilstrekkelig opplæring ikke har blitt gitt og at ansatte ikke har nok kunnskap rundt IT sikkerhetsreglement. Dette er i mange tilfeller grunnen til at ansatte blir lurt av e-poster med skadelig programvare og manipulert på andre måter (Bekkevik et al., 2018, s. 6).

I litteraturstudien til Bekkevik et al. (2017) presenteres forslag fra Hagen et al. (2009) om å fremheve sikkerhetskultur ved å rette fokus mot en gruppe ansatte av gangen. Dette vil ifølge forfatterne bidra til en positiv sikkerhetskultur ettersom ansatte selv vil velge å etterkomme anbefalt sikkerhetspraksis i henhold til deres arbeidspraksis, det blir også understreket at ledelsen bør oppfordre ansatte til å delta på informasjonssikkerhetskurs for å anskaffe seg nødvendig kunnskap (Bekkevik et al., 2018, s. 6; J. M. Hagen & Albrechtsen, 2009).

#### *2.4.3.2 Tillit*

I en kvantitativ studie av Ferreira med kolleger (2010) ble det utviklet et spørreskjema hvorav helsefagpersonell deltok som respondenter. Spørreskjemaet tok blant annet for seg et fiktivt scenario hvor respondentene ble bedt om å ta stilling til hvorvidt pasienter burde kunne aksessere sine pasientjournaler gjennom en minibank. Av 23 respondenter som tok stilling til spørsmålet, svarte 17 av dem at dette ikke er en god metode, der 13 av svarene ble begrunnet med etiske problemstillinger og ytterligere 13 med mangel på sikkerhet (flere alternativer kunne krysses av). Som oppfølgingsspørsmål ble respondentene bedt om å ta stilling til hvorvidt de mener minibanken utgjør et sikkert system, hvorav 18 av 25 svarte nei (Ferreira et al., 2010).

I sin eksplorative sammenligning av sykehus i Sveits og USA, presenterer Luethi og Knolmayer (2009) prinsipper for sikkerhetsretningslinjer. Blant disse er tilgangsstyring og informasjonsflyt, og det siste defineres som *trusted computing base* (TCB). TCB innebærer at datasystemer som håndterer personlig helseinformasjon skal ha et delsystem som håndhever hvert av prinsippene på en effektiv og sikker måte (Luethi & Knolmayer, 2009).

Elmrabit og kolleger (2015) gjennomførte en litteraturstudie som tar for seg innsidetrusler innen ISM. Forfatterne konkluderer med at tillit er en vanskelig problemstilling som innebærer at forskere ser på problemet fra et holistisk perspektiv, henholdsvis i form av menneskelig atferd, teknologiske kontroller og organisatoriske aspekter (Elmrabit, Yang & Yang, 2015).

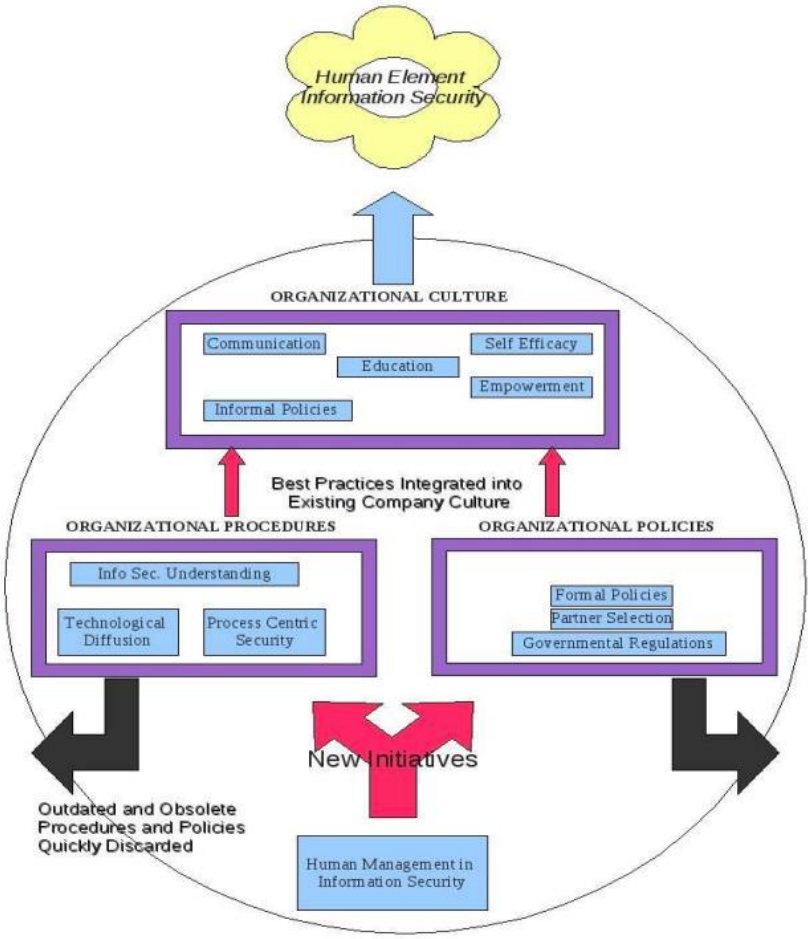
### 2.4.4 Klinisk arbeidsflyt

Tilgangsstyring i helsetjenester skaper ofte barrierer for aksept og de er koblet til brukbarhetsproblemer som påvirker klinisk praksis og arbeidsflyt. Retningslinjer for tilgangsstyring burde utformes og distribueres med utgangspunkt i helsepersonellets behov og arbeidsflyt, henholdsvis for å forårsake færre problemer for deres adgang til informasjon relatert til arbeidsoppgaver, samt øke effektiviteten (Ferreira et al., 2010). Ved utformingen av løsninger for tilgangsstyring burde sluttbrukere inviteres til å delta i prosessen for å redusere barrierer for aksept, samt forenkle implementeringen og opplæringen for å ta i bruk løsningen. Til utformingen foreslås bruk av fokusgrupper og spørreskjema for å samle informasjon om brukernes behov og deres arbeidsprosesser, både for å øke sannsynligheten for at implementeringen av sikkerhetsløsninger lykkes, samt redusere problemer relatert til opplæring og arbeidsflyt (Smaradottir, 2018).

## 2.5 Konseptuelt rammeverk

Litteraturstudien skal hjelpe til å bidra med et konseptuelt rammeverk for forskningen vår. Store deler av det konseptuelle rammeverket er utledet – og rettferdiggjort – gjennom en studie av litteraturen (Oates, 2006, s. 34-35).

I studien vår har vi tatt særlig utgangspunkt i et spesifikt rammeverk presentert av Nemati & Church (2009) (*Figur 1: "A Human Centered Framework for Information Security Management"*). Denne artikkelen er også inkludert i vår liste over utvalgte artikler *(Tabell 7: Konseptmatrise)*.




*Figur 1: "A Human Centered Framework for Information Security Management" (Nemati & Church, 2009, s. 3)*

Studien innledes med: *"Research on the human element of information security is fragmented at best"* (Nemati & Church, 2009, s. 1) og presenterer et ledelsesrammeverk for helseforetak som ønsker å forbedre deres informasjonssikkerhetsprosedyrer for å overholde HIPAA (Health Insurance Portability and Accountability Act) og andre forskrifter/reguleringer. Artikkelen vektlegger å sikre en organisasjon fra interne trusler ved å lære opp ansatte til å bygge en organisasjonskultur hvor sikkerhetsinitiativer blir verdsatt og respektert. Den kulturelle tilnærmingen er viktig å vektlegge for å sikre et allsidig sikkerhetsmiljø som er i stand til å overholde strenge reguleringer (Nemati & Church, 2009, s. 1).

Forfatterne foreslår følgende modell oppdelt i tre komponenter (Nemati & Church, 2009, s. 3-4):

- **Organisatoriske retningslinjer** er ansett som de metoder som implementeres og integreres med bedriftskultur. Et nytt system kan ha retningslinjer for tilgangsstyring; retningslinjene bør da ha en forutsetning om at tilgangen er midlertidig, men samtidig bør en prosedyre vedtas til trening og opplæring rundt et system. På denne måten blir ansatte en del av allsidige og effektive retningslinjer for sikkerhet.
- **Organisatoriske prosedyrer** omhandler design av systemer og sikkerhetsmaskinvare og infrastruktur for menneskelige brukere. Sikkerhet anses som en forretningsprosess, der organisasjonen har et kulturelt synspunkt på systemer og sikkerhet, uavhengig av teknologi.

Systemer designes for å integrere sikkerhetsmekanismer sømløst og usynlig overfor deres brukere.

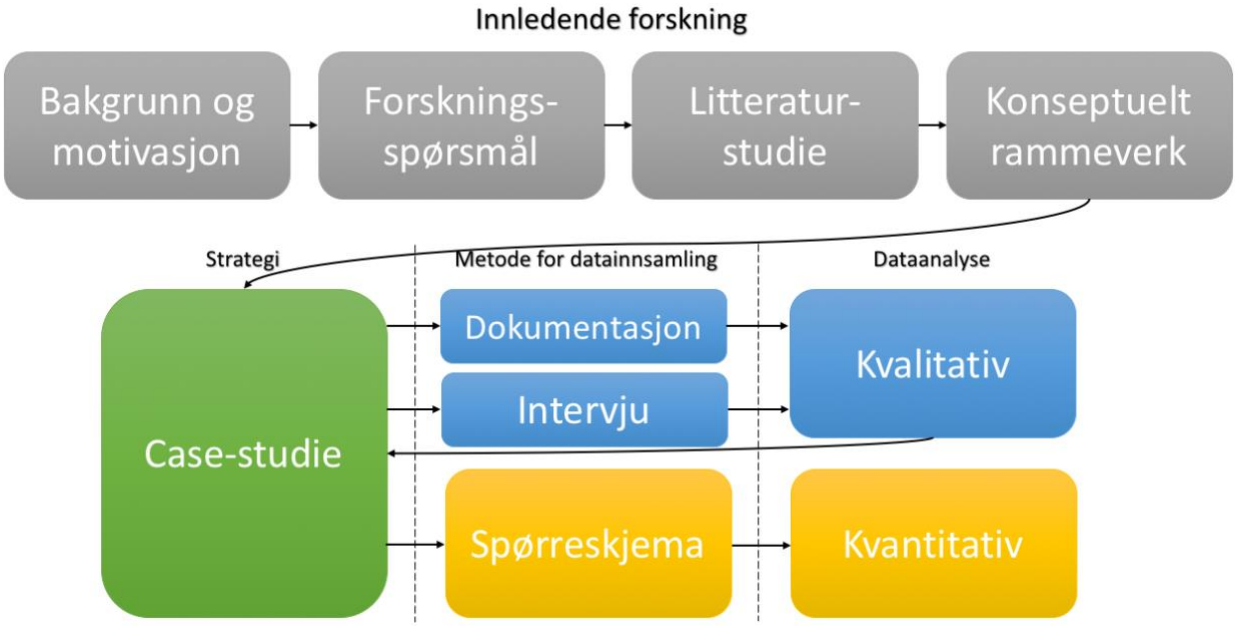
- **Organisasjonskultur** vektlegger opplæring av ansatte og deres selvstendighet til å følge opp informasjonssikkerhet. Organisasjonskultur vektlegger brukeropplæring, informasjon, selvstendighet og selvmestring for å styrke lagarbeid.

For vår egen tolkning av modellen henviser vi til neste kapittel, der vi presenterer vår egen skreddersydde forskningsmodell med utgangspunkt i de ovennevnte komponentene *(kap. 3.2.2: Kvantitativ analyse)*.

# 3. Forskningstilnærming og -kontekst

I dette kapittelet vil vi forsøke å beskrive hvordan vi har valgt å gå frem i arbeidet vårt mot å besvare forskningsspørsmålet og med det belyse problemstillingen. Vi har gjennom forskningsarbeidet vårt hatt et kontinuerlig rettet fokus mot å påse at forskningsarbeidet vårt utføres på en etisk riktig måte i henhold til formelle krav, noe vi går nærmere inn på avslutningsvis i kapittelet.

Vi har forsøkt å fremstille forskningsprosessen vi har fulgt for prosjektet vårt i en grafisk modell. Modellen er en skreddersydd versjon basert på elementer presentert av Oates (2006) i *«Model of the research process»* (Oates, 2006, s. 33).




*Figur 2: Forskningsprosessen*

Modellen *(Figur 2)* tar for seg fire periodiske faser for forskningsprosessen; innledende forskning, strategi, metode for datainnsamling og dataanalyse. Pilene illustrerer hvordan prosessene har forløpt i prosjektet fra start, med *bakgrunn og motivasjon* til slutt, med *kvantitativ dataanalyse*.

Vi påbegynte forskningsprosjektet med å diskutere hva vi ønsket å forske på, samt bakgrunn og motivasjon for å forske på det. Dette la grunnlaget for defineringen av forskningsspørsmålet som prosjektet har hatt som formål å besvare, som igjen la grunnlaget for en avgrenset litteraturstudie hvorfra vi hentet et passende rammeverk til å bruke som forklaringsmodell i studien vår. Dette har vi rapportert om tilbake i første kapittel (*kap. 1: Innledning*).

Når forskningsspørsmålet var utarbeidet, kunne vi begynne å se etter litteratur innenfor det temaområdet vi valgte oss. Ved bruk av smarte verktøy, kvalitetssikrede databaser og en gjennomarbeidet konseptmatrise kunne vi etterhvert kartlegge litteraturen på en slik måte at vi var i stand til å avgrense oss til de mest aktuelle og relevante artiklene for vårt fokusområde, der vi blant annet strebet etter å hente mest mulig forskningslitteratur av empirisk oppbygning. På bakgrunn av

disse tre første fasene i forskningsprosessen kunne vi ta videre utgangspunkt i et passende konseptuelt rammeverk som vi bygde en egen forskningsmodell ut av. Dette rapporterte vi om i forrige kapittel (*kap. 2: Teori)*.

Etter utført innledende forskning, satt vi med kunnskap nok til å kunne gå videre i prosessen med å definere en forskningsstrategi.

## 3.1 **Forskningsstrategi**: Case-studie

En case-studie fokuserer på en instans av 'tingen' som skal undersøkes; eksempelvis en organisasjon. Denne ene instansen studeres i dybden, ved bruk av en variasjon av metoder for generering av data (Oates, 2006, s. 141). I denne case-studien er SSHF gjeldende instans, og intervjuer, dokumentasjon og spørreskjema har vært metodene vi har tatt utbytte av.

Vi undersøker blant annet hvorvidt teknologien som benyttes av organisasjonen dekker de ansattes behov, så vel som å sikre pasientdata i tilstrekkelig grad. Samtidig ser vi nærmere på hvor tilfreds den enkelte ansatte er med tilgjengelig maskin- og programvare, opplæring i bruk av systemer og bruk av privat mobiltelefon som arbeidsredskap. Vi har jobbet mot å danne oss et bilde av organisasjonens evne til å kommunisere internt hva gjelder kartlegging av behov, og vurdere deretter på hvilke plan vi kan bidra gjennom forskningsarbeidet vårt.

### 3.1.1 Planlegging og gjennomføring

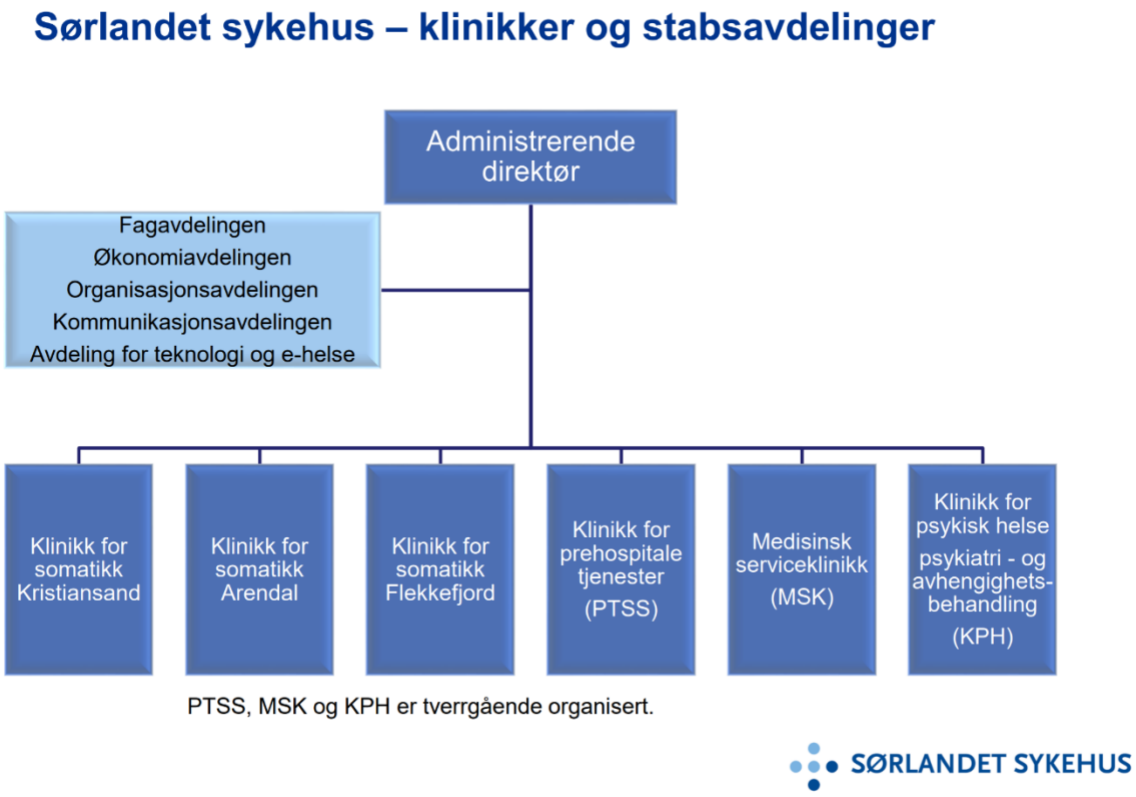
Yin (2003) foreslår at det finnes tre generelle typer case-studier: utforskende, beskrivende og forklarende (Oates, 2006, s. 143) Vi har i vårt prosjekt gått frem med en utforskende tilnærming i det vi kaller en *eksplorativ studie* der vi ser nærmere på problemstillingen i en kontekst av norske sykehus i offentlig sektor og behov i forhold til den. Som presentert i forrige kapittel finnes det nok av litteratur for problemstillingen vi har valgt oss, men ved å velge case-studie som strategi har vi avgrenset oss til en kontekst som gjør at eksisterende litteratur ikke er like dekkende. Vi har inkludert en artikkel som tar for seg en studie av lignende problemstilling i en kontekst av norske sykehus i offentlig sektor av Faxvaag og kolleger (2011). Denne har vi tatt utgangspunkt i under utformingen av enkelte spørsmål i vårt spørreskjema, noe Oates (2006) omtaler som *testing av eksisterende teori*. Ved å sammenligne resultater i en undersøkelse fra 2011 med resultater for identiske spørsmål i en ny undersøkelse fra 2019, kan vi til en viss grad se en eventuell utviklingstrend over tid og mulige situasjonsbetingede forskjeller ved de ulike instansene for emnene som tas opp. En case-studie kan også ha varierende tilnærminger til tidsaspekt (Oates, 2006, s. 144); fra historiske studier som undersøker hva som har skjedd i fortiden til langvarige studier som følger en case over lengre tid. Vårt forskningsprosjekt tar for seg en *kortvarig samtidsstudie* hvor vi undersøker hva som foregår her og nå.

Oates (2006) presenterer flere ulike faktorer som valg av case kan baseres på (Oates, 2006, s. 144-145). For oss har *bekvemmelighet* vært en sentral faktor, ettersom vi har vært heldig stilt med at universitetet har et offisielt samarbeid med SSHF. En annen faktor som også bør nevnes er at organisasjonen kan anses å være en såkalt *typisk instans*, og kan i teorien dermed regnes for å være representativ for hele klassen. Dette vil si at funn vi gjør ut av studien kan generaliseres til å gjelde for alle norske sykehus i offentlig sektor. De generaliserbare funnene vi gjør oss i denne case-studien

bygger i all hovedsak på rik innsikt. Implikasjoner fra studien er forslag til hva som muligens også foregår ved andre sykehus med eventuelle anbefalinger for handling (Oates, 2006, s. 146).

### 3.1.2 Populasjon og utvalg

Populasjonen for problemstillingen vi har hatt som mål å belyse i oppgaven er sykehus i offentlig sektor. Denne empiriske studien er gjennomført i samarbeid med Sørlandet sykehus HF (SSHF) og har som hensikt å kartlegge sykehusets forvaltning av teknologi. Vi har lykkes i å finne gode og aktuelle respondenter ved SSHF som har vært villige til å dele sin kunnskap og sine erfaringer med oss.




*Figur 3: Sørlandet sykehus – klinikker og stabsavdelinger (Sørlandet sykehuset HF, i.d.)*

Figuren viser hvordan SSHF er organisert gjennom klinikker og stabsavdelinger. Det er en stor organisasjon med et rikt mangfold av ulike avdelinger, og en holistisk studie av hele organisasjonen ville derfor vært svært tidkrevende. For vår utredning valgte vi derfor å avgrense studien ved å samle data fra kun noen få avdelinger, der vi kunne komme i kontakt med både teknisk og klinisk ansatte. I samarbeid med flere forskere ved universitetet som har kjennskap til organisasjonen, diskuterte vi oss frem til hvilke avdelinger som kunne utgjøre typiske instanser for rollene vi var ute etter. Vi bestemte oss da for å finne teknisk ansatte gjennom lederstillinger ved avdeling for teknologi og e-helse (TEH), og klinisk ansatte gjennom intensivenheten, Kristiansand (IE). Av organisasjonskartet over kan vi se at TEH utgjør en av organisasjonens fem stabsavdelinger, mens IE v/Kristiansand ligger under «klinikk for somatikk Kristiansand».


*Figur 4: Sørlandet sykehus – Avd. for teknologi og e-helse (Sørlandet sykehuset HF, i.d.)*

TEH er igjen oppstykket i flere seksjoner (Se *figur 4*). Innenfor TEH valgte vi igjen å avgrense oss til de to seksjoner vi vurderte som mest givende instanser for vår forskning; seksjon for *e-helse* og *klinisk IKT*.

**Seksjon for e-helse** arbeider med å lage strategier for videreutvikling av SSHF, og forbereder også organisasjonen på det digitale skiftet som nå kommer. De har ansvar for innovasjon og nytenkning i tillegg til bestilling av tjenester, avtaleoppfølging etc. Seksjonen kommuniserer tett med *Sykehuspartner* som er ansvarlige for utvikling og drift av systemene som brukes av organisasjonen. I tillegg til *leder ved seksjon for e-helse* (R1) som vi avholdt vårt første intervju med, består seksjonen av 11-12 ansatte som jobber mot alle nivåer i organisasjonen. En av disse har rollen som *leder for informasjonssikkerhet* (R2), som vi avholdt vårt andre intervju med.

**Seksjon for klinisk IKT** har sitt hovedansvar i forvaltningen av organisasjonens kjernesystem, kalt «DIPS». Det er særlig i sammenheng med dette systemansvaret at seksjonen i stadig økende grad legger fokus på tilgangsstyring, ettersom systemet brukes hyppig i arbeidshverdagen på klinikkene, samtidig som det lagrer på sensitive pasientdata. Vi avholdt vårt tredje og siste intervju i TEH med *leder ved seksjon for klinisk IKT* (R3).

**Intensivenheten, Kristiansand** består av klinisk ansatte som gir avansert behandling til alvorlig og kritisk syke og skadede pasienter. Her får pasientene kontinuerlig overvåkning og ofte respiratorbehandling. Enheten har en egen seksjon som kalles postoperativ hvor pasienter overvåkes etter operasjon (SSHF, i.d.). Ved denne seksjonen fordeles tre arbeidsstasjoner på syv til åtte ansatte i et vaktskift, noe som byr på utfordringer for klinikernes arbeidsflyt. Vi kommer nærmere inn på dette når vi presenterer resultatene fra datainnsamlingen i rapporten *(kap. 4.3: Maskinvare).* En av respondentene ved enheten omtaler den som *«en serviceavdeling for de andre avdelingene, hvor vi skal ha nokså fri flyt når pasientene trenger hjelp»*.

#### *3.1.2.1 Datakilder*

Vi har opprettet to tabeller for å presentere kildene vi har samlet data fra. En for intervjuene (*tabell 8: Intervjuobjektene*) og en for dokumentasjon (*tabell 9: Dokumentasjon*).

| Avdeling | Kode | Rolle |
|---|---|---|
| **TEH** (ARE) | R1 | Leder v/seksjon for e-helse |
| **TEH** (KRS) | R2 | Leder for informasjonssikkerhet |
| | R3 | Leder v/seksjon for klinisk IKT |
| **IE** (KRS) | R4 | Intensivsykepleier |
| | R5 | Intensivsykepleier |
| | R6 | Intensivsykepleier |
| | R7 | Intensivsykepleier |

| | | |
|---|---|---|
| | R8 | Sykepleier |

*Tabell 8: Intervjuobjektene*

Tabellen for intervjuobjekter viser hvilken avdeling respondenten jobber i og hvilken geografisk lokasjon de hører til (ARE = Arendal, KRS = Kristiansand), hva slags kode vi har gitt respondenten og hvilken rolle respondenten har i organisasjonen.

| Dokument | Omhandler | Versjon | Supplerer (kap.) |
|---|---|---|---|
| Normen | Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten | 5.3 | |
| Faktaark 9 | Opplæring av ledere og medarbeidere | 4.1 | 5.1.2 |
| Faktaark 14 | Tilgangsstyring | 4.1 | 5.2 |
| Faktaark 31 | Passord og passordhåndtering | 2.1 | 2.3; 5.2.2 |
| Faktaark 38 | Sikkerhetskrav for systemer | 5.0 | 1.2 |

*Tabell 9: Dokumentasjon*

Tabellen for dokumentasjon tar for seg navnet på dokumentet, hva dokumentet omhandler, hvilken versjon vi baserer oss på og hvilke kapitler den eventuelt supplerer i Normen. Faktaarkene er ment som supplerende dokumenter til Normen 5.3 som siden 20.07.2018 har vært gjeldende versjon av Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.

### Intervjuer i TEH

Vi avholdt intervjuer innledningsvis med tre ledere ved TEH:

1. **R1** har siden 2006 vært leder ved seksjon for e-helse og har omlag 20 års erfaring med prosjektledelse. Seksjonslederen koordinerer de 11-12 ansatte ved seksjonen som på mange måter er en stabsfunksjon til sykehuset, organisert i stab til direktøren under teknologidirektøren. De ansatte fungerer som rådgivere for sykehuset i mange sammenhenger i forhold til teknologiutvikling.
2. **R2** har siden 2013 vært leder for informasjonssikkerhet i organisasjonen. Hvert av foretakene i Helse Sør-Øst har en ansatt i denne stillingsrollen, som sammen diskuterer og arbeider med sikkerhetsorganiseringen for hele regionen.
3. **R3** er leder ved seksjon for klinisk IKT og har omlag 22 års arbeidserfaring innen IT. Seksjonslederne for e-helse og klinisk IKT utgjør IT-lederne i organisasjonen på hvert sitt område; der klinisk IKT først og fremst har ansvar for pasientsystemer og alt som ligger rundt, mens e-helse har et mer tradisjonelt ansvar.

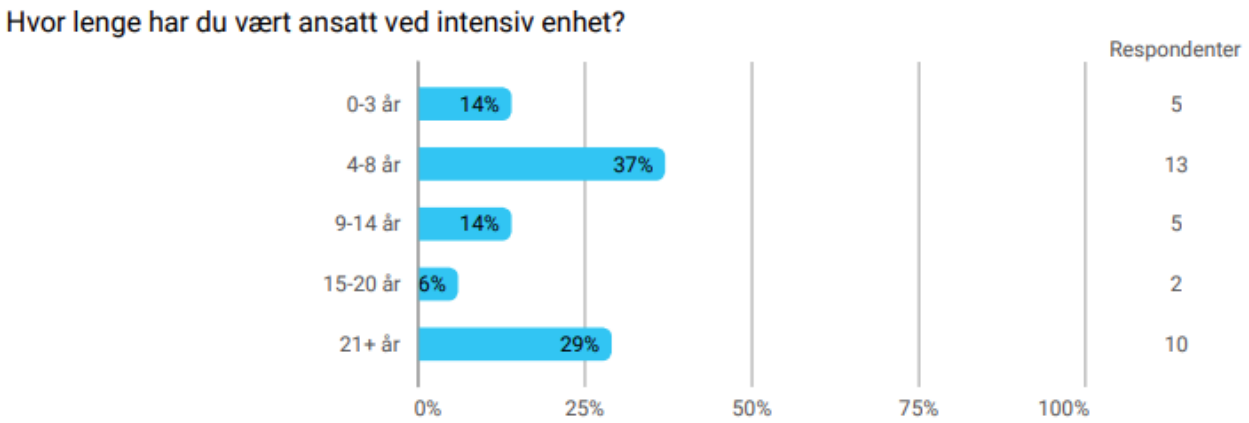
### Intervjuer i IE

Med kunnskapen fra disse tre intervjuene lagt til grunn, kunne vi strukturere videre intervjuer med klinikere i en intervjuguide som påser at vi samler mest mulig givende informasjon både for forskningen og sykehuset. Vi avholdt så intervjuer med fem sykepleiere ved IE som sitter på et mangfold av ulike bakgrunner:

1. **R4** er intensivsykepleier, har vært stasjonert i IE i 14 år og har en fartstid i SSHF fra 2001. Respondenten har tidligere vært i medisinsk avd., samt medisinsk intensiv som nå har blitt en del av IE.
2. **R5** er intensivsykepleier, har vært stasjonert i IE i 3 år og har en fartstid i SSHF fra 2011. Respondenten har tidligere vært ved akuttmottaket og ble uteksaminert som intensivsykepleier i 2016.
3. **R6** er intensivsykepleier, har vært stasjonert i IE i 23 år og har en fartstid i SSHF fra 1979. Respondenten har tidligere vært i gynekologisk-, medisinsk- og hjertemedisinsk avd., samt medisinsk intensiv og avd. for rus- og avhengighetsbehandling (ARA). Respondenten har også vært i geriatrisk opptreningsavd. i Oslo i løpet av sine 40 år med erfaringer i helsesektoren. Respondenten bidrar også i dagkirurgisk avd. ca. fire ganger i måneden som IE forsørger med en person hver dag for å få turnus til å gå opp.
4. **R7** er intensivsykepleier, koordinator og assisterende koordinator ved IE og har vært ansatt i SSHF siden 1989. Koordinatoren har en overordnet stilling uten pasientansvar og styrer avdelingen i forhold til pasientflyt. Assisterende koordinator har sjekkoppgaver og ansvar for pasienter som skal reise til behandling. Respondenten ble uteksaminert som intensivsykepleier i 2007.
5. **R8** er sykepleier og har vært ansatt i SSHF i 21 år. Respondenten var med på å starte opp lindrende enhet (LE) ved Kristiansand og var stasjonert her i 15 måneder. I denne perioden jobbet respondenten ved begge enheter, med ca. 75 % av arbeidstiden ved LE og de resterende 25 % ved IE.

### Undersøkelse i IE

Oates (2006) påpeker at det i mindre forskningsprosjekter – som for eksempel førstegangs forskningsprosjekter – er en god tommelfingerregel å ta utgangspunkt i å samle minst 30 svar. Det er ikke unormalt at man får om lag 30 besvarelser dersom man sender ut et spørreskjema til 100 personer, og en svarprosent på 10 % er heller ikke uvanlig (Jacobsen, 2005, s. 262; Oates, 2006, s. 99). Utvalgsstørrelsen for spørreundersøkelsen vår tar utgangspunkt i størrelsen på intensivenheten i Kristiansand hvor vi nådde ut til 59 ansatte. I arbeidet mot å få en best mulig svarprosent mener vi at vi har gjort spørreskjemaet enkelt å forstå for målgruppen og utvalget, samt at vi har med hensikt gjort spørreskjemaet gjennomførbart på relativt kort tid. I tillegg tror vi avdelingen består av ansatte med mange ulike meninger som ønsker å bli hørt, som gjerne vil engasjere seg i prosjektet vårt. Dette har vi også sett tendenser til i de kvalitative intervjuene. Vi stilte respondentene et indirekte emnerelatert spørsmål innledningsvis for å kartlegge utvalgets bakgrunn:




*Figur 5: Spørreskjema – indirekte emnerelatert spørsmål*

Blant de 35 respondentene totalt er det et rikt mangfold av ulike fartstider ved enheten. Den største gruppen har en fartstid mellom 4 og 8 år og utgjør 37 %. 29 % har vært del av IE i over 21 år, en gruppe vi anser for å utgjøre representative respondenter i svært høy grad. 14 % er 'nykommere' ved enheten, og de resterende 20 % fordeler seg på en fartstid mellom 9 og 20 år. Basert på dette rike mangfoldet av bakgrunner, vurderer vi utvalget som godt representativt for enheten.

## 3.2 Kombinerte metoder

En case-studie karakteriseres av mangfoldige kilder og metoder for generering av data (Oates, 2006, s. 142). Vi har hatt som målsetting å gjennomføre denne case-studien ved bruk av både kvalitative og kvantitative metoder for datainnsamling, i det vi i forskningssammenheng kaller *kombinerte metoder*, ofte omtalt som *«mixed methods»* i engelsk litteratur. Creswell (2014) definerer kombinerte metoder som en tilnærming til å forske på det sosiale, atferd og helsevitenskap hvor forskeren samler både kvalitative og kvantitative data, integrere de to, for så å trekke tolkninger basert på den kombinerte styrken av begge sett med data for å forstå problemstillingen (Creswell, 2014, s. 2).

> *Mixed methods research is an approach that combines quantitative and qualitative research methods in the same research inquiry. Such work can help develop rich insights into various phenomena of interest that cannot be fully understood using only a quantitative or a qualitative method.* (Venkatesh, A. Brown & Bala, 2013, s. 1)

Creswell & Zhang (2013) argumenterer for at verken kvalitative eller kvantitative forskningsmetoder alene kan fullt ut levere etter sin forutsetning om å etablere sannheten om fenomener av interesse for forskere i helsesektoren (Zhang & Creswell, 2013). Med utgangspunkt i tidligere litteratur har vi gjennom kombinerte metoder samlet data fra SSHF med hensikt om å teste de lokale forholdene som ligger til grunn for fenomenet. Ved å bruke flere datainnsamlingsmetoder har vi vært i stand til å generere mer beskrivende data med en kombinasjon av foreslående og forklarende funn i en eksplorativ tilnærming. På denne måten har vi vært i stand til å utvikle spørreskjema basert på funn fra intervjuer, og videre bruke funn fra intervjuer til å finne forklaringer i funnene vi gjør oss av undersøkelsen. Dette mener vi har bidratt til å forbedre kvaliteten på studien vår og gjort utredningen av problemstillingen mer komplett, der vi har kunne belyst den ved å besvare to forskningsspørsmål, henholdsvis ett kvantitativt og ett kvalitativt ladet. Vi mener at bruken av kombinerte metoder i denne

sammenhengen har vært hensiktsmessig for studien for å danne et empirisk grunnlag i denne forskningskonteksten, ved å bygge videre fra eksisterende litteratur til kvalitativ metode for så å analysere resultatene og dermed utforme en kvantitativ undersøkelse, og til slutt sammenstille resultatene. Metoden har også bidratt til at vi har kunnet danne et kunnskapsgrunnlag rundt en sektor vi ikke kunne så mye om i forkant. Det omhandler også å få innsikt i meninger og holdninger blant respondenter uten å nødvendigvis insinuere at faktorene man undersøker er viktige blant respondentene i henhold til problemstillingen. Det har også vært ved nyttig å sette seg inn i respondentenes situasjon og posisjon for å forstå deres innsikt i problemstillingen ved å ta i bruk denne metoden. Vi har dermed hatt empirisk grunnlag fra intervjuer til å basere spørreundersøkelse på, noe vi ellers ikke ville hatt om vi hadde gått for kun en av tilnærmingene.

### 3.2.1 Kvalitativ datainnsamling

Etter å ha definert forskningsstrategien kunne vi sette oss ned og diskutere hva slags metode(r) vi burde ta i bruk for å utlede strategien på best mulig vis. Vi øynet tidlig muligheten til å teste eksisterende teori med SSHF som ny instans. Men studien vi ønsket å sammenligne resultater fra egen studie med var åtte år gammel, og vi ønsket derfor å gå utforskende til verks med intervjuer for å kunne gjøre sentrale funn på innovasjon og andre faktorer for temaet som kunne bidra til å påvirke studien. I tillegg ønsket vi å gi noe tilbake til SSHF som har sagt seg villige til å la oss samle data hos dem, ved å også fokusere på hva de ønsker å vite mer om internt i sin egen organisasjon. Jacobsen (2005) argumenterer for at en av de sterkeste sidene ved den kvalitative tilnærmingen, er at vi kan hele tiden tilpasse metoden til den nye kunnskapen vi tilegner oss i løpet av undersøkelsesprosessen (Jacobsen, 2005, s. 187).

#### *3.2.1.1 Dokumentasjon*

Dokumentasjon kan benyttes som en alternativ kilde til data fra intervjuer og spørreskjemaer, noe som oftest regnes som en kvalitativ tilnærming til innsamling av data. Oates (2006) stykker dokumentasjon opp i to typer; *funnet dokumentasjon* og *dokumentasjon generert av forsker* (Oates, 2006, s. 232). At dokumentet er generert av forsker vil si at det blir opprettet utelukkende for forskningsprosjektet. I vårt prosjekt fokuserer vi kun på det som kalles funnet dokumentasjon, som vil si at den allerede eksisterer. Siden SSHF er et offentlig foretak må de også forholde seg til formelle nasjonale krav fra Direktoratet for e-helse. Direktoratet har en database på nett hvor de tilbyr stor grad av transparens for folket i sine dokumenter. Dette gjorde at vi ikke behøvde å gå gjennom noen søknadsprosess for å samle data gjennom denne metoden. Gjennom *e-helse.no* fikk vi tilgang til det som kalles *Norm for informasjonssikkerhet* (Normen):

***«Normen skal bidra til å etablere mekanismer hvor virksomhetene kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå. Normen stiller krav som detaljerer og supplerer gjeldende regelverk.»*** (Direktoratet for e-helse, i.d.)

I tillegg til det overordnede vedtaksdokumentet *Normen 5.3*, består Normen-dokumentene av en rekke faktaark som supplerer det overordnede dokumentet. Faktaarkene refererer til dokumentet på en oversiktlig måte der man kan se hvilke(t) faktaark som supplerer hvert av emnene som tas opp. Vi presenterte alle dokumentene vi har tatt i bruk tidligere i kapittelet (*kap. 3.1.2.1: Datakilder*).

Innsamling av data gjennom dokumentasjon har bidratt til at vi i større grad har kunne samle formell informasjon om konseptene og begrepene vi bruker i studien vår. Dette har hjulpet oss i operasjonaliseringen av variablene som består av disse konseptene, noe vi rapporterer om senere i kapittelet (*kap. 3.2.2.1: Forskningsmodell*).

#### *3.2.1.2 Intervju*

Til gjennomføringen av kvalitativ datainnsamling utviklet vi i forkant av prosjektperioden en intervjuguide med åpent formulerte spørsmål som tilbød stor grad av fleksibilitet, med fokus på å hente mest mulig informasjon som er relevant for problemstillingen vår. I samarbeid med instituttet fikk vi testet intervjuguiden vår ved hjelp av to ansatte ved *Senter for eHelse* med bakgrunn innen helseinformatikk, der vi avholdt ett intervju gjennom fysisk nærhet til informanten (ansikt-til-ansikt), og ett fysisk atskilt fra den andre informanten (e-post). På denne måten kunne vi sikre at intervjuguiden ville være i stand til å tjene sitt formål gjennom begge hovedformer for avholdelse av intervju (Jacobsen, 2005, s. 143).

Basert på krav fra Norsk Samfunnsvitenskapelig Datatjeneste (NSD) utarbeidet vi et informasjonsskriv som ble tildelt og godkjent av respondenter før vi avholdt intervjuer med dem (8.5: *Informasjonsskriv for kvalitativ datainnsamling*). Vi går nærmere inn på hva disse kravene innebærer senere i kapittelet (*kap. 3.5: Etikk*) Informasjonsskrivet er basert på mal fra NSD. Det gir full informasjon om prosjektet og baserer seg på formelle etiske retningslinjer innen forskning; blant annet påser den at alle respondenter avgir *fritt og informert samtykke*.

Data ble innsamlet gjennom å avholde *åpne individuelle intervjuer* (Jacobsen, 2005, s. 142-143) med ansatte ved SSHF. Vi valgte å avholde intervjuer først med ledere ved avdeling for teknologi og e-helse, med en baktanke om at det kunne være fordelaktig å – tidligst mulig i forskningsprosessen – snakke med fagpersoner som har innsikt i det overordnede i form av arbeidsrutiner (retningslinjer, opplæring, kultur, osv.). Vi avholdt såkalte *semi-strukturerte intervjuer* (Jacobsen, 2005, s. 144-147; Oates, 2006, s. 188) for å avdekke funn som har bidratt til å besvare deler av forskningsspørsmålet vårt og med dette belyse problemstillingen. Et semi-strukturert intervju har en åpen strukturform og blir definert som *«et intervju som har som mål å innhente beskrivelser av den intervjuedes livsverden, med henblikk på fortolkning av de beskrevne fenomenene»* (Kvale, Brinkmann, Anderssen & Rygge, 2009, s. 21). Til tross for at vi hadde forberedt intervjuguide, lot vi respondentene snakke åpent og fritt store deler av tiden. Vi gikk også stadig utenfor intervjuguiden med tilleggende spørsmål der vi så at det kunne være hensiktsmessig. På denne måten kunne vi tidlig i datainnsamlingen danne oss et holistisk bilde av de aktuelle konseptene med et fokus satt av organisasjonens eget perspektiv, slik at vi kunne påvirke videre datainnsamling med denne nye kunnskapen.

På grunnlag av dette var vi bedre rustet til å påse at det avgis relevant informasjon i senere intervjuer med klinikere, i en noe mer strukturert intervjutilnærming enn tidligere. Denne fremgangsmåten har vi ansett som svært givende, da vi har sett at det kan være vanskelig for klinikerne å vite eller forstå nøyaktig hva vi snakker om eller er ute etter til enhver tid. Vi var forberedt på det ettersom vi oppdaget tendenser til dette allerede i den tidligere nevnte testingen av intervjuguiden, da en av våre informanter hadde en mer teknisk bakgrunn, der den andre hadde en mer klinisk bakgrunn. Vi

presenterte detaljer for utvalget av respondenter som har bidratt i datainnsamlingen tilbake i *kap. 3.1.2 (Populasjon og utvalg)*.

Vi dokumenterte intervjuene gjennom lydopptak og notater underveis, der vi ba om hver enkelt intervjupersons tillatelse til å ta opp intervjuet, noe vi fikk fra samtlige deltakere. I tillegg til å forenkle den senere jobben med transkribering, bidro det at vi tok notater underveis til å sende ut et signal til intervjupersonen om at det som blir sagt, er interessant for oss (Jacobsen, 2005, s. 152). Ut fra lydopptakene kunne vi så sette oss ned og transkribere intervjuene. Idealet i transkriberingen er at intervjuer skal skrives ut i sin helhet, noe vi har strebet mot (Jacobsen, 2005, s. 189). Takket være hyppig notering underveis i intervjuene, ble resterende transkribering en mye mindre tidkrevende oppgave enn mange forskere rapporterer om for sine prosjekter. Ved å også inkludere *meningsfortolkende* notater underveis kunne vi validere dataene vi samlet ved å stille oppfølgingsspørsmål som bekrefter at respondenten mener det vi tror, i stedet for å bare ta antagelser som kan føre til nye utfordringer i prosessen med å bearbeide, analysere og presentere dataene. Vi går inn på etiske aspekter i behandlingen av dataene senere i kapittelet *(kap. 3.5: Etikk)*.

#### *3.2.1.3 Kvalitativ analyse*

Analyse av kvalitative data kan deles inn i tre kategorier (Jacobsen, 2005, s. 186):

- Beskrive: en beskrivelse av innsamlet datamateriale.
- Kode: systematisere og redusere uoversiktlig informasjon, utsiling og forenkling, for å få oversikt.
- Sammenbinde: fortolking av data, lete etter meninger, osv.

*«Den vanligste formen for dataanalyse er i dag å kode, eller kategorisere intervjuuttalelser. Koding innebærer at man knytter et eller flere nøkkelord til et tekstsegment for å tillate senere identifisering av en uttalelse»* (Kvale, Brinkmann, Anderssen & Rygge, 2015, s. 226).

Vår tilnærming til analyse etter datainnsamling var i første omgang å samle rådata der hvor det logisk hørte hjemme etter kategorier og utvalg. Transkriberte intervjuer ble organisert i et samlet dokument for hvert utvalg, henholdsvis IE og TEH. Derav ble intervjuene inndelt i tabeller for kategorier tilhørende spørsmålene fra intervjuene og data ble systematisert gjennom forenkling og utsiling. Koding i kategorier ble også gjort i et eget regneark hvor vi delte inn etter hovedkategorier og underkategorier. Hovedkategoriene samsvarer med forskningsmodellen ettersom intervjuguiden ble utviklet med den og tidligere arbeid med forskningslitteratur som utgangspunkt. Eksempelvis vil kategorien tilgangsstyring åpenbart forekomme som en hovedkategori ettersom dette er en sentral del av fokuset i intervjuet og for oppgaven.

Vi leste gjennom all data vi hadde etter systematiseringen, dermed kunne vi identifisere mønster og tema i dataene (Oates, 2006, s. 268). Etter denne prosessen kunne vi inndele dataene i segmenter basert på relevans. Oates (2006) foreslår å dele det inn i tre segmenter: Segmenter som ikke har relevans for studien. Segmenter som tilføyer generell beskrivende informasjon som trengs for å beskrive forskningskonteksten for leserne, som eksempelvis bedriftshistorie, antall ansatte og arbeidserfaring. Denne informasjonen gikk vi inn på tidligere i kapittelet (*kap. 3.1: Strategi: Case-studie*). Til slutt segmenter som tilsynelatende er relevante for forskningsspørsmålet (Oates, 2006, s.

268). Dette ble gjort i systematiseringsfasen hvor irrelevant eller overflødig informasjon ble luket ut og vil ikke bli tatt med som en del av funn og resultater. De resterende segmentene ble stående.

### *3.2.2 Føler du det settes av nok tid og ressurser til kursing og opplæring? (Bruk av verktøy og systemer, sikkerhet...)*

| | | |
|---|---|---|
| R4 | Ønsker mer avsatt tid til opplæring i alt; også fag, noe det er alt for lite tid til. Nå er det slik at alt må prioriteres (ta vare på pasient eller ulike ting som er pålagt sertifisering). Har heller ikke lyst til å gjøre research når jeg kommer hjem fra jobb. | Opplæring |
| R5 | Ja, det tror jeg. Nyansatte blir sendt på DIPS-kurs. For min egen del føler jeg ikke at vi trenger noe mer kurs på det vi allerede har. | DIPS<br>Opplæring |
| R6 | Det kan ikke gjøres (det blir aldri nok tid). Det er så mange og så spesielle ting vi sjelden kommer oppi på denne enheten, som vi allikevel må gjennom i blant. Det blir aldri nok kursing, noe jeg ikke tror vi har som mål heller. | Opplæring |
| R7 | Har ikke fått så mye nytt i det siste. Tror ansatte generelt har grei kontroll på systemer som brukes. Problemet er hele tiden at vi er for få folk. | |
| R8 | Nei. Men skjønner dette. Vi er ikke nok folk. Det gjøres absolutt forsøk, og det står ikke på viljen. Men vi kunne hatt mer organisert der man vet at man skal på kurs i stedet for undervisning midt i arbeidstiden. Jeg er en av de som driver med opplæring, så jeg vet hvor hardt det sitter inne. Vi har krav til HLR skal alle gjennom en gang i året for å få lov til å styre med det. Og det er alltid noen som ikke er med på de kursene som vi har, så må vi ha inn noen få etterslepende, det er vanskelig å få til logistikken i det. | Opplæring |

*Tabell 10: Utdrag fra tabell for systematisering; meningsfortetting og koding*

Figuren over ble utarbeidet i Excel og kodet basert på innholdet i intervjuene. Denne tabellen forteller noe om forekomsten av underkategorier samt hvilke respondenter som har snakket om dette. Når vi ser at en stor andel av underkategoriene i kategorien tilgangsstyring forekommer hos et flertall respondenter vil det være hensiktsmessig å jobbe videre med denne kategorien i kvantitativ sammenheng. Eksempelvis ser vi at forekomsten av underkategoriene «workarounds», «opplæring/kunnskap» og «DIPS» (EPJ) har vært diskutert blant alle respondentene. Det er viktig å presisere at respondentene også naturligvis har svart på spørsmål relatert til spørsmålene som ligger innunder disse kategoriene, men at også blant samtlige respondenter ble tilgangsstyring diskutert før vi hadde kommet til spørsmål som var tilknyttet tilgangsstyring.

| Kategorier | Underkategori | TEH | | | IE | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | R1 | R2 | R3 | R4 | R5 | R6 | R7 | R8 |
| **Tilgangsstyring** | Autentisering | | * | * | * | * | * | * | * |
| | Autorisering | * | * | * | * | | * | * | * |
| | Passord | | * | * | * | * | * | * | * |
| | Logging/Sporing | * | * | * | | | | | |
| | Multifaktor/tokens | | | * | | | | | |
| **Programvare** | DIPS | * | * | * | * | * | * | * | * |
| | EK-WEB | | | | * | * | * | * | * |
| | Felleskatalogen | | | | * | * | * | * | |
| | Brukervennlighet | | * | | * | * | | | * |
| | Mail | | | | | * | * | | * |
| **Maskinvare** | Mobile enheter | | | | * | * | * | * | |
| | PC | | * | | * | | * | * | |
| **Organisasjon / Bruker** | Pasientsikkerhet | | | | | | * | * | * |
| | Taushetsplikt | | * | * | * | * | | * | * |
| | Motivasjon | | | * | * | | * | * | |
| | Tillit | * | | | | | | | |
| | Opplæring/kunnskap | * | * | * | * | * | * | * | * |
| | Retningslinjer | * | | * | | | | | |
| | Kultur | * | | | | | | | |
| **Arbeidsrutiner** | Workarounds | * | * | * | * | * | * | * | * |
| | Dobbeltarbeid | * | | | | | | | |

*Tabell 11: Kvalitativ analyse og koding av kategorier*

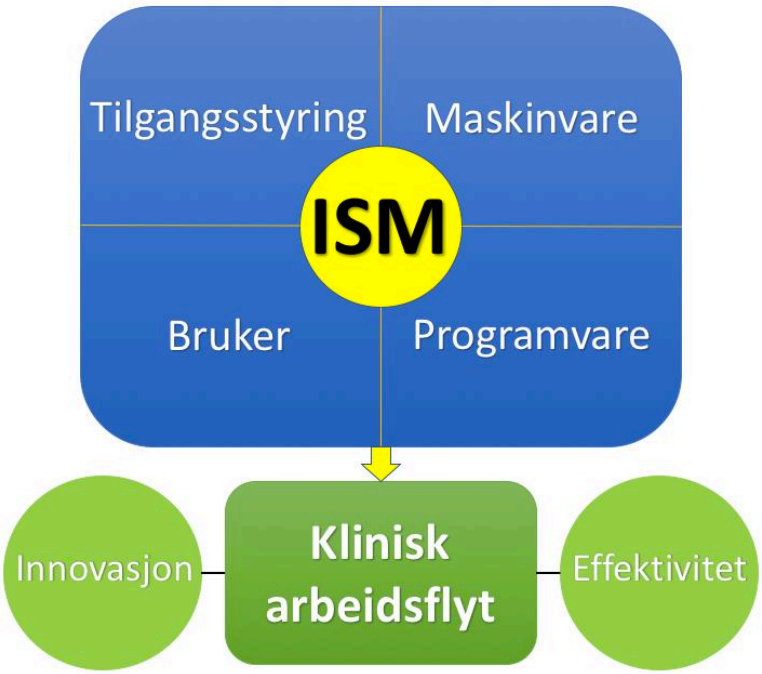
### 3.2.2 Kvantitativ datainnsamling

Kvantitative metoder benyttes når problemstillingen har til hensikt å utforske hvilke av de kjente teoriene som er mest relevante for å forklare det vi kan observere empirisk, i kontrast til å trekke mulige forklaringer ut fra kvalitative intervjuer. Vi er ute etter et svar som medfører en generalisering fra et utvalg til en større populasjon når det gjelder hvordan ISM kan tenkes å påvirke forhold ved klinisk arbeidsflyt.

Etter å ha innsamlet data og analysert den i en kvalitativ tilnærming, kombinert med relevant bakgrunnslitteratur, hadde vi et godt grunnlag for å utarbeide et spørreskjema som utgjør den kvantitative innsamlingen av data i prosjektet. Bruken av flere metoder for å understøtte funn og forsterke validiteten kalles for *metodetriangulering* (Jacobsen, 2005, s. 136; Oates, 2006, s. 37).

#### *3.2.2.1 Forskningsmodell*

På bakgrunn av eksisterende litteratur som presentert i forrige kapittel *(kap. 2: Teori)* og kvalitativ analyse som vi presenterte tidligere i kapittelet *(kap. 3.2.1: Kvalitativ datainnsamling)* utarbeidet vi en forskningsmodell. Vi gjør i denne sammenheng oppmerksom på at vår modell ikke er utviklet for å fungere som representativ for temaene ISM og klinisk arbeidsflyt i enhver sammenheng. Det er en skreddersydd versjon basert på vår case-studie som vi beskrev tidligere i kapittelet (*kap. 3.1: Strategi: Case-studie*).




*Figur 6: Forskningsmodell for kvantitativ undersøkelse*

Med utgangspunkt i klinisk arbeidsflyt som avhengig variabel har vi benyttet oss av tidligere litteratur og resultater fra kvalitativ datainnsamling, henholdsvis intervjuer og dokumentasjon for formelle krav og retningslinjer, til å undersøke hva som kan utgjøre uavhengige variabler i form av sykehusets situasjonsbetingede tilnærming til ISM. Dokumentasjonen vi presenterer i dette delkapittelet er del av den kvalitative datainnsamlingen, men presenteres her for å definere hver av variablene. Forskningsmodellen vår består av en avhengig variabel (*klinisk arbeidsflyt*) med to kontrollvariabler (*effektivitet* og *innovasjon*), og fire uavhengige (*tilgangsstyring, maskinvare, programvare, bruker*) som sammen utgjør vår tolkning av ISM for denne studiens kontekst.

**Avhengig variabel**: Klinisk arbeidsflyt

**Kontrollvariabler**: Vi har lagt ved to kontrollvariabler som har til hensikt å belyse vår spesifikke definisjon av konseptet klinisk arbeidsflyt som avhengig variabel:

- **Innovasjon** i prosesser: Et klinisk arbeidsmiljø krever kontinuerlig fokus på nytenking iht. endringer i arbeidsprosesser (eks. innføring av nye systemer) som bidrar positivt til arbeidsflyten. Vi inkluderer denne kontrollvariabelen med formål om å teste hvorvidt innovasjon i arbeidsprosessene påvirkes av organisasjonens håndtering av informasjonssikkerhet.
- **Effektivitet** i prosesser: Et klinisk arbeidsmiljø er i mange tilfeller hektisk og uforutsigbart, og krever også at arbeidsprosesser flyter på en mest mulig effektiv måte. Vi inkluderer denne kontrollvariabelen med formål om å teste hvorvidt effektivitet i arbeidsprosessene påvirkes av organisasjonens håndtering av informasjonssikkerhet.

**Uavhengige variabler**: ISM

Som presentert i forrige kapittel (*kap. 2.1: Informasjonssikkerhet*), utgjør ISM bare ett mindre konkretisert fokus innenfor et massivt temaområde som informasjonssikkerhet består av. For vår

studie har vi stykket opp den uavhengige variabelen (ISM) i fire delvariabler som vi vil presentere enkeltvis videre i dette delkapittelet. Her rapporterer vi om aktuelle funn fra dokumentasjon som har bidratt til å definere hver variabel og beskriver hvordan vi har valgt å operasjonalisere den. Vi rapporterte om hvordan vi gikk frem for å samle inn kvalitative data tidligere i kapittelet *(kap. 3.1.2: Populasjon og utvalg)*. Vi rapporterer om funn fra intervjuer som variablene også grunner fra i neste kapittel *(kap. 4: Resultater)*.

### Tilgangsstyring

I rammeverket som vi viste til tidligere i kapittelet *(Figur 1: A Human Centered Framework for Information Security Management)* går tilgangsstyring innunder «organisatoriske retningslinjer». Som presentert i kapittelet, er tilgangsstyring et høyaktuelt emne innen temaene ISM og klinisk arbeidsflyt. Ut fra dokumentasjon har vi funnet følgende:

> *«Pasientopplysninger skal vernes, men helsepersonell som yter helsehjelp må gis mulighet til å søke opp og registrere relevante og nødvendige opplysninger i pasientens journal. Dette ivaretas bl.a. ved tilgangsstyring»* (Direktoratet for e-helse, 2018b).
>
> Tilgangsstyring berører hvordan man foretar (Direktoratet for e-helse, 2018d, s. 28):
>
> - Autorisering som er tildeling av rettigheter til å kunne lese, registrere, rette, slette og/eller sperre helse- og personopplysninger.
> - Autentisering som sikrer identifisering av autorisert bruker.
> - Tilgjengeliggjøring av helse- og personopplysninger om bestemte pasienter/brukere for autorisert personell.
> - Tilgjengeliggjøring av helse- og personopplysninger til annet personell enn virksomhetens eget personell.
> - Regulering av privat bruk av virksomhetens informasjonssystemer.
> - Kontrollerende tiltak.

I en kvantitativ spørreundersøkelse tester vi klinisk ansattes grad av tilfredshet med organisasjonens håndtering av passordbytter, autorisering og autentisering i form av inn- og utlogging av arbeidsstasjon og system, samt evne til å gi tilgang til informasjon innen rimelig tid. Vi presenterer resultatene av dette i *kapittel 4.1 (Tilgangsstyring)*.

### Programvare

Programvare går i det konseptuelle rammeverket innunder kategorien «organisatoriske prosedyrer» i rammeverket vi har hentet inspirasjon fra. Variabelen tar for seg alle systemer som ligger til grunn for å understøtte arbeidsprosesser og sikring av informasjon. Vi presenterte funn fra litteraturen rundt EPJ-systemer i *kap. 2.3.1.2 (EPJ)*. I tillegg har vi brukt funn fra kvalitativ datainnsamling til å operasjonalisere variabelen. Ut fra dokumentasjon har vi funnet følgende:

> Virksomheten skal ha oversikt over alt IKT-utstyr. Denne oversikten skal inkludere stasjonære og bærbare datamaskiner, mobiltelefoner og annet kommunikasjonsutstyr, servere, nettverksutstyr (rutere, svitsjer, brannmurer, osv.), skrivere, lagringsnettverk, apper, IP-telefoner mv. I større virksomheter bør følgende tiltak gjennomføres (Direktoratet for e-helse, 2018d):

- Utarbeide oversikt over maskin- og programvare som vedlikeholdes med automatiske verktøy
- Inventarsystemet for programvare bør spore versjon av det underliggende operativsystemet samt programmer som er installert på det.

Faktaark 38 viser til sikkerhetskrav som skal ivaretas i systemer som behandler helse- og personopplysninger. Faktaarket staterer at virksomhetens leder er ansvarlig for at systemer som tas i bruk for behandling av helse- og personopplysninger inneholder nødvendige sikkerhetsløsninger. Kravene som presenteres følger av Normen, og for enkelte krav er det angitt en utdypning av kravet som ikke direkte kan leses ut av Normen. Disse er angitt som «Utdypning av kravet:». Faktaarket dekker ikke samtlige krav ved tilgang til helseopplysninger mellom virksomheter. Grunnen er at flere av kravene kan løses utenfor systemene (Direktoratet for e-helse, 2018a).

I spørreundersøkelsen tester vi klinisk ansattes grad av tilfredshet med systemene ved arbeidsplassen, henholdsvis kjernejournalsystemet «DIPS» hvor all pasientdata lagres og prosedyreoppslagsverket «EK-web» som viser retningslinjer for prosesser. I tillegg tester vi ansattes behov for å gjøre doble føringer i arbeidet sitt, henholdsvis i form av å overføre data fra papir til system, og fra et system til et annet. Vi presenterer resultatene av dette i *kapittel 4.2 (Programvare)*.

### Maskinvare

For vår studie utgjør maskinvare – sammen med programvare – de to perspektivene av «organisatoriske prosedyrer». Variabelen angår alt teknisk utstyr som brukes til å understøtte arbeidsprosesser og sikring av informasjon. Den er i all hovedsak basert på funn fra kvalitativ datainnsamling som foreslår at maskinvare kan ha en betydelig innvirkning på ISM og klinisk arbeidsflyt i vår studies kontekst. Ut fra dokumentasjon har vi funnet følgende:

Normen sier at sikkerhetstiltak skal hindre at personer som ikke er autoriserte får tilgang til helse- og personopplysninger gjennom brukerutstyr – enten ved adgangsregulert kontroll av lokaler med utstyr, eller ved at utstyret sikres mot misbruk og skjermer, utskrifter mv. skjermes mot uautorisert innsyn. Sikkerhetstiltak skal også hindre at annet enn autorisert personell får adgang til driftsutstyr. Alle lagringsmedia, dvs. disker, minnepinne, CD, mv., skal merkes, og alle helse- og personopplysninger skal slettes når lagringsmediet tas ut av bruk. Plikt til arkivering av opplysningene må uansett overholdes. For mobilt utstyr kan man ikke sikre lokaler, og utstyret må derfor sikres. Det skal gjennomføres risikovurdering av de løsninger som benyttes. Det skal etableres administrative prosedyrer for bruk av mobilt utstyr og hjemmekontor. Sikkerhetstiltak skal hindre at personer som ikke er autoriserte får tilgang til helse- og personopplysninger ved at (Direktoratet for e-helse, 2018d):

- Tekniske tiltak iverksettes slik at det kun kan kommuniseres med predefinert utstyr. Autentisering skal ikke innebære økt risiko utover det som gjelder for stasjonært utstyr. En risikovurdering må vise at autentiseringsløsningen gir tilstrekkelig sikkerhet.
- Helse- og personopplysninger skal bare lagres lokalt når dette er nødvendig ut fra tjenstlig behov og skal alltid lagres kryptert.

- All kommunikasjon, enten dette skjer ved hjelp av trådløst samband eller ved hjelp av linjer sikres ved kryptering iht. «NSM Cryptographic Requirements v3.1» (Norwegian National Security Authority, 2016)

I spørreundersøkelsen tester vi klinisk ansattes grad av tilfredshet med tilgang og responstid for arbeidsstasjoner, samt egen og andres bruk av private enheter i arbeidet. Dette emnet omtales ofte i litteraturen som *«bring your own device»* (BYOD). Vi presenterer resultatene av dette i *kapittel 4.3 (Maskinvare)*.

#### Bruker

Bruker utgjør vår tolkning av rammeverkets siste komponent, «organisasjonskultur». Variabelen tar for seg kultur i to perspektiver; organisasjonskultur med organisatoriske tiltak for å understøtte ansattes bruk av systemer og verktøy i arbeidsprosesser; og brukerkultur med brukerens egen oppfatning og utførelse. Emnet er godt dekket oppunder i litteraturen, noe som tyder på at det er en viktig faktor innenfor temaet. Vi presenterte funn som variabelen baseres på i *kap. 2.3.2.2 (Kunnskap)* og *kap. 2.3.3 (Uformell praksis)*. Fra innsamling av data gjennom dokumentasjon har vi gjort følgende funn:

> Opplæring av ledere og medarbeidere krever forankring i organisasjonen og at det stilles krav til både innhold og kvalitet. Opplæringen anbefales basert på en opplæringsplan slik at det settes av tid besluttet av ledelsen. Det anbefales at opplæringen i personvern og informasjonssikkerhet knyttes til annen opplæring i virksomheten (Direktoratet for e-helse, 2018a).
>
> Virksomheten skal iverksette tiltak som ivaretar at:
>
> - alle som gis tilgang til og/eller drifter informasjonssystemene og tilhørende informasjon skal ha tilstrekkelig kunnskap til å utnytte systemene for sin rolle og til å ivareta informasjonssikkerheten.
> - alle som har tilgang til helse- og personopplysninger behandler disse etter gjeldende regelverk, Normen og virksomhetens rutiner.
>
> Kompetansebygging må skje kontinuerlig og være tilpasset de ulike roller og brukergrupper. Særskilte opplæringstiltak må vurderes for nyansatte og ved endringer i informasjonssystemene eller i behandlingen av helse- og personopplysninger (Direktoratet for e-helse, 2018d, s. 27).

I spørreundersøkelsen tester vi hvordan klinisk ansatte opplever organisasjonens håndtering av opplæring, henholdsvis for sikring av informasjon og bruk av systemer; samt deres ulike oppfatning av hvorvidt rapportering elektronisk gjennom EPJ-system er positivt eller negativt, henholdsvis for sikring av pasientdata og behandling av pasient. Vi presenterer resultatene av dette i *kapittel 4.4 (Bruker)*.

### *3.2.2.2 Spørreundersøkelsen*

Vi utarbeidet spørreskjemaet med hensikt om å besvare det som utgjør andre del av forskningsspørsmålet; nemlig **i hvilken grad** aspekter ved ISM påvirker den kliniske arbeidsflyten. Vi har lagt stor vekt på å gjøre spørsmålene i spørreskjemaet enkle å forstå, så vel som å gjøre det enkelt å ta stilling til svaralternativene. Vi har strebet mot å få stor andel av utvalget som mulig til å delta i undersøkelsen, slik at vi til en viss grad kunne generalisere funn til å gjelde for hele populasjonen.

Når vi utformet spørsmål til spørreskjemaet tok vi utgangspunkt i den daværende forskningsmodellen som baserte seg på de kvalitative funnene, i tillegg til tidligere litteratur. Den var igjen bygd på resultater som blant annet indikerte at tilgangsstyring var et hensiktsmessig konsept å fokusere på. Forskningsmodellen utgjorde hypoteser som vi hadde et mål om å finne svar på i spørsmålenes utforming. Dette vil si at vi i stor grad linket spørsmålene til blant annet tilgangsstyring, i tillegg til de andre variablene vi hadde satt sammen, som presentert tidligere *(kap. 3.2.2.1: Forskningsmodell)*. Vi fokuserte på *direkte emnerelaterte spørsmål* (Oates, 2006, s. 94) som for denne studien innebærer at spørsmålene er direkte rettet mot respondentene og deres forhold til – og erfaringer fra – temaet «ISM og klinisk arbeidsflyt» i deres arbeidshverdag ved sykehuset. Vi inkluderte ett *indirekte emnerelatert spørsmål* (Oates, 2006, s. 94) for å kartlegge utvalgets ulike fartstider i enheten vi undersøkte. På denne måten var vi bedre rustet for å kunne oppdage samvariasjoner mellom utvalgets beskrivelse og resultater fra undersøkelsen.

Vi tok også utgangspunkt i validerte spørreskjema fra tidligere kvantitativt studie; som Faxvaag et al. (2011). Jacobsen (2005) omtaler dette som at operasjonaliseringene er «ferdigvaliderte», som vil si at spørsmålene er testet ut i andre sammenhenger (Jacobsen, 2005, s. 238). Operasjonalisering er konkretisering for å kunne måle abstrakte begreper. Eksempelvis ville det ikke vært hensiktsmessig for oss å stille spørsmål som *«Hva syns du om tilgangsstyringen i organisasjonen?»*, men vi måtte heller konkretisere dette begrepet og stykke det opp i flere mer entydige delspørsmål. Dermed spør vi heller om forekomst eller hyppighet av innlogging/utlogging av et system de ansatte bruker, som «DIPS». Når spørsmålet omhandler frekvens eller hyppighet vil det være et «naturlig rangordnet nivå» (Jacobsen, 2005, s. 242). Dette forteller oss noe om hyppigheten av avbrudd i arbeidsprosessene grunnet sikkerhetsmekanismer som tilgangsstyring.

**Hvor ofte må du logge ut andre kolleger fra DIPS før egen bruk?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Alltid

*Figur 7: Eksempel på hvordan vi har utformet spørsmålene*

Når man snakker om å måle nyanser i respondentenes svar vil det være et forsøk på å måle intensiteten i enkelte forhold, ikke om de bare er for eller imot noe men hvor mye svarene spriker. Dette betegnes som «rangordnede svar» eller «ordinalt målenivå» (Jacobsen, 2005, s. 241). Vi har basert oss på ordinalt målenivå når vi utviklet spørreskjemaet for å kunne finne svaret på spørsmålet om graden av sammenheng mellom ISM og klinisk arbeidsflyt.

Til utformingen av spørreskjemaet har vi, basert på anbefaling fra en professor ved instituttet, tatt utgangspunkt i et format som kalles *semantisk differensialskala* (Oates, 2006, s. 224). Dette formatet bygger på en skala med to ytterpunkter som beskrives med adjektiver eller adverb. Vi har i tillegg tatt i bruk skalerte spørsmål der en semantisk differensialskala ikke er hensiktsmessig (se eksempel over). Dette er tilfelle for våre spørsmål som måler grad av hyppighet, samt vårt ene indirekte emnerelaterte

spørsmål (demografi). Vi har forholdt oss til en 6-punkts skala for samtlige direkte emnerelaterte spørsmål, med ulike verdier for punktene ut fra hva det blir spurt om. Fordelene med å bruke en skala med seks punkter, og ikke eks. fem, er at man ekskluderer det man kaller et *nøytralt midtpunkt*. Vi tror dette kan fordre at respondenten i større grad tar stilling til spørsmål i situasjoner hvor det kan være enkelt å bare velge midtpunktet. Vi har i tillegg inkludert et alternativt punkt som gir respondenten mulighet til å ikke ta stilling til spørsmålet der vi har ansett det som relevant. Eksempelvis på spørsmål om hvordan ulike opplæringsprogrammer oppleves, kan respondenten krysse av for «Jeg har ikke fått noen opplæring». Vi har allikevel forsøkt å unngå å inkludere for mange spørsmål som gjør et slikt punkt nødvendig, ettersom vi ønsket at flest mulig av respondentene skulle ta stilling til hvert enkelt spørsmål.

Selv om spørreskjemaet i utgangspunktet er en kvantitativ metode for datainnsamling, åpnet vi også for kvalitativ datainnsamling i metoden hvor vi opprettet tekstfelt som var frivillige å fylle inn. Dette gjorde vi gjennom å inkludere kvalitative tilleggsspørsmål som kun ble aktivert for respondenter som avga bestemte svar. Eksempelvis la vi til en aktivering for alle som ikke svarer at de alltid logger av arbeidsstasjonen når de forlater den, der de får muligheten til å nevne spesifikke situasjoner hvor de ikke logger av. Dette bidro til at vi også kunne få en mer holistisk forståelse av funnene vi gjorde oss.

Før vi inviterte utvalget til å delta i undersøkelsen sendte vi ut spørreskjemaet til tre personer med ulike spesialiseringer for evaluering. Vi sendte det først ut til to professorer ved instituttet; en som sitter på mye kunnskap rundt kvantitative studier og en som sitter på mye kunnskap rundt helseinformatikk. Etter tilbakemeldinger fra professorene, sendte vi til slutt en revidert versjon til forsker ved sykehuset som vi har hatt som kontaktpunkt i henhold til datainnsamlingen.

### Undersøkelsens gyldighet

En god forsker vil vurdere et spørreskjemas *innholdsvaliditet*, *begrepsvaliditet* og *reliabilitet* (Oates, 2006, s. 227):

- **Innholdsvaliditet**: tar for seg vurderingen av hvorvidt spørsmålene utgjør et velbalansert utvalg av domenet vi skal dekke. Vi har sikret innholdsvaliditet i spørreskjemaet vårt ved å utforme spørsmålene ut fra resultater fra kvalitativ innsamling for hver av variablene i forskningsmodellen som presentert tidligere i kapittelet (*kap. 3.2.2.1: Forskningsmodell*).
- **Begrepsvaliditet**: tar for seg vurderingen av hvorvidt vi måler det vi tror vi måler gjennom spørsmålene. Både ved utformingen av spørsmålene og analyseringen av svarene, har vi hatt fokus på å sikre begrepsvaliditet. I utformingen ved at respondentene forstår hva vi spør etter, og ikke minst at de får en lik forståelse. Vi har sett at enkelte spørsmål er mer utfordrende å sikre begrepsvaliditet for enn andre. Eks.: «For sikring av pasientdata mener jeg elektronisk rapportering er positivt/negativt» kan være et vanskelig spørsmål å ta stilling til, eksempelvis fordi noen respondenter kan fokusere på sikring i form av at ingen uvedkommende får tilgang til data, mens andre kan fokusere på sikring i form av at autorisert personell har tilgang.
- **Reliabilitet**: tar for seg vurderingen av hvorvidt vi ville fått samme resultat om vi sendte ut spørreskjemaet til de samme respondentene flere ganger. Ettersom vi tar for oss en case-studie med miksede metoder har vi verken hatt tid eller ressurser til å sikre reliabilitet på denne måten. Mye av denne undersøkelsens reliabilitet ligger i felles tillit, der vi stoler på at de

ansatte ønsker å belyse situasjoner som reflekterer virkeligheten, samtidig som vi håper de ansatte stoler på at vi ønsker å arbeide mot å finne løsninger for situasjonene som belyses.

Som tidligere nevnt i kapittelet, nådde vi ut til 59 personer med vårt spørreskjema. Å oppnå minst 30 gjennomførte svar fra dette utvalget og dermed en svarprosent på over 50 % har vært et mål vi har strebet mot, som igjen har gjort at vi har hatt tett dialog med avdelingsleder som har distribuert spørreundersøkelsen og ellers bidratt med hyppig påminnelse av de ansatte. Gjennom kontinuerlig påminnelse muntlig ved arbeidsplassen i lunsjpauser og lignende, samt en formell påminnelse per mail fikk vi økt svarprosenten betraktelig, og samlet til slutt inn 28 gjennomførte svar. Dette tilsvarer en fullstendig svarprosent på 47,46 % (28 svar av 59 respondenter). I tillegg har vi 7 ufullstendige svar, og noen av spørsmålene har derfor en høyere svarprosent enn andre (35 deltakere totalt). Dette tilsvarer en total deltakelsesprosent på 59,32 %. Hvis man får mindre enn 30 svar fra respondenter kan ikke statistisk analyse som for eksempel beregning av gjennomsnitt eller median regnes å være pålitelig. Ved ønske om å vil illustrere resultatene prosentvis, bør man også presentere antall svar i tilfeller med færre enn 30 respondenter (Oates, 2006, s. 99-100). Dette vil si at statistisk analyse kan i teorien regnes å være pålitelig kun for enkelte av resultatene fra spørsmålene i undersøkelsen. Vi presenterer samtlige resultater både i form av prosent og antall svar gjennom skjermbilder fra SurveyXact i neste kapittel *(Kap. 4: Resultater)*. Noe annet som er verdt å nevne er at samtlige av de syv respondentene som ikke gjennomførte hele skjemaet falt av etter muligheter til å avgi en mer kvalitativ respons i et tekstfelt som var frivillig å fylle inn. Først tre etter første mulighet, så de resterende fire etter andre mulighet. Det kan i denne sammenhengen tenkes at mange respondenter la mye i de kvalitative svarene sine og ikke fikk tid til å gjennomføre hele skjemaet. At noen velger å legge mer tid i de kvalitative svarene og andre mer tid i de kvantitative anser vi bare som fordelaktig for oss som dyrker en kombinasjon av kvalitative og kvantitative metoder i studien vår.

I likhet med kvalitativ, har vi også opprettet et informasjonsskriv for kvantitativ datainnsamling *(8.6: Informasjonsskriv for kvantitativ datainnsamling).* Vi går nærmere inn på hva dette skrivet tar for seg senere i kapittelet (*kap. 3.5: Etikk*). Skrivet ble tildelt på mail sammen med selvopprettelseslenke for undersøkelsen for samtlige respondenter, etter først å ha blitt tildelt avdelingsleder for evaluering.

## 3.4 Verktøy

### 3.4.1 EndNote X9

Vi har brukt EndNote X9 for å strukturere og organisere referansene våre. Det har gjort det enkelt å holde oversikt over kildebruk i oppgaven, samt at alle referansene er standardisert ved at de holder samme format gjennom hele teksten. Referansene er i tillegg samlet i programmet og synkronisert gjennom et delt bibliotek via våre UiA-brukerkontoer, dette sørger for at kilder som er ført inn i EndNote har skylagret støtte og ikke forsvinner. EndNote håndterer dato fra samme forfattere og årstall ved at det settes a, b, c, osv. etter dato. Derfor ser flere av våre referanser i tekst eksempelvis ut som: (NIST, i.d-a). Dette er for å skille de forskjellige referansene med samme forfatter og årstall. Måten vi har jobbet med EndNote er at vi har lastet ned filer som er kompatible med programmet fra databasene vi har brukt, som Oria og Scopus, der man har mulighet til å laste ned referansefiler som deretter blir lagt inn i og leses automatisk av EndNote. Dette har effektivisert arbeidet i stor grad ved at vi avlastes den manuelle innskrivingen, selv om det i en del tilfeller har vært uunngåelig legge inn kilder

manuelt hvor det har vært referert til nettsteder, dokumenter og annet. Vi lastet ned norsk APA-stil fra Universitetet i Sørøst-Norge for å få APA stilen på norsk (Universitetet i Sørøst-Norge, 2018). Vi ble henvist hit på en kobling fra UiA's egne nettsider:
https://www.uia.no/bibliotek/kildebruk-og-opphavsrett/endnote

### 3.4.2 Office 365

*Office 365* er en ypperlig tjeneste levert av Microsoft som alle studenter og ansatte ved universitetet har tilgang til med sin unike UiA-brukerkonto (UiA, i.d.-e). Kontoen er derfor under kontroll kun av den enkelte bruker, samt IT-administrasjonen ved universitetet. Dette betyr at data kan lagres på en trygg måte gjennom tjenesten, i skylagringsløsningen *OneDrive*. Dette er en løsning som NSD har godkjent i vår databehandleravtale, noe vi kommer tilbake til i neste del av kapittelet (*kap. 3.5: Etikk*).

I tillegg til sikker lagring gjennom **OneDrive**, tilbyr tjenesten en rekke verktøy som vi har tatt utbytte av i kommunikasjon og bearbeiding av data og rapport under prosjektarbeidet (Microsoft, i.d.):

- **Outlook**: Tillater oss å holde god oversikt i kommunikasjonen med samarbeidspartnere over mail. Applikasjonen sender ut varsel til innlogget enhet når ny mail mottas, slik at vi kunne føre dialoger på en rask og effektiv måte.
- **Word**: Tillater oss å skrive på samme dokument i samtid med flere maskiner. Applikasjonen inkluderer versjonskontroll, en funksjon som har bidratt til at arbeid aldri går tapt i ulike settinger.
- **Excel**: På samme måte som Word, tillater Excel oss utforming av tabeller i samme dokument. Applikasjonen har et mangfold av smarte funksjoner for fremstilling av data som vi har tatt i bruk, både i denne rapporten og underveis i datainnsamlingen.
- **PowerPoint**: I likhet med Word og Excel, tillater PowerPoint oss å arbeide på samme dokument fra flere maskiner. Vi har tatt utbytte av applikasjonen til utformingen av egne modeller og figurer som vi presenterer gjennom denne rapporten. I tillegg vil vi ta i bruk dette til en muntlig presentasjon av masterutredningen vår ved prosjektets slutt.

Ettersom verktøyene er en del av samme tjeneste og utviklet av samme firma er de godt integrert, noe som har gjort overføring av data mellom verktøyene til en enkel oppgave for oss.

### 3.4.3 SurveyXact

*SurveyXact* er en tjeneste levert av Rambøll Management Consulting som, i likhet med Office 365, alle studenter og ansatte ved universitetet har tilgang til med sin unike UiA-bruker. Tjenesten brukes til gjennomføring av spørreundersøkelser og er også det offisielt brukte verktøyet til dette i SSHF, noe som bidro til å forenkle samarbeidet med de involverte ansatte. Det foreligger databehandleravtale mellom UiA og Rambøll Management i henhold til personopplysningsloven og -forskriften (UiA, i.d.-d).

Applikasjonen tillot oss å utforme spørreskjema, distribuere det og overvåke innsamlingen underveis, for så å analysere resultatene ved hjelp av smarte funksjoner. Den tillater også å inkludere såkalte «aktiveringer» i utformingen av skjemaet, noe som var en forutsetning for vårt valg av tjeneste. Dette

innebærer at noen spørsmål kun vises for enkelte deltakere ut fra hvilke svar de har oppgitt tidligere i skjemaet.

Tjenesten driftes på egne servere av universitetsbiblioteket som systemansvarlig, noe som innebærer at undersøkelsen ikke kan deles med andre enn studenter og ansatte ved UiA. Av deres egne hjemmesider heter det at brukerstyringen er endret etter omlegging i forbindelse med GDPR, og at undersøkelser kun kan deles med brukere som har *UiA FEIDE*-tilknytning (UiA, 2019). Det optimale for datainnsamlingen vår ville naturligvis vært å kunne gi tilgang til de involverte samarbeidspartnerne ved SSHF, slik at vi kunne overholdt et enda tettere og mer effektivt samarbeid i innsamlingen.

## 3.5 Etikk

***«Forskning er av stor betydning – for enkeltmennesker, for samfunnet, og for global utvikling. Forskning er også en betydelig maktfaktor på alle disse nivåene. Av begge grunner er det vesentlig at forskning foregår på måter som er etisk forsvarlige.»*** (De nasjonale forskningsetiske komiteene, 2016b)

De nasjonale forskningsetiske komitéene (FEK) presenterer generelle forskningsetiske retningslinjer. Disse skal fungere som en inngangsport til forskningsetiske prinsipper og hensyn, men erstatter ikke de fagspesifikke retningslinjene. For vårt prosjekt er det de spesifikke retningslinjene fra Den nasjonale forskningsetiske komité for naturvitenskap og teknologi (NENT) som gjelder. I tillegg gjelder øvrige internasjonale bestemmelser, samt universitetets egne rutiner for behandling av personopplysninger (UiA, i.d.-c). Disse ble sist vedtatt av Universitetets forskningsutvalg 15.11.2018. Vedtaket innebar blant annet at lydopptak som kan identifisere en person, kun er tillatt for opptaksenheter uten internett-tilkobling, jf. del 1 punkt 7. Dette medførte utfordringer for instituttene, ettersom det ikke var tilrettelagt for utleie av slike enheter. Vi løste utfordringen ved å gå til innkjøp av vår egen diktafon, da vi hadde lagt en optimistisk plan for prosjektet og ikke hadde noen tid å miste hva gjaldt å starte datainnsamlingen. Vi ser at Universitetsbiblioteket i ettertid også har løst utfordringen og nå tilbyr diktafoner til utlån for studenter med NSD-godkjente forskningsprosjekter, noe vi er glad for på vegne av våre etterkommere (UiA, i.d.-a).

***«Begrepet «forskningsetikk» viser til et bredt sett av normer, verdier og institusjonelle ordninger som bidrar til å konstituere og regulere forskningsvirksomhet. Dette inkluderer forskningens sannhetsforpliktelse så vel som ansvaret overfor kollegaer, andre mennesker, dyr, miljø og samfunn i vid forstand.»*** (De nasjonale forskningsetiske komiteene, 2016a, s. 5)
I tillegg til ovennevnte definisjon av forskningsetikk, presenterer NENT velutformede retningslinjer detaljert for alle faser av forskningsprosessen i sin publikasjon. I stedet for å gå gjennom alle, vil vi presentere noen grunnleggende aspekter som utgjør generelle rettigheter som et forskningsobjekt har:

- **Fritt og informert samtykke**: Respondenten informeres om at det er frivillig å delta i studien og at de kan trekke seg når som helst. For at deltakelsen skal være frivillig, må respondenten få full informasjon om undersøkelsens hensikt, hvilke fordeler og ulemper det kan medføre, hvordan data skal benyttes, osv. Full informasjon er oppgitt i de tidligere nevnte informasjonsskrivene for kvalitativ- og kvantitativ datainnsamling. I tillegg har vi tildelt det Jacobsen (2005) kaller

*tilstrekkelig informasjon* muntlig for de som ikke har hatt tid til å lese gjennom skrivet i forkant av intervjuet (Jacobsen, 2005, s. 46-47; Kvale et al., 2009, s. 104; Oates, 2006, s. 56-58).

- **Konfidensialitet**: Går ut på at man ikke skal offentliggjøre personlig data som kan avsløre respondentens identitet, i tillegg til å vurdere hvor følsom og privat den dataen som samles inn er (Jacobsen, 2005, s. 47-50; Kvale et al., 2009, s. 106; Oates, 2006, s. 59). I henhold til databehandleravtalen, stiller NSD krav til lovlig oppbevaring av *personidentifiserbare data* (NSD, i.d.-b). Blant annet sier den at data skal anonymiseres før publisering. Man bør være oppmerksom på at NSD skiller mellom *anonyme* og *personidentifiserbare data*. NSD skriver mer om kontroll av anonymitet på sine nettsider (NSD, i.d.-a).

### 3.5.1 Avtale om databehandling med NSD

Basert på nasjonale krav til behandling av data i forskning inngikk vi en databehandleravtale med NSD. Denne avtalen tar for seg retningslinjer for lagring, behandling, publisering og utlevering av data. Databehandleravtalen med NSD har gjort utfordringen med å utføre forskningsprosjektet på etisk riktig vis mye enklere, fordi vi allerede i forkant av prosjektet la ned prosjektplan og forberedende arbeid for datainnsamlingen i forhold til formelle krav. Det vi la frem måtte igjen godkjennes av kvalifiserte fagfolk i NSD, noe som gjorde oss trygge på at vi ville gjennomføre databehandlingen på etisk riktig vis. Avtalens elementer tar utgangspunkt i den nye *personvernforordningen* av EØS-avtalen, som utgjør første kapittel av *lov om behandling av personopplysninger (personopplysningsloven)* (Justis- og beredskapsdepartementet, 2018). Alle nevnte artikler i dette delkapittelet er hentet fra denne lovsamlingen.

Avtalen fordret at prosjektet vårt la opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Vi opprettet informasjonsskriv for både kvalitativ og kvantitativ datainnsamling. Ved å krysse av to bokser (1, 2) og skrive under informasjonsskrivet samtykker deltakeren til (1) å delta i personlig intervju/spørreundersøkelsen og (2) at opplysninger publiseres slik at deltakeren kan gjenkjennes ved at funn kobles til demografi (bakgrunn og erfaringer). Lovlig grunnlag for behandlingen er dermed den registrertes samtykke, jf. art. 6 nr. 1 bokstav a. I begge informasjonsskriv presenterer vi rettigheter for deltakeren, gjeldende så fremt man vil kunne identifiseres i datamaterialet:

- Åpenhet (art. 12)
- Informasjon (art. 13)
- Innsyn (art. 15)
- Retting (art. 16)
- Sletting (art. 17)
- Begrensning (art. 18)
- Underretning (art. 19)
- Dataportabilitet (art. 20)

NSD har vurdert at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, j.fr. art. 12.1 og art. 13. NSD legger også til grunn at behandlingen oppfyller de kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1 f) og sikkerhet (art. 32). NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

### 3.5.2 Avtale om datainnsamling med SSHF

Vi har vært i dialog med fagansvarlig ved sykehuset siden starten av semesteret som ga oss klare retningslinjer på hva vi måtte gjøre for å få tillatelse til å samle data hos dem. SSHF hadde egen mal for masterstudenter til søknad om datainnsamling som vi fulgte. I denne la vi frem

- fullstendig informasjon om prosjektet og 'teamet' vårt,
- hva slags data vi ønsker å samle,
- hvor, hvordan og innenfor hvilket tidsrom vi ønsker å samle data,
- samt hvordan vi vil oppbevare dataene.

I tillegg la vi ved prosjektskisse, kopi av godkjent databehandleravtale med NSD, kopi av informasjonsskriv godkjent av veileder, samt signert taushetserklæring og databrukerkontrakt i SSHF. Siden studien vår kun fokuserer på teknologien og ikke behøver tilgang til helseopplysninger, pasientdata, o.l. var det begrenset hvor mye vi måtte dokumentere sett i forhold til mange andre studier innen helsevitenskap. Etter å ha fått godkjent denne søknaden kunne vi starte datainnsamlingen i de ulike avdelingene.

### 3.5.3 Forskningsetikk ved UiA

For å forsikre oss om at de ulike etiske kravene ble oppfylt, måtte vi også følge interne retningslinjer og rådføre oss med behandlingsansvarlig institusjon etter behov. Som forskere på UiA har vi ansvar for å kjenne og følge anerkjente forskningsetiske normer og retningslinjer, både innen vårt fag og generelle retningslinjer ved universitetet. UiAs forskning skal være preget av fire grunnverdier (UiA, i.d.-b).:

1. **Åpenhet**: Åpenhet er det beste forebyggende middel mot uredelighet i forskning. Derfor skal ingen bevisst holde skjult for andre noen sider ved sin forskningsvirksomhet, utenom de tilfellene hvor det er gode og allment aksepterte grunner for konfidensialitet.
2. **Tillit**: Forskning er, som all mellommenneskelig samhandling, basert på tillit. Enhver må kunne stole på sine medarbeidere og overordnede.
3. **Ansvar**: All forskning medfører et ansvar for at den kunnskapen man får tilgang til ikke misbrukes, og at den kommer samfunnet til gode.
4. **Respekt**: Alle som er involvert i og berørt av forskningsarbeid, har krav på respekt fra andre. Enhver ansatt skal ha respekt for sine kollegers forskningsarbeid, både innen eget fagområde og på fagområder en selv ikke kjenner til.

I god ånd med universitetets grunnverdier for etisk forskning har vi tilbudt intervjupersonene å oversende materialet vi ønsker å ta i bruk fra intervjuet før vi publiserer det. Dette takket samtlige åtte intervjupersoner ja til. I tillegg til å sikre habilitet, medfører dette at data blir riktig presentert og

eventuell *følsom* og/eller *privat informasjon* (Jacobsen, 2005, s. 47-48) som individet ikke ønsker inkludert rettes om på eller fjernes fra utredningen. Siden vi anonymiserer all data og hele tiden har vært åpne med respondentene på bruk av demografi som kan identifisere personer involvert, har ikke dette bydd på noen store utfordringer for oss.

# 4. Resultater

I dette kapittelet viser vi til resultater fra vår case-studie i SSHF. Som presentert i forrige kapittel har vi triangulert metoder for datainnsamling gjennom en kombinasjon av kvalitative og kvantitative tilnærminger. Vi vil videre ta for oss resultater fra spørreundersøkelsen og bruke funn fra intervjuer til å forklare dem. Vi fremviser resultatene gjennom delkapitler som bygger på forskningsmodellen vår, som vi presenterte i forrige kapittel *(kap. 3.2.2.1: Forskningsmodell)*. For relevante funn fra dokumentasjon henviser vi også til dette delkapittelet.

Datamaterialet som ligger til grunn for resultatene vi viser til i dette kapittelet er tilgjengelig via OneDrive: *https://uiano.sharepoint.com/:f:/t/RickOgJorgi/ErGg_ICh-9FLjwvipK6TkXgBBxvU_qeVwStO58r-GXBMpw?e=VHQodX*. Dessverre har vår organisasjon (UiA) stengt av tilgang via lenke til å kun gjelde for brukerkontoer som er tilknyttet UiA. Ved behov for innsyn i datamateriale bes de som ikke har en UiA-brukerkonto derfor ta kontakt med oss på mail, så finner vi en løsning på det (jorgeb13@student.uia.no / rickyo13@student.uia.no).

## 4.1 Tilgangsstyring

I dette delkapittelet viser vi til resultater for variabelen som presentert i *kap. 2.5.2.1 (Tilgangsstyring)*. I intervju med leder for informasjonssikkerhet definerer respondenten (R2) organisasjonens overordnede håndtering av tilgangsstyring slik: *«Tilgangsstyringen i [EPJ-systemet] DIPS gjøres i utgangspunktet ved at det er en journalsperre for alle, men systemet vet hvor du er. DIPS vet hvilken avdeling du er på, så journalen vil åpnes for den tiden du er på avdelingen; det er både rollebasert og litt tidsmessig styrt.»*

### 4.1.1 Passord og passordhåndtering

R2 beskriver prosessen med passordhåndtering for ansatte: *«Når du blir ansatt så signerer du taushetserklæring og databrukerkontrakt. Når du starter i arbeid vil du få et brukernavn og et engangspassord som må byttes. Det er få systemer som støtter to-faktor autentisering, men vi får snart noe i forhold til å ha VPN-tilgang. Noen systemer har det, men det er ikke ordentlig to-faktor av type «bankID», mer som en «en-og-en-halv-faktor» med autentisering over SMS som ikke er helt skuddsikkert»*.

R3 sier følgende: *«Ansatte må bytte passord med jevne mellomrom, vi har satt intervall på det*.» Respondenten sier passordene er synkronisert, som vil si at byttet gjelder for alle systemer, og eksemplifiserer: *«pålogging på AD [Active Directory] og pålogging på DIPS. Men du må skrive inn passord hver gang du logger på DIPS, så du kommer ikke rett inn fra AD. Vi kunne ha satt det på, men har satt det på sånn at du må angi passordet. Det er fordi at mange på sykehuset ikke sitter på kontor, men sitter i et felleskap og kanskje løper litt rundt og da kan man risikere at PC-er står pålogget etter*

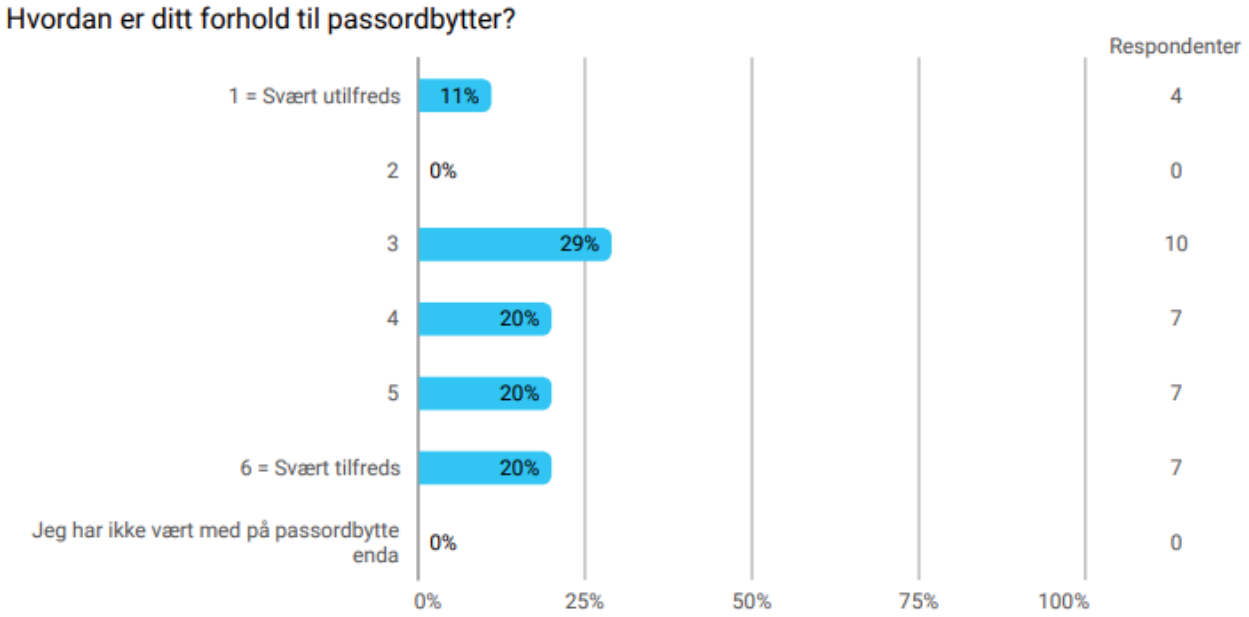
*en som er rundt og gjør en jobb, men at noen kanskje logger seg inn i eksempelvis DIPS med denne personens bruker. Det er ikke noe ønskelig situasjon, men i den hverdagen som er der så vil det nok det skje, vi er veldig tydelig på at det er ikke aktuelt å logge seg på med noen andre eller deler passord osv. og det er vesentlig for at alt skal logges på deg selv. Det tror jeg gjøres i mye mindre grad i alle fall».*

Under intervjuene med klinikere spurte vi om hvordan respondentene forholder seg til passord, hvorpå R4 bekrefter uttalelsene fra R3: *«Vi har nå fått samkjørt systemene slik at byttet gjelder for alle systemer, og man slipper å gjøre tre-fire passordbytter på en dag»*. Respondenten sier videre at tidligere mangel på integrerte systemer medførte større utfordringer hvor man glemte passord, ikke fikk passordbytte godkjent, og lignende – noe som skapte mye «dobbeltarbeid».

R5 sier følgende: *«Man bruker jo passordet så ofte at man kommer fort inn i det»*. Flere av respondentene argumenterer for at man må finne en egen logikk på utformingen av passordene for å huske dem. Samtidig forteller tre av dem videre at problemene oppstår når det tas ferie, hvorpå man ikke bruker passordet på fire uker. To av respondentene legger i denne sammenheng til at de da får et behov for å skrive ned passordet, enten i et papirnotat eller på privat mobiltelefon.

Avslutningsvis argumenterer R8 for at dagens teknologi burde være tilstede for at man kan innføre alternative løsninger for autentisering: *«Hvis man kan logge inn på telefonen med tommelen, kunne man fint logget inn på PC-en med tommelen også»*.

Basert på disse uttalelsene benyttet vi oss av spørreundersøkelse til å stille klinisk ansatte ved intensiv enhet (Kristiansand) følgende spørsmål:




*Figur 8: Tilgangsstyring - Forhold til passordbytter*

På spørsmål om ansattes forhold til passordbytter i organisasjonen svarer 40 % at de er utilfreds, mens de resterende 60 % er i mer eller mindre grad tilfreds med organisasjonens håndtering av passordbytter. 11 % sier seg svært utilfreds, noe som kan indikere at organisasjonen har en vei å gå hva gjelder å dekke individuelle behov blant de ansatte når det kommer til passordhåndtering.

På mulighet til å utdype tanker om **ting som kan gjøres annerledes når det gjelder bytting av passord**, gir fem av seks respondenter uttrykk for at det byttes for ofte. En respondent argumenterer også for at dette etterhvert gjør det vanskelig å finne gode passord.

For formelle krav og retningslinjer til passord og passordhåndtering som SSHF må forholde seg til henviser vi til kap. 2.3 og kap. 5.2.2 i Normen (2018) og Faktaark 31 ( Direktoratet for e-helse, 2018c, d).

### 4.1.2 Autorisering og autentisering

R3 har følgende å si om de klinisk ansatte som brukere av systemene: *«Vi tenker at de har ganske høy respekt for innlogging i DIPS, fordi de vet om konsekvensene, eksempelvis at hvis noen snoker gjennom deres bruker så blir de selv ansvarlige. Så er det nok litt mindre bevissthet i henhold til pålogging på PC, og det har nok noe med måten å jobbe på å gjøre: av- og pålogging på PC tar litt tid, tid som du kanskje ikke har i en travel hverdag. Av- og pålogging på DIPS går relativt mye fortere. Men at en ansatt ser på pasientdata med en annen pålogget bruker er jeg ganske sikker på at skjer»*.

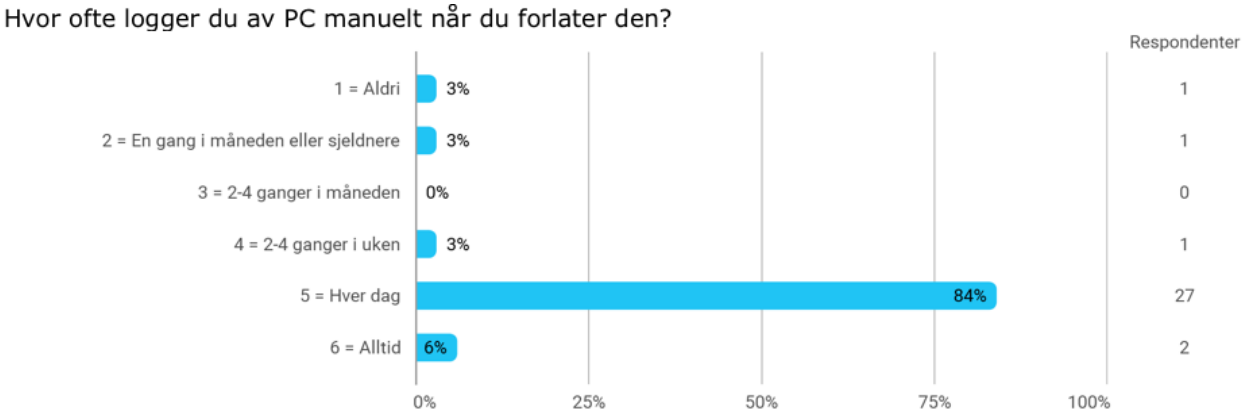
I likhet med flere av respondentene, innleder R4 med at *«Det blir noen ganger, men det varierer hvor mye man er inne på PCen».* R5 konstaterer at det avhenger av hvilken rolle man har og hvor man er plassert for dagen: *«Hvis man er assistent og på forskjellige rom hvor man ikke har hovedansvar for pasient, er det ikke ofte man behøver å logge seg på».* Vi presenterer situasjoner med hensyn til arbeidsstasjoner for ulike roller og seksjoner i enheten senere i kapittelet *(kap. 4.3: Maskinvare)*.

R7 sier: *«Vi har en fellesbruker, men denne har kun tilgang til prosedyrene og lignende, og vi får ikke tilgang til pasienter herfra.»*. R4 sier: *«PC-skjermen går i lås etter en viss tid – en sikkerhetsfunksjon for at ingen skal kunne ta i bruk noen andres autoritet»* og fortsetter: *«Pasienten kommer først, men man må logge seg inn minst en gang for å skrive rapport [...] vanligvis skjer avbrytelsene på intensiv slik at man bare må gå, og man prioriterer ikke å logge av. Blir man avbrutt må man logge seg inn flere ganger for å fortsette der man slapp».* Med «flere ganger» sikter respondenten til at både arbeidsstasjonen (Active Directory) og DIPS krever innlogging. I sammenheng med funksjonen automatisk utlogging konkluderer R4 med følgende: *«Sikkerhetsfunksjonen er nødvendig for å verne om pasientene våre, slik at ingen uvedkommende får tilgang til dataene. Vi behandler tross alt opplysninger som er konfidensielle»*.

Flere av respondentene argumenterer for risikoen ved å ikke logge av egen bruker. R4 sier: *«Det kan være en risiko dersom man har spesielle tilganger, der man kan få skylden for å snuse i noe man ikke hadde noe med»*. Vi stilte R6 et alternativt spørsmål om det kan tenkes at en ansatt vil kunne skrive i journalen med en annen ansatts bruker, dersom flere av de ansatte jobber på den samme pasienten. Respondenten (R6) svarer følgende: *«Ikke i journalen. I journal kvitterer vi alltid med navn under hvis vi ikke bruker egen bruker [...] det har egentlig bare vært tilfelle der noen har skrevet en journal, glemt å godkjenne, og så godkjenner vi for de»*.

På oppfølgingsspørsmål om inn- og utlogging oppleves som tidkrevende, oppsummerer R8 med følgende: *«Det går med årsverk»*.

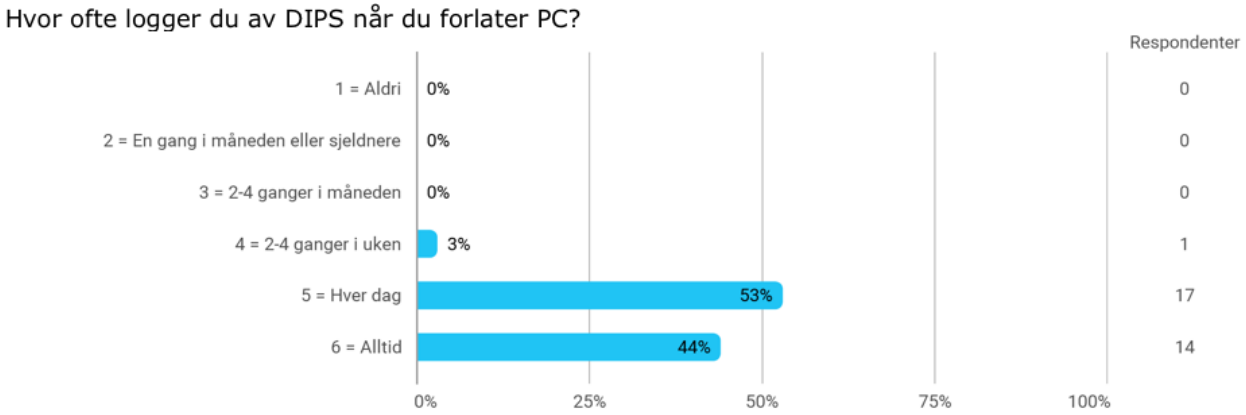
På bakgrunn av disse uttalelsene benyttet vi oss av undersøkelse til å stille følgende spørsmål:




*Figur 9: Tilgangsstyring - Logge av PC*

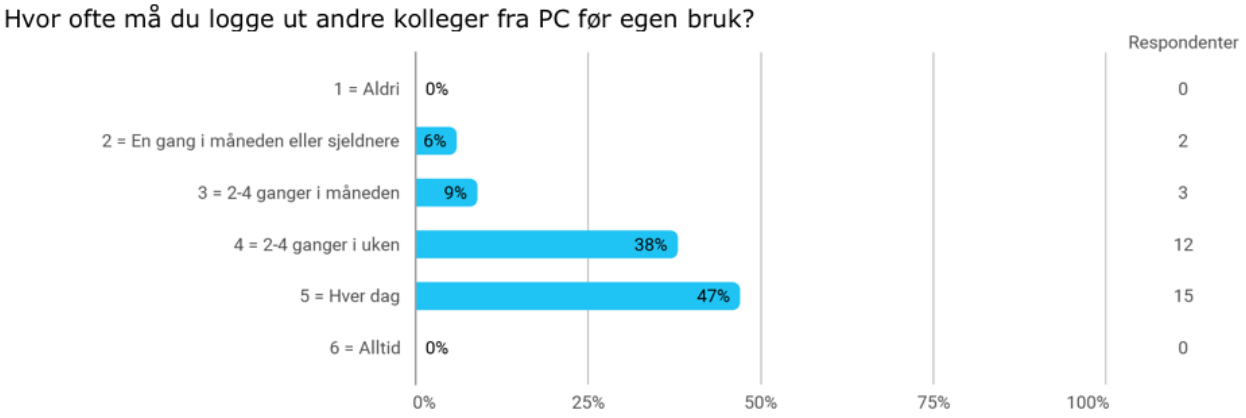
På spørsmål om hvor ofte de logger av arbeidsstasjonen når den forlates, svarer 90 % av respondentene at dette blir gjort minst hver arbeidsdag, hvorav 6 % svarer at de alltid logger av. Av de øvrige 10 % fordeler svarene seg jevnt med enkeltpersoner som ikke følger trenden i organisasjonen og sjelden eller aldri logger av.

For dette spørsmålet ga vi respondenter som ikke alltid, men heller ikke aldri logger av (verdi: 2-5) mulighet til å oppgi typiske situasjoner hvor de ikke logger av. En av respondentene skriver: *«Jeg har eget kontor og låser som oftest kontordøren når jeg forlater PC»*. Dette kan tenkes å være en medvirkende årsak til de øvrige 10 % som svarer at de ikke logger av arbeidsstasjonen hver dag, ved at ikke alle ansatte er i lik situasjon ved enheten. Vi ga også respondenter som svarte at de aldri logger av muligheten til å forklare hvorfor de aldri logger av arbeidsstasjonen, noe respondenten som avga dette svaret valgte å ikke svare videre på.



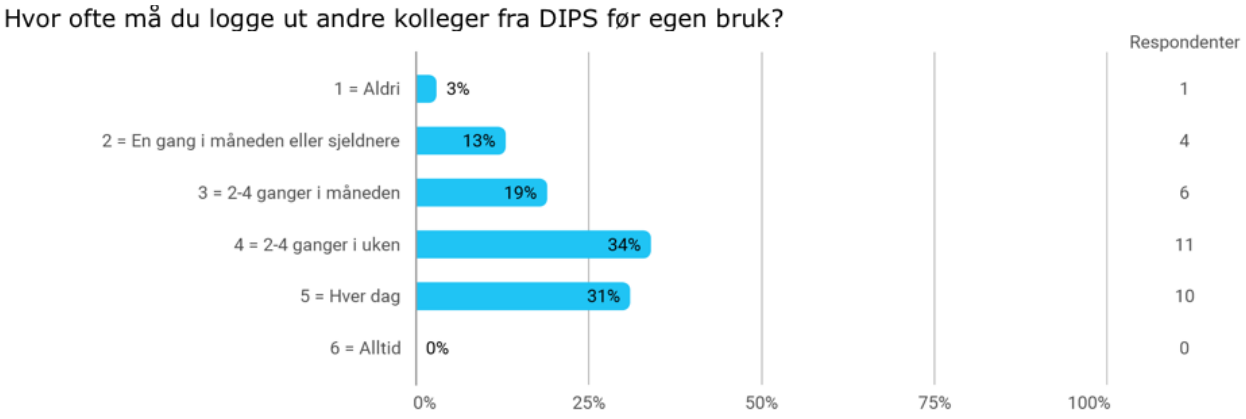

*Figur 10: Tilgangsstyring - Logge av DIPS*

På spørsmål om hvor ofte de logger av EPJ-systemet «DIPS» når arbeidsstasjonen forlates (eller her), svarer hele 97 % at de gjør dette hver dag, hvorav 44 % logger av hver gang (figurtekst her?). En respondent (3 %) svarer at dette er noe som blir gjort nærmere annenhver dag (eller her?).




*Figur 11: Tilgangsstyring - Logge ut andre fra PC før bruk*

Nesten halvparten av respondentene (47 %) rapporterer om at de daglig må logge andre kolleger ut av arbeidsstasjonen før de kan bruke den selv. 38 % anslår at dette er noe de gjør 2-4 ganger i uken. De resterende 15 % svarer at dette skjer mindre enn fire ganger i måneden.




*Figur 12: Tilgangsstyring - Logge ut andre fra DIPS før bruk*

På spørsmål om hvor ofte de må logge ut andre kolleger fra EPJ-systemet «DIPS» før de selv kan bruke arbeidsstasjonen, svarer 65 % av respondentene at dette gjøres mellom annenhver og hver dag, hvorav 31 % sier det gjelder for hver dag. En respondent mener dette aldri skjer, mens de resterende 32 % sier det skjer mindre enn fire ganger i måneden.

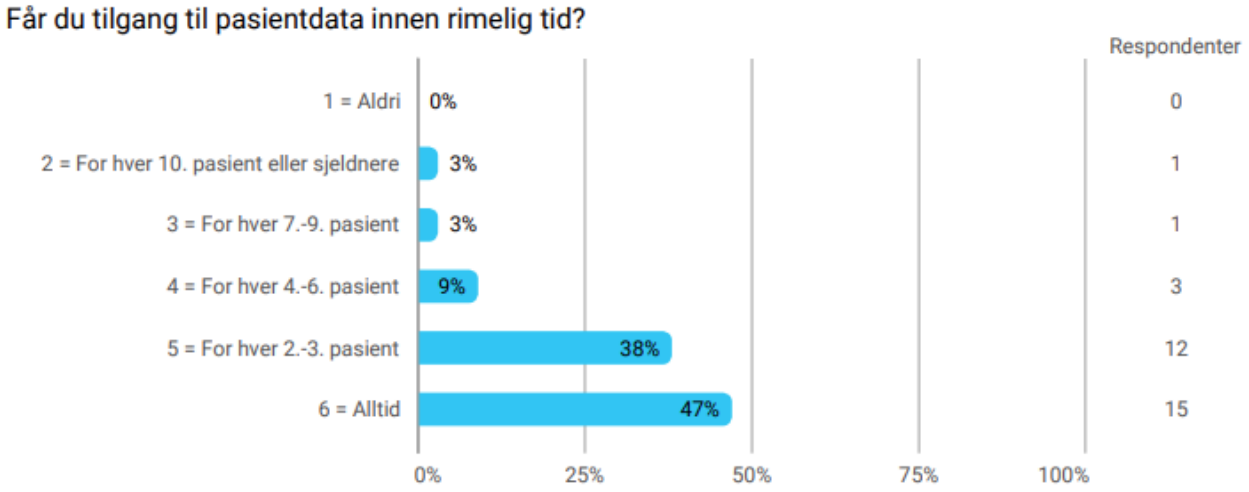
### 4.1.3 Kontroll av tilgangsrettigheter (s. 31)

I sammenheng med tilgangsstyring snakker R1 også om logging: *«I DIPS har man logging/sporbarhet med hensyn til informasjonen som ligger der. Dette viser noe av det endrede fokuset på informasjonssikkerhet i nyere tid, der man nå kan få oversikt over hvem som har vært inne og sett på de forskjellige dokumentene, journalene osv. Det er krav som pasienten har»*.

Respondenten sikter til en funksjon som er blitt innført basert på krav som Normen stiller til organisasjonen i henhold til logging av tilgang. R2 bekrefter videre i forhold til loggingen at *«det har blitt gjort en stor jobb for å dokumentere behov for tilgangsstyring på ulike roller»*.

Underveis i intervjuene går flere av klinikerne inn på egen tilgang til pasientdata, og hvordan kravene til dette har blitt mer omfattende over tid. Flere av klinikerne bekrefter uttalelsene fra lederne. R7 sier: *«Det finnes nå en logg hvor man legger fra seg spor av at man har vært inne og lest på pasientdata».* R6 sier: *«Tidligere kunne vi gå inn og se på alle pasienter på hele huset, nå er det begrenset til at vi får se alle på vår egen avdeling og noen på akuttmottaket»*.

På bakgrunn av disse uttalelsene benyttet vi oss av undersøkelsen til å stille følgende spørsmål:




*Figur 13: Tilgangsstyring - Tilgang til pasientdata*

På spørsmål om hvorvidt de får tilgang til pasientdata innen rimelig tid, svarer nesten halvparten av de ansatte (47 %) at dette er tilfelle i enhver situasjon, mens 38 % svarer at det er tilfelle for hver andre til tredje pasient. De resterende 15 % svarer at dette er tilfelle for hver fjerde pasient eller sjeldnere, hvorav en respondent (3 %) mener dette skjer for hver tiende pasient eller sjeldnere.

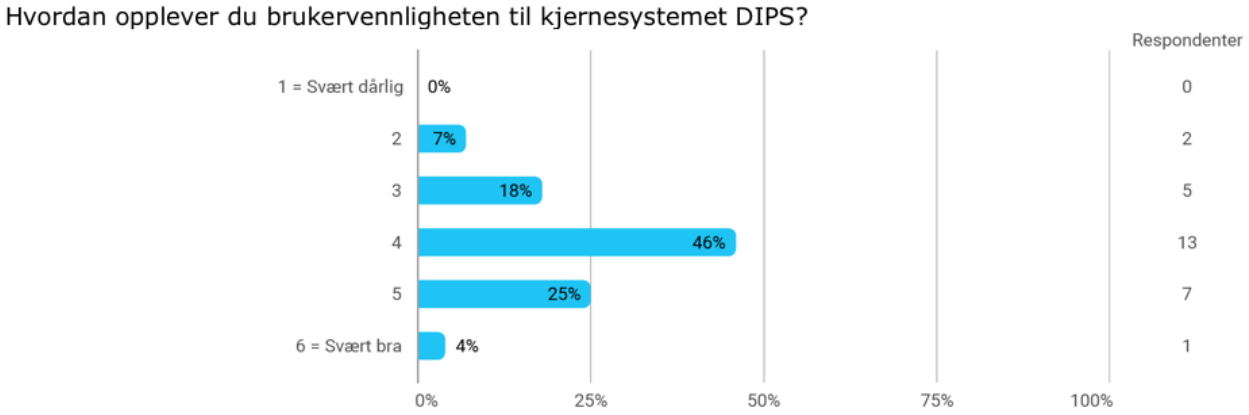
## 4.2 Programvare

### 4.2.1 EPJ-system

EPJ systemet som brukes av organisasjonen heter «DIPS». Det bekreftes av funn fra intervjuene. R2 beskriver systemet på følgende måte: *«DIPS, som er pasientjournalsystemet vårt, har flere tusen brukere. Alle som jobber for å yte helsehjelp har en lovpålagt dokumentasjonsplikt, så DIPS gjør to ting: Den ene er at det har dokumentasjonsdelen i pasientjournal; også er det et logistikkelement der for å følge pasienten rundt i systemet».* Informasjonssikkerhetslederen fortsetter å beskrive systemet: *«DIPS har veldig mange integrasjoner. DIPS er et godt eksempel å bruke som en viktig applikasjon fordi den understøtter sykehusdriften. Det er knyttet både til andre fagsystemer på sykehuset, laboratoriesystem, radiologisystem, osv. Man kan sitte i DIPS og booke en MR-undersøkelse av pasienten, så går den informasjonen i en kø hos radiologer, som da vet at det kommer en pasient som skal ha bilde av ulike deler av kroppen».*

I intervjuene med klinikere spurte vi respondentene om hvilke systemer de bruker, hvorpå R5 svarer følgende: *«Stort sett DIPS. Føler jeg har tilgang til alt jeg trenger her [...] det er greit å bruke, da jeg er vant til det. Det gikk også greit å sette seg inn i ved nyansettelse, men jeg kan ikke huske at vi fikk noen organisert opplæring for systemet den gangen [2011]»*. Bruken av DIPS understøttes av R7: *«Jeg bruker mest DIPS i forhold til pasient.».* R8 bygger videre på uttalelsene om systemet: *«Jeg syns systemene fungerer greit. DIPS er et veldig stort program, og jeg bruker ikke så mange av de funksjonene som ligger inne. Det går både på tilgang og behov, og legene bruker mye mer av DIPS enn vi [sykepleierne] gjør»*.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å spørre respondentene om hvordan de opplever brukervennligheten i systemet DIPS:




*Figur 14: Programvare - Brukervennlighet i DIPS*

Tre av fire (75 %) av respondentene mener brukervennligheten til DIPS i mer eller mindre grad er bra. En av fire (25 %) mener den i mer eller mindre grad er dårlig. En respondent (4 %) mener brukervennligheten er svært bra, mens ingen viser sterk misnøye.

**Forslag til hva som kan gjøres annerledes i DIPS**: Gjøre pleieplanen enklere.

### 4.2.2 Oppslagsverk for prosedyrer

Basert på intervjuene ble det konstatert at respondentene bruker et prosedyreoppslagsverk som heter «EK-web». Det nevnes av 4/5 klinikere i starten av intervjuene. R7 sier følgende: *«Vi tar ut prosedyrer fra EK-web; et system vi bruker mye, som går på pasientsikkerhet»*. Respondenten sikter i denne sammenheng til pasientens sikkerhet i form av å motta riktig behandling. R8 sier følgende om systemet: *«EK-web kan være litt vanskelig å navigere i. Du må vite hva du skal søke etter. Av og til er ikke søkeordene nødvendigvis konstante, ting blir ikke kalt det samme. Er du på jakt etter en prosedyre kan du bruke litt tid før du finner det du skal ha. Kan få mange treff man må lete gjennom alle for å finne den man er ute etter. Så ligger prosedyrer som f.eks. gjelder for Arendal og en annen som gjelder for Kristiansand. Så må finne ut hvilke prosedyrer man sitter og leser på og om en prosedyre som er skrevet i Arendal faktisk gjelder her også»*.

Videre i intervjuene følger respondenter fra IE opp med ytterligere betraktninger rundt EK-web på spørsmål om hvordan de opplever å bruke systemene:

R7 sier følgende: *«Det er blitt veldig standardisert, der alle prosedyrer ligger på EK-web for at alt skal være og utføres likt. Enkelt å finne frem til de prosedyrene jeg skal. Vi har blitt mye flinkere til å legge inn prosedyrer i vår avdeling. Hver morgen vet vi nøyaktig hva vi skal gjøre, slik at vi ikke gjør forskjellig».*

R4 sier: *«Det er varierende – noen er gode, noen er dårlige. I EK-web må man vite akkurat hvor man skal klikke. Hvis man lager en prosedyre uten søkbare stikkord, kan det være tilnærmet umulig for andre å finne den. Man må kjenne systemet og logiske søkemetoder, og evt. alternative måter å lete på»*. Respondenten (R4) eksemplifiserer hvordan dette skaper «workarounds»: *«Hvis jeg ikke finner prosedyrene ved å søke på logiske stikkord, kan jeg eksempelvis gå på 'barneposten' siden det er dem som sannsynligvis har den. Eventuelt tar jeg bare en telefon og spør»*.

R5 sier følgende om EK-web: *«Jeg syns kanskje dette systemet kan være litt uoversiktlig, ja. Essensielle felter står i liten tekst, og oppsettet og brukervennligheten burde generelt vært smartere og bedre».* R4 fortsetter å forklare hvordan systemet ikke oppleves som optimalt: *«Misfornøyd med logikken i søkemotorikken. Litt fritt opp til den som lager prosedyren med logisk tittel, etiketter. Et fint system når man forstår hvordan å bruke det best mulig, noe som har tatt tid å forstå. Ikke alle har tilgang. Jeg var selv fagsykepleier i fire år uten å få tilgang, og brukte da andres brukere»*.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å spørre respondentene om hvordan de opplever brukervennligheten i systemet EK-web:


*Figur 15: Programvare - Brukervennlighet i EK-Web*

På spørsmål om hvordan de opplever brukervennligheten til systemet for prosedyreoppslagsverk, svarer 58 % at den i mer eller mindre grad er god. 42 % svarer at den i mer eller mindre grad er dårlig. Vi ser en stor spredning her. Det kan være verdt å merke seg at kun én av respondentene (4 %) opplever brukervennligheten som svært bra, samtidig som tre (11 %) opplever den som svært dårlig.

Gjennom aktivering ga vi respondentene som svarte at brukervennligheten til EK-web i mer eller mindre grad er dårlig muligheten til å komme med forslag til hva som kan gjøres annerledes i systemutformingen:

- Prosedyren på intensiv ligger fast som et ikon
- Enda mer oversiktlig og raskere å finne prosedyrer.
- Rydde opp i gamle dokumenter, skille bedre i dokumenters titler, slik at man enklere kan finne de som er aktuelle. Jeg bruker kun søk for å finne det jeg trenger, og funnene er uoversiktlige
- Kunne søke på et ord og få opp tilsluttende tema. Også ved skrivefeil i søkefeltet hadde det vært praktisk å få opp det maskinen "tror" vi har ment å skrive, komme med forslag...
- Søkefunksjonen er svært dårlig - stort forbedringspotensial.
- Alt for mange utdaterte prosedyrer. Får opp prosedyrer som ikke gjelder eget sykehus.
- Øke antall søkeord man kan bruke.
- Flere søkeord som når frem til de ulike prosedyrene.
- Logiske søkemuligheter, kunne søke «termer» som relateres til det man søker etter – øker treffmulighetene
- Vanskelig å finne rett søkeord.

### 4.2.3 Doble føringer

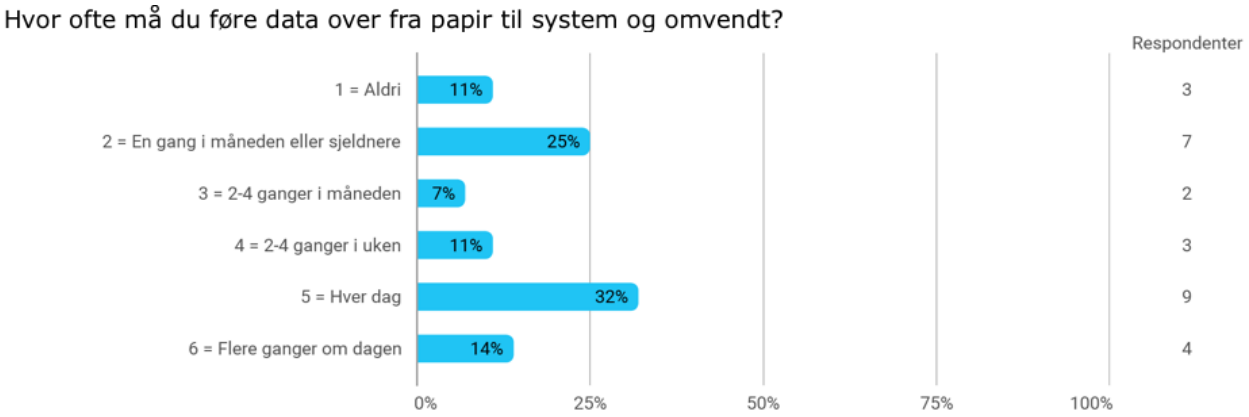
Under intervjuer kunne alle respondentene fra utvalget av klinikere bekrefte forekomst av 'doble føringer' eller 'dobbeltarbeid' som følge av dokumentasjonsarbeid. Det kom frem at det skal innføres et nytt system for kurveføring og rapportering som heter «Metavision».

R1 svarer følgende på spørsmål om det oppstår dobbeltarbeid: *«Ja, helt sikkert en del dobbeltarbeid, og det er mye kontrollarbeid også. Om du får andre til å skrive for deg, må man til slutt inn å lese dokumentet etterpå og å se til at det er riktig. Og det er dobbeltarbeid»*.

R4 sier: *«Vi logger all overvåkningsdata ved å føre kurver på papir»*. Videre forklarer R6: *«Vi har våre intensivkurver som bare vi forholder oss til, så vi må dobbeltføre en del for avdelingene, i hovedsak postoperative pasienter, fordi vi har 'scanning-systemer'. Hvis vi har medikamenter som blir gitt kontinuerlig skal disse skrives over på kurven. Har også litt dobbeltføring på medikamenter. Våre intensivkurver fører vi over til avdelingskurvene. Dette skal lukes vekk når vi får denne dataføringen [Metavision]»*.

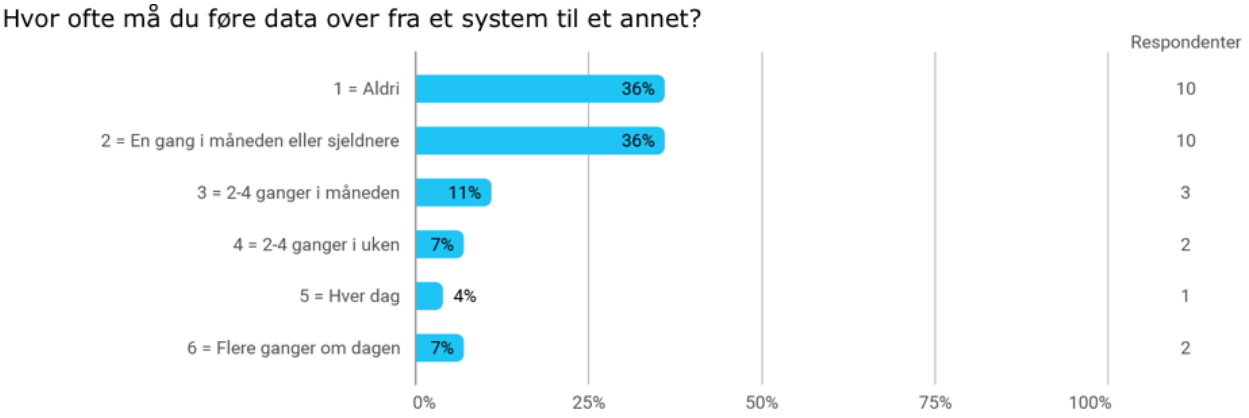
R7 eksemplifiserer: *«Kurveføring, medisinark, rapport... Vi har mye dobbeltføringer. Dette blir trolig bedre med Metavision, men innføringen byr også på nye problemstillinger: Da må man begynne å lære alle navnene. Alle medisinene skal ha et generisk navn»*. Dette understøttes av R8: *«I forhold til pasientdokumentasjon skal det dokumenteres elektronisk, på papir, kurver, avdelingskurver. Vi kan skrive ned samme tall tre forskjellige plasser eksempelvis. Når Metavision kommer vil det forsvinne eller være mye mindre dobbeltarbeid. Når det først kommer vil det være minst like mye, da det ikke er alle avdelinger som har Metavision som fortsatt må ha det på papir, en avdeling har sine kurver og en annen har sine kurver. Det er en del dobbeltarbeid, ja»*.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å stille følgende spørsmål:




*Figur 16: Programvare - data fra papir til system*

På spørsmål om de må føre data fra papir til system og omvendt svarer 46 % av respondentene at dette gjør de minst hver dag, hvorav 14 % svarer at dette er noe de gjør flere ganger daglig. 11 % svarer at de aldri gjør dette. De resterende 43 % rapporterer at det er tilfelle sjeldnere enn hver dag.




*Figur 17: Programvare - data fra ett system til annet*

På spørsmål om hvor ofte de må overføre data fra et system til et annet, svarer 36 % at dette aldri er tilfelle. Ytterligere 36 % svarer at det er tilfelle en gang i måneden eller sjeldnere. 11 % melder om at dette gjøres hver dag, mens de resterende 18 % gjør dette omtrent en til fire ganger i måneden. Understøtter påstander om at de systemene som ligger til grunn for å bistå klinikerne i deres arbeidsprosesser er godt integrert.

## 4.3 Maskinvare

R3 kommer med en generell uttalelse om IT-systemene i organisasjonens arbeidsmiljøer: «*Jeg skulle ønske vi kunne få IT-systemene til å støtte arbeidsprosessene enda bedre, som av/pålogging, mobile enheter (personlig) osv. Av- og pålogging på PC som deles av andre er en utfordring*».

### 4.3.1 Tilgang på arbeidsstasjoner

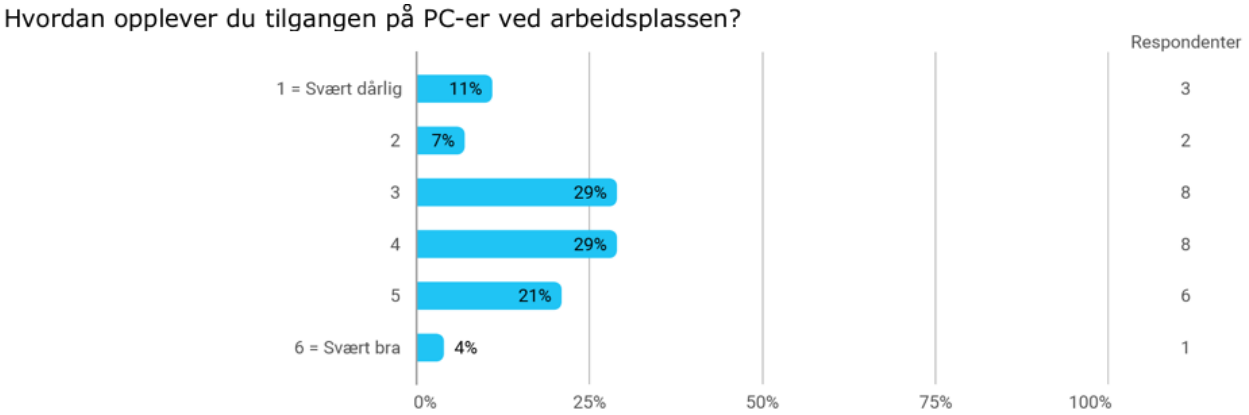
I sammenheng med sikring av informasjon sier leder for informasjonssikkerhet (R2) følgende om tilgang på arbeidsstasjoner: «Det er lite PC-er og systemer som er i åpne lokaler ved klinikkene. De er

som regel skjermet, som på vaktrom eller steder hvor det er andre klinikere til stede. Dette reduserer sannsynligheten for at uvedkommende får tilgang til sensitive data».

R7: *«Vi har litt få maskiner, men vi har også fått flere i det siste. Skriver rapporter på hver vår maskin, noe som fungerer greit»*.

R6 sier: *«Vi driver med en-til-en behandling veldig ofte, med en pasient og arbeidsstasjon. Da er det om å gjøre å få en PC til den stasjonen, for det har vi ikke alltid»* og fortsetter: *«På postoperativ har vi tre brukte stasjoner, der må vi inn og ut av DIPS hele tiden. Og dette kan gå mange ganger [med trykk] i løpet av en dag hvor flere av de ansatte jobber med de samme pasientene»*. R8 rapporterer om at det er 7-8 ansatte på en vakt ved postoperativ seksjon.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å stille følgende spørsmål:




*Figur 18: Maskinvare - tilgang på PC*

På spørsmål om hvordan de opplever tilgangen på arbeidsstasjoner ved arbeidsplassen, svarer 54 % av respondentene at tilgangen i mer eller mindre grad er bra. 46 % svarer at den i mer eller mindre grad er dårlig. 3 respondenter (11 %) svarer at tilgangen er svært dårlig, mens bare en respondent (4 %) mener den er svært bra.

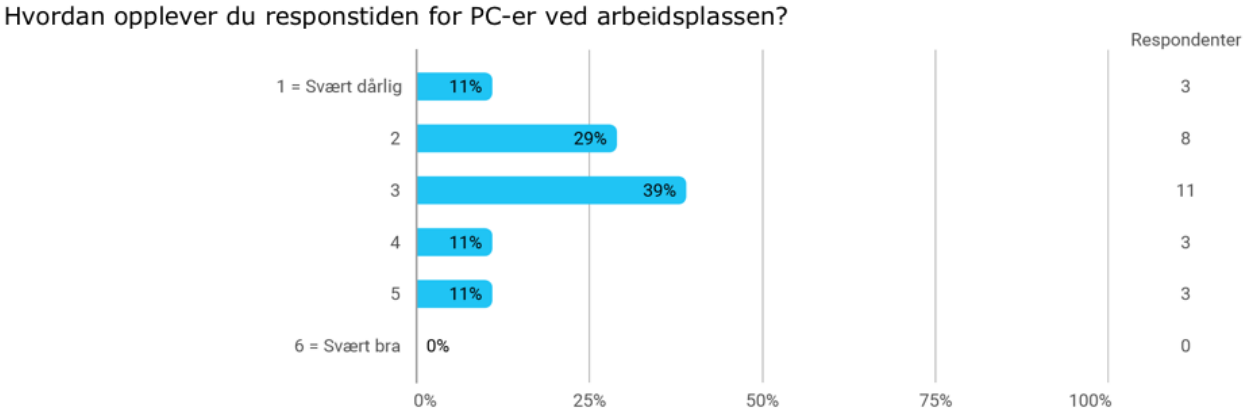
### 4.3.2 Responstid for arbeidsstasjoner

R5 sier: *«Maskinene våre kan virke litt treige til tider, noe som kan virke frustrerende»*. Dette understøttes av flere respondenter. R6 sier: *«På intensiv enhet må vi jobbe pro-aktivt, og det å vente på gamle maskiner virker både frustrerende og ødeleggende»*. R8 sier: *«Det er trege PC-er med store programmer som skal dras i gang her på enheten. Så er ikke alle PC-ene '2019' [nyere modeller], og det er stor forskjell på de»*.

R8 kommer videre med et konkret eksempel på situasjoner som typisk opptar tid: *«Noe som er veldig frustrerende er hvis en kollega har vært på PC-en og den har låst seg, så har man vanligvis mulighet til å logge av den som er logget på, noe som ikke alltid kommer opp. Da må man fysisk slå av PC-en via knapp slik at den starter opp fra bunn av, og alle startprogrammene må kjøres i gang på nytt. Da bruker du jo en halv arbeidsdag»,* avslutter respondenten med en litt overdreven tone og et megetsigende blikk.

Basert på argumenter om behovet for pro-aktivt arbeid ved enheten kommer R6 med et spesifikt ønske om flere og nyere maskiner som er bedre tilpasset for akutte situasjoner.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å stille følgende spørsmål:




*Figur 19: Maskinvare - Responstid*

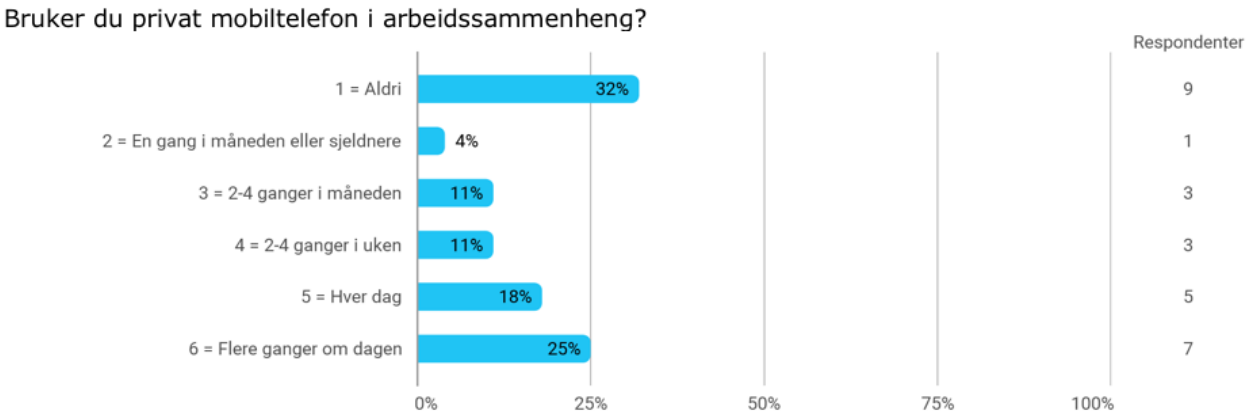
På spørsmål om hvordan de opplever responstiden for arbeidsstasjonene, svarer 78 % av respondentene at den i mer eller mindre grad er dårlig. 22 % svarer at den i mer eller mindre grad er bra, hvorav ingen mener den er svært bra.

### 4.3.3 Bruk av private enheter (BYOD)

Under intervjuene med klinikere spurte vi respondentene om de bruker mobile enheter i jobbsammenheng. På dette spørsmålet kunne vi se tendenser til en viss uenighet internt blant de klinisk ansatte. R4 svarer følgende: *«Jeg bruker privat mobiltelefon til å slå opp i felleskatalogen og Google-research, fordi den er enkelt tilgjengelig»*, noe som understøttes av R5: *«Jeg bruker privattelefon til felleskatalogen, fordi det er det enkleste»*. R7 sier: *«Jeg bruker aldri mobilen på jobb, men mange gjør det. Jeg går selv bare inn på internett på datamaskinen ved behov […] noen bruker telefonen mye, men jeg gjør ikke det»*.

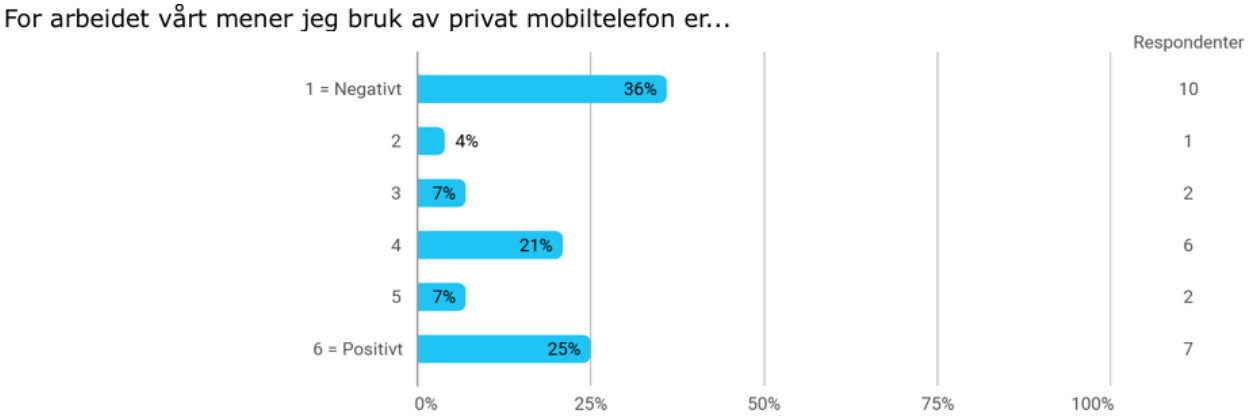
R6 argumenterer for at samtidig som telefonen er blitt et arbeidsredskap, er den også blitt en 'tidstyv': *«Det er klart, de som går med telefonen i lomma kan slå inn på mange ting veldig fort, men det blir også feil med andre ting. Det opptar arbeidsdagen til mange»*. Med «andre ting» sikter respondenten til sosiale medier og varsler som kan tenkes å virke distraherende for en person i arbeid. Respondenten (R6) utdyper ytterligere om BYOD senere i intervjuet relatert til spørsmål om hvordan de opplever IT- og sikkerhetskulturen blant ansatte: *«Vi har fire fagmøter i året, der det blant annet blir forsøkt gjort noe med mobilbruk – en diskusjon jeg deltar i stort sett hver gang»*. Respondenten mener det bør foreligge et sterkt fokus på å unngå forstyrrelser: *«Vi har litt dødtid av og til. Men jeg har jobbet så langt tilbake at jeg sier til barna at om de er skadet eller syke, så ikke ring mamma, for hun er på jobb. Nå er det helt andre grenser, og det er ikke helsevesenets skyld, men samfunnet som har endret seg. Dette må jeg jo forholde meg til. Men så fort andres bruk går utover tidsbruk i behandling av pasienter, så blir det et problem for meg».* Respondenten avslutter med: *«Jeg er ikke enig i at en person som sitter på telefonen, er like mye på alerten som en som sitter og strikker. En kultur som har endret seg her»*.

Basert på disse uttalelsene benyttet vi oss av undersøkelsen til å stille følgende spørsmål:




*Figur 20: Maskinvare - Bruk av mobiltelefon*

På spørsmål om respondenten bruker privat mobiltelefon i arbeidssammenheng svarer 43 % at dette gjør de hver dag, hvorav 25 % gjør det flere ganger om dagen. 32 % svarer at de aldri bruker privat mobiltelefon i arbeidssammenheng. Resultatene viser stor spredning, noe som bekrefter tendensene vi så i intervjuene.




*Figur 21: Maskinvare - Mening om bruk av mobiltelefon*

På spørsmål om hva respondenten mener om bruk av privat mobiltelefon i arbeidet, svarer 53 % av respondentene at det i mer eller mindre grad er positivt, mens 47 % svarer at det i mer eller mindre grad er negativt.

## 4.4 Bruker

### 4.4.1 Opplæring og kompetanse

I intervjuer med klinikere spurte vi respondentene om de føler de har tilstrekkelig kunnskap om sikker bruk, hvorpå R4 svarer følgende: *«Jeg har tatt e-læringskurs i datasikkerhet ut fra det som vi er pålagt. Vi ansatte gjør av og til vurderinger på egenhånd, noe som kan gi forskjellige måter å oppfatte ting på. Dette kan henge sammen med mangel på tid til opplæring og lignende. Vi snakker om det internt, diskuterer det på møter, og kommer nesten alltid frem til at flere har oppfattet ting litt forskjellig»*.

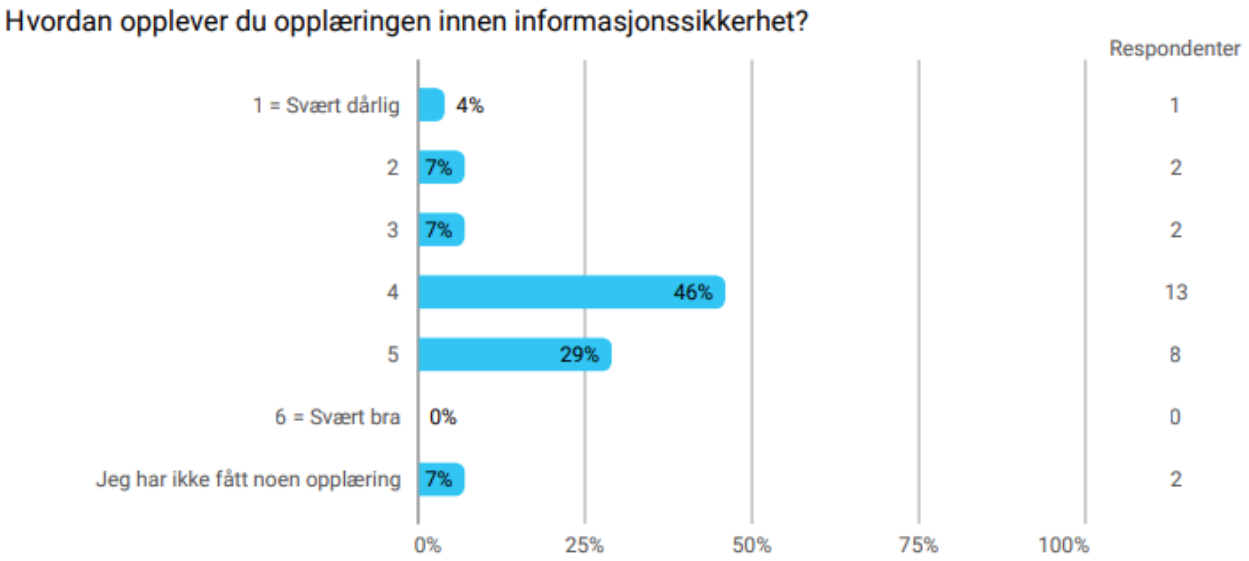
Under intervjuer med ledere spurte vi hvordan organisasjonen håndterer ansattes kunnskap om sikker bruk av systemene, hvorpå R1 svarer følgende: *«Vi er nok for lette på det totalt sett, men det er nok noen e-læringspakker, noe informasjon for nyansatte. Så har vi hatt en total opplæring av hele organisasjonen, men det begynner å bli en del år siden, og det er nok et område hvor jeg mener det er potensiale for forbedring. Jeg vet at andre organisasjoner sender ut falske e-poster for å 'monitorere' hvordan bevisstheten er ift. håndtering av tvilsom innkommende e-post, og det kunne vi godt ha sett på i større grad. Vi har nok et potensiale hva gjelder å bevisstgjøre og følge opp våre ansatte»*. R7 bekrefter at det finnes slike e-læringspakker: *«Vi har en læringsportal i EK-web hvor du kan teste dine kunnskaper. Hvis du eksempelvis har vært logget inn som doktor, kan du ikke gå fra den uten å logge av. Da kan alle gå inn og lese sensitive opplysninger»*. På spørsmål om hva som kan tenkes å gjøres annerledes svarer R1 følgende: *«Jeg tror vi kan bli flinkere på å bruke intranett som informasjonskilde, og å sende ut informasjonsskriv periodisk. På sikt vil vi kunne ha mer regelmessig oppfriskningskurs av de ansatte, typisk gjennom e-læring og lignende. Så jeg tror det vil skje mer der, og at det blir viktigere i tiden fremover»*.

I intervjuene med klinikere spurte vi om de selv føler det settes av nok tid og ressurser til kursing og opplæring hvorpå R4 svarer følgende: *«Kunnskap om systemene er ikke bare problematisk for nyansatte, men også etterhvert som man blir mer voksen, trenger man mer tid til å sette seg inn i dem. Det er ikke prioritert tid til opplæring, vi må bruke ressursene våre der de er viktigst, nemlig hos pasienten. Det trenger ekstra motivasjon og vilje for å sette seg inn i systemet og bruke det både riktig og effektivt»*. Flere av respondentene understøtter påstanden om mangel på avsatte ressurser. R7 sier: *«Jeg tror ansatte generelt har grei kontroll på systemer som brukes. Problemet er at vi hele tiden er for få folk»*. R8 bekrefter dette: *«Nei, det settes ikke av nok ressurser. Men det skjønner jeg, for vi er ikke nok folk. Det gjøres absolutt forsøk, og det står ikke på viljen. Jeg er en av de som driver med opplæring, så jeg vet hvor hardt det sitter inne»*.

R4 fortsetter å forklare hvordan mangelen på avsatte ressurser medfører utfordringer: *«Nå er det slik at alt må prioriteres, eksempelvis at man må velge mellom å ta vare på pasient eller gjennomføre pålagt sertifisering. Jeg har heller ikke lyst til å begynne med research når jeg kommer hjem fra jobb»*.

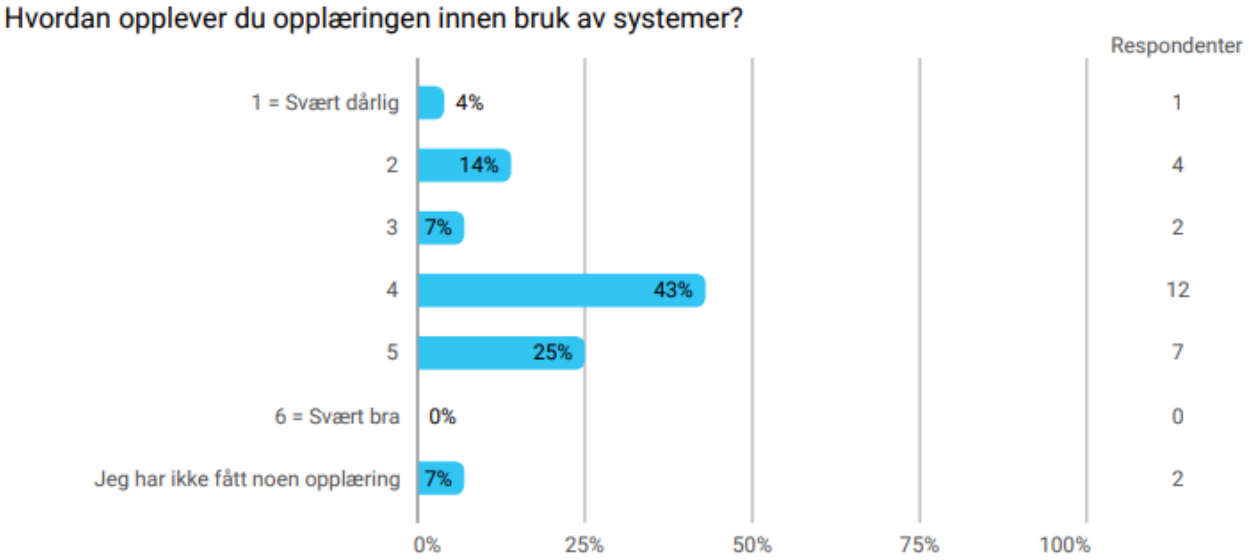
Avslutningsvis kommer R4 med et spesifikt ønske om *«mer avsatt tid til opplæring i alt; også fag, noe det er alt for lite tid til».*

Basert på disse uttalelsene ønsket vi å måle ansattes tilfredshet med organisasjonens håndtering av opplæring og kompetanse. Vi benyttet oss av undersøkelsen til å stille respondentene to spørsmål angående opplæring, henholdsvis for informasjonssikkerhet og bruk av systemer:




*Figur 22: Bruker - Opplæring innen sikkerhet*

75 % av respondentene er i mer eller mindre grad tilfreds med opplæringen innen informasjonssikkerhet. 18 % mener opplæringen i mer eller mindre grad er for dårlig. De resterende 7 % har ikke fått noen opplæring innen informasjonssikkerhet.



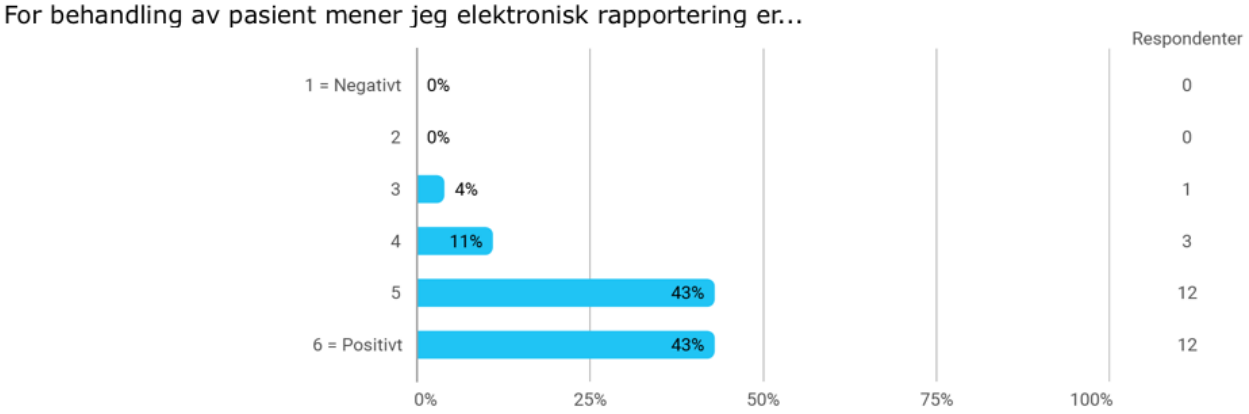

*Figur 23: Bruker - Opplæring innen systembruk*

Når det gjelder opplæring innen bruk av systemer er 68 % av respondentene i mer eller mindre grad tilfreds. 25 % mener opplæringen er for dårlig, hvorav en respondent viser kraftig misnøye. De resterende 7 % har, i likhet med informasjonssikkerhet, heller ikke fått noen opplæring innen bruk av systemer. Dette indikerer at to av respondentene ikke har deltatt i noe opplæringsprogram.

### 4.4.2 Behandling av pasient og pasientdata

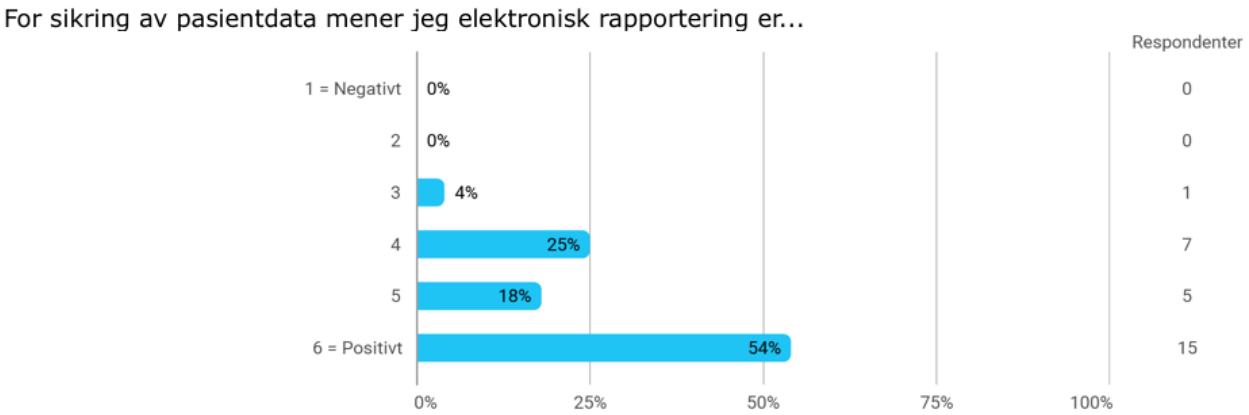
På spørsmål om hvordan IT- og sikkerhetskulturen oppleves blant de klinisk ansatte svarer R7 følgende*: «Vi ringer, legger inn blodprøver i DIPS. Helt normalt.»* Respondenten tror de ansatte har en god sikkerhetskultur, og fortsetter: *«Jeg tror nok det har vært noen kampanjer med fokus på å gjøre ansatte flinkere til å ta vare på pasientdata»*.

I forhold til dilemmaet med sikring av pasientdata satt i kontrovers med behandling av pasient konkluderer R3 med følgende: *«Vi kan ikke finne oss i en situasjon der de ansatte ikke får tilgang til opplysninger ved behov. Det er mye mer kritisk enn at noen får tilgang til noe de ikke skulle. Liv og helse trumfer sikring av data når de står opp mot hverandre»*. R8 sier: *«Hvis jeg kan gå inn i en akutt situasjon og vite hva jeg står ovenfor, er det mye lettere å gå inn og utgjøre en forskjell – en god jobb»*.




*Figur 24: Bruker - Elektronisk rapportering iht. pasient*

På spørsmål om behandling av pasient svarer hele 96 % at elektronisk rapportering er mer positivt enn negativt. Dette vitner om at systemene som etterhvert har erstattet rapportering i papirform har gjort dette på en god måte. En av respondentene er allikevel ikke overbevist, og mener dette er noe mer negativt enn positivt.




*Figur 25: Bruker - Elektronisk rapportering iht. pasientdata*

På spørsmål om sikring av pasientdata forholder også 96 % seg mer positive enn negative til elektronisk rapportering, med en litt ulik fordeling. Samtidig som enda flere mener det er utelukkende positivt, er det også flere som tipper mot midten av positivt/negativt-skalaen.

# 5. Diskusjon

I dette kapittelet tar vi for oss resultatene for hver av variablene og presenterer det i delkapitler, diskuterer dem med utgangspunkt i litteraturen og kommer med egne refleksjoner. Videre beskriver vi med egne ord det vi mener utgjør begrensningene for denne studien.

## 5.1 Resultatene

### 5.1.1 Tilgangsstyring

Undersøkelsen viser at 60 % av respondentene er i mer eller mindre grad tilfreds med organisasjonens håndtering av passordbytter. Respons fra intervjuer indikerer at mange ansatte virker å synes det er en plage med så mange formelle krav til passord, samtidig som de er innforstått med nødvendigheten av det. Vi tror organisasjonen har gjort en god jobb med å bevisstgjøre de ansatte rundt sikkerhetsaspektet dette bunner i, samt å inngå kompromiss i henhold til klinikernes behov sammen med organisasjonens behov for sikkerhet.

Fra våre intervjuer med ansatte i intensiv avdeling kom det frem at det ofte oppstår avbrudd i arbeidsprosessene relatert til tilgangsstyring, ofte som et resultat av mangelfull tilgang og dårlig responstid på arbeidsstasjoner. Med utgangspunkt i tidligere forskning, av blant annet Ferreira et al. (2010) og Smaradottir (2018) kan dette omtales som brukbarhetsproblemer og barrierer for aksept, i tillegg til et tidspress i arbeidet som kan medføre avbrudd som igjen kan gjøre det tidkrevende å logge inn igjen i systemene på grunn av avbrudd i henhold til automatisk avlogging fra systemene. Hvis vi tar utgangspunkt i undersøkelsen til Faxvaag et al. (2011) som blant annet viser at 45 % av respondentene på sykehus opplevde at de måtte logge ut andre før de kunne sette i gang med eget arbeid. Vår spørreundersøkelse viser at omlag halvparten av respondentene (47 %) at de daglig må logge ut andre kolleger fra arbeidsstasjoner før de selv kan ta det i bruk. 38 % anslår at det skjer 2-4 ganger i uken. Dermed mener 85 % at dette forekommer flere ganger i uken. 34 % av respondentene opplever at de må logge ut andre kolleger fra EPJ-systemet 2-4 ganger i uken, mens 31 % av respondentene svarer at dette forekommer hver dag. Det vil si at 65 % av respondentene opplever at de må logge ut andre fra EPJ systemene flere ganger i uken før de selv kan starte arbeidet.

Undersøkelsen viser at over halvparten (53 %) av respondentene ikke alltid opplever å få tilgang til pasientdata i tide, noe som i særlig grad er uheldig for avdelinger som intensiv enhet hvor vi avholdt undersøkelsen. Respons fra intervjuer understøtter at enheten har et spesielt behov for å arbeide pro-aktivt, noe som gjør organisasjonens håndtering av tilgangsstyring til en kritisk faktor i arbeidsprosessene. Organisasjonen gjør rett i å bruke logging av tilganger til å vurdere behov for tilgang. Vi anbefaler at SSHF fortsetter å kontrollere tilganger gjennom logging og innfører tiltak der de ser behov.

En av informantene, R8, mente at dagens teknologi burde være tilstede for at man kan innføre alternative løsninger for autentisering: *«Hvis man kan logge inn på telefonen med tommelen, kunne man fint logget inn på PC-en med tommelen også»*. Dette kan være interessant å forske videre på i sammenheng med ISM og klinisk arbeidsflyt. Vi tror innføring av nye løsninger for autentisering ved bruk av nye teknologiske verktøy som eksempelvis biometrisk leser for fingeravtrykk kan bidra til en

reduksjon av konflikter hva angår tilgangsstyringen i organisasjonen. Det er for oss åpenbart at en slik innføring over tid spesifikt vil kunne redusere dagens tall for tidsforbruk i forhold til autentisering blant klinisk ansatte i SSHF. Dette kan igjen bidra til større grad av aksept blant de ansatte, som videre potensielt kan resultere i at flere av de ansatte følger formelle retningslinjer.

### 5.1.2 Programvare

I tråd med funn fra Smaradottir (2018), understøtter resultater fra studien vår at brukervennligheten påvirker akseptansebarrieren blant de ansatte i organisasjonen. Respondentene i undersøkelsen vår uttrykker at de er relativt positive når det kommer til brukervennligheten i DIPS. 75% har svart at brukervennligheten i mer eller mindre grad er bra . Dermed kan vi anslå at brukervennligheten i DIPS har et akseptabelt nivå og ikke skulle indikere at konflikter iht. til brukervennlighet og arbeidsflyt er utbredt i den sammenhengen.

Vi ser tendenser til intern uenighet angående i EK-web med en stor spredning i resultatet fra undersøkelsen. Kvalitative innsamlede data har i denne sammenheng fanget opp elementer som hinter til at brukernes kjennskap til systemet avgjør deres syn på systemets brukervennlighet. Kvalitativ respons fra undersøkelsen (som presentert i *kap. 4.2.2: Oppslagsverk for prosedyrer*) er implikasjoner som bør tas med til videre vurdering i organisasjonens håndtering av systemet. Her kommer klinisk ansatte med gode og konkrete eksempler på hva som kan gjøres annerledes.

I undersøkelsen rapporterer nesten halvparten av respondentene at de overfører data fra system til papir og omvendt daglig. Dette utgjør dobbeltarbeid som ikke er ønskelig ved kliniske arbeidsmiljøer, og i særlig grad ved avdelinger som intensiv enhet, hvor det er kritisk at de ansatte har en effektiv flyt i sine arbeidsprosesser. Kvalitativ datainnsamling har avdekket at organisasjonen er i ferd med å innføre systemet Metavision som skal erstatte føring av pasientdata på papir. Vi tenker at jo raskere innføringen finner sted, desto bedre er det for alle parter. Dette vil også kunne medføre bedre flyt i samarbeidet med andre sykehus som allerede opererer med systemet, eksempelvis ved pasientoverføring.

Resultater som tilsier at de ansatte på generell basis sjelden er nødt til å overføre data fra et system til et annet vitner om at de systemene og funksjonene som ligger til grunn for å bistå klinikerne i deres arbeidsprosesser er godt integrert. Videre forskning bør i denne sammenheng rettes mot å belyse beste praksis for implementering av pasientdatasystemet Metavision i integrasjon med kjernesystemet DIPS.

### 5.1.3 Maskinvare

Som vi nevnte i *kap. 3.1.2 (Populasjon og utvalg)* og videre presenterte i forrige kapittel, fordeler de ved postoperativ seksjon tre arbeidsstasjoner på 7-8 ansatte. Med andre ord; om alle ansatte ved seksjonen samarbeider parvis med hverandre om deling av stasjoner, har de fremdeles en stasjon for lite.

I undersøkelsen rapporterer tre av fire (78 %) at responstiden for arbeidsstasjoner i mer eller mindre grad er dårlige, noe som vitner om stor enighet. Dette fenomenet ble vi oppmerksom på allerede under intervjuer med klinikerne, der flere respondenter kunne melde om ekstremt treige maskiner

som opptar mye av arbeidsdagen. Vi mener det er ekstremt uheldig om gamle og utdaterte maskiner skal ha en innvirkning på offentlig helsehjelp i vårt samfunn. Ut fra informasjon fra intervju med en av lederne vet vi at organisasjonen har en statlig budsjettramme å forholde seg til, og at det krever sterke argumenter for å ha noen innflytelse på denne rammen. Videre forskning bør strebe mot å belyse viktigheten av å ha raske og effektive arbeidsstasjoner i denne typen arbeidsmiljø.

Ut av resultater fra undersøkelsen presentert i *kap. 4.3.3 (Bruk av mobile enheter (BYOD))* kan vi se en tydelig sammenheng mellom svarene. Andelen respondenter som er positive til bruk av privat mobiltelefon i arbeidet samsvarer godt med andelen respondenter som bruker privat mobiltelefon i arbeidet. Dette kan ha mange forklaringer; eksempelvis mangel på tilstrekkelig maskinvare og programvare i arbeidsmiljøet, tilstrekkelig tilgang til informasjon, og tilstrekkelig opplæring for systemer. En oppfordring til videre forskning kan være å lete etter årsaker til at ansatte velger å bruke privat mobiltelefon i arbeidet, samt undersøke muligheten for å innføre formelle praksiser for bruk av privat mobiltelefon i arbeidsprosesser.

### 5.1.4 Bruker

Smaradottirs (2018) argumentering for at tilgangsstyring krever opplæring av brukere og påvirker arbeidsflyt og daglige rutiner for helsepersonell understøttes av resultater fra denne studien. I undersøkelsen kommer det frem at majoriteten av respondenter er fornøyd med opplæringen de får, hvorav tre av fire (75 %) mener opplæringen for sikring av informasjon i mer eller mindre grad er god. For opplæring i bruk av systemer svarer 68 % at den i mer eller mindre grad er god. Uttalelser fra kvalitative intervjuer har avdekket at det ikke nødvendigvis er kvaliteten på opplæringen det står på, men avsatte ressurser til å gjennomføre den. R1 kommer med konkrete eksempler på tiltak som kan iverksettes for å bidra til økt fokus rundt sikkerhet; (intern utsending av falske e-poster, bruke intranett som informasjonskilde og sende ut informasjonsskriv, oppfriskningskurs gjennom e-læring o.l.), og tror det vil skje mye på denne fronten fremover. Vi støtter dette og tror organisasjonen vil kunne oppnå gode resultater ved å følge anbefalinger om beste praksis basert på erfaringer fra andre sykehus i offentlig sektor.

Undersøkelsens største utvalgskonsensus oppnådde vi på spørsmål om hvorvidt respondenten mener elektronisk rapportering av pasientdata er positivt eller negativt, både i form av behandling av pasient og sikring av pasientdata. Samtlige respondenter med unntak av én (96 %) svarte at de mener elektronisk rapportering i mer eller mindre grad er positivt, både for pasientbehandlingen og informasjonssikkerheten.

## 5.2 Begrensninger

Helt siden vi startet planleggingen av prosjektet har vi vært bevisst på at vi som forskere kun er to uerfarne masterstudenter som på ingen måte ville kunne gjennomføre en studie av like god kvalitet som en godt erfaren forsker. Vi har erfart at å avholde semi-strukturerte intervjuer består av så mye mer enn å stille en rekke individer et sett av identiske spørsmål og la dem snakke fritt. Vi har også erfart at å samle kvantitative data gjennom utvikling av spørreskjema er mye mer avansert enn å bare kjøre en tankemyldring på aktuelle spørsmål og svaralternativer. Bidragene fra våre veiledere og andre fagpersoner både ved universitetet og sykehuset underveis i prosjektet har vært til stor hjelp for oss, blant annet ved at vi har kunne fått intervjuguide og spørreskjema evaluert før innsamling av data. Vi

har lært enormt mye om metodene vi har tatt i bruk underveis i studien som vi ikke var kjent med i innledende arbeid, noe vi heller ikke ønsker å legge skjul på. Bruken av kombinerte metoder har hjulpet oss med å få en så holistisk studie som mulig, til tross for at vi ikke har mye erfaring innen forskningen. Den manglende erfaringen har blant annet medført at innledende arbeid mot datainnsamling som eksempelvis utforming av intervjuguide ikke nødvendigvis har blitt utført på en veldig god måte i enhver sammenheng, noe vi har avdekket og rettet på gjennom møter og dialoger med samarbeidspartnere. Sammen har veilederne og andre samarbeidspartnere sørget for at vi har gjennomført prosjektet med en god trygghet internt i arbeidet vårt. Vi kontrollerte kvaliteten på vårt spørreskjema gjennom evaluering først av veiledere og professor ved instituttet med ekspertise innen kvantitativ forskning, og videre evaluering av revidert versjon fra fagansvarlig ved sykehuset, før vi distribuerte skjemaet til utvalget. Veilederne har gitt oss indikasjoner på relevante konsepter og begreper som typisk foreligger i litteraturen, samt avdekket gode og dårlige valg av oss i innledende arbeid, eksempelvis med uhensiktsmessig struktur og dårlige formuleringer i intervjuguide og spørreskjema. Vi anser oss selv å ha blitt satt i en ekstremt heldig situasjon av universitetet, ved at vi har fått denne muligheten til å benytte oss av UiAs offisielle samarbeid med SSHF og fått tildelt veiledere med ekspertise innenfor hvert sitt felt; henholdsvis informasjonssikkerhet og e-helse. Vår ene veileder med ekspertise innen informasjonssikkerhet har gitt oss klare tilbakemeldinger på måten vi har valgt å avgrense temaet informasjonssikkerhetsledelse. Dette var blant annet bidragsytende til å definere kategorier i konseptmatrisen, og videre i utformingen av intervjuguide basert på disse. Vår andre veileder med ekspertise innen e-helse har bidratt med sin brede kompetanse på forskningslitteraturen innen fagområdet. Vi har fått kontinuerlige tips om hva som potensielt kan utgjøre «de gode spørsmålene» for studien og hvordan vi bør angripe dem med hensyn til vår kontekst. Veilederen har også gitt oss henvisning til dokumentasjon som utgjør formelle krav og retningslinjer utarbeidet av Direktoratet for e-helse som er gjeldende for SSHF. Vi fremla våre planer for hva som kan utgjøre et representativt utvalg tidlig, hvorpå veilederen vurderte valgene våre og kom med alternative forslag. Takket være dette mener vi at vi har fått et godt representativt utvalg i datainnsamlingen for studien vår, og vi synes måten vi har gått frem på i datainnsamlingen har vært heldig for misjonen med å belyse problemstillingen. Ved å først gå undersøkende frem med intervjuer for så å ta utgangspunkt i resultatene fra disse i et spørreskjema, har vi vært i stand til å besvare forskningsspørsmålene: *Hvilke aspekter for informasjonssikkerhetsledelse er viktige i organisasjonen? (RQ1)* og *I hvilken grad er aspektene tilstede i organisasjonen? (RQ2)*.

# 6. Konklusjon og implikasjoner

I dette kapittelet konkluderer vi med hovedfunn og implikasjoner fra studien. Et av våre hovedfunn bygger på at det foreligger 96 % enighet om at det er mer positivt enn negativt med elektronisk rapportering, både for behandling av pasient og sikring av pasientdata. På grunnlag av dette kan vi med høy sannsynlighet konkludere at EPJ-systemet er kommet for å bli i organisasjonen, og at «DIPS» gjør en god jobb med å understøtte klinikernes arbeidsprosesser. Videre viser resultater fra undersøkelsen til 78 % enighet om at responstiden for arbeidsstasjoner i mer eller mindre grad er dårlig. Respons fra intervjuer med klinikere indikerer at arbeidsstasjonene med dårlig responstid opptar store deler av arbeidsdagen for enkelte. Vi vil anbefale organisasjonen å vurdere muligheten til å avsette ressurser til nye arbeidsstasjoner i form av datamaskiner som understøtter klinikernes arbeidsprosesser på en mer effektiv måte. Videre forskning bør i denne sammenheng rettes mot å belyse graden av konflikter og konsekvenser som kan oppstå som følger av mangel på understøttende arbeidsverktøy. Basert på tidligere forskning og litteratur som ser brukervennlighet i sammenheng med tilgangsstyring, undersøkte vi brukervennligheten for programvare som brukes blant de ansatte. Respondentene virker stort sett fornøyd med brukervennligheten i «DIPS», der tre av fire (75 %) mente at denne i mer eller mindre grad er god. Basert på resultater fra spørreundersøkelse og intervjuer kunne vi se større uenighet rundt brukervennligheten til prosedyreoppslagsverket, EK-web. Kvalitative innsamlede data har i denne sammenheng fanget opp elementer som hinter til at brukernes kjennskap til systemet i stor grad avgjør deres syn på systemets brukervennlighet. Kvalitativ respons fra undersøkelsen (som presentert i *kap. 4.2.2: Oppslagsverk for prosedyrer*) er implikasjoner som bør tas med til vurdering i organisasjonens videre håndtering av systemets utforming. Her kommer brukerne i form av klinisk ansatte med gode og konkrete eksempler på hva som kan gjøres annerledes. Vi ser klare konflikter mellom aspekter ved informasjonssikkerhetsledelse og arbeidsflyt i helsesektoren. Dette henger blant annet sammen med resultater fra undersøkelsen omkring tilgangsstyring, som viser at klinikere i organisasjonen på bakgrunn av ulike forhold opplever å måtte logge ut andre kolleger fra DIPS og arbeidsstasjoner før de selv kan sette i gang med arbeidet. Dette kan i noen tilfeller skyldes at arbeidsstasjoner er utilgjengelige, og i andre tilfeller at responstiden for dem ikke er tilstrekkelig. I tilfeller hvor det er snakk om programvare vil nok maskinvare også ha en innvirkning i forhold til systemets responstid og dermed også hvor lang tid det tar å logge inn og ut av «DIPS». Resultatene fra spørreundersøkelsen viser at 65 % av respondentene opplever at de må logge ut andre fra EPJ-systemene flere ganger i uken, mens 85 % av respondentene opplever å måtte logge ut andre fra arbeidsstasjoner flere ganger i uken. Majoriteten av klinikere i undersøkelsen er fornøyd med kvaliteten på opplæringen innen informasjonssikkerhet. Kvalitative funn har avdekket at organisasjonens utfordringer relatert til opplæring og kunnskap handler om hyppighet og mangel på avsatte ressurser. En respondent fra IT-ledelsen (R1) mener at det finnes et forbedringspotensial: *«Vi har nok et potensiale hva gjelder å bevisstgjøre og følge opp våre ansatte»*. Vi anbefaler SSHF å følge opp etter nevnte konkrete tiltak fra respondenten selv (intern utsending av falske e-poster, intranett som informasjonskilde og sende ut informasjonsskriv, oppfriskningskurs). Vi avslutter rapporten med å gjengi noen velvalgte ord fra to av våre respondenter: leder for klinisk IKT (R3): *«Vi kan ikke finne oss i en situasjon der de ansatte ikke får tilgang til opplysninger ved behov. Det er mye mer kritisk enn at noen får tilgang til noe de ikke skulle. Liv og helse trumfer sikring av data når de står opp mot hverandre»*.

# 7. Referanser


Barker, E., Barker, W., Burr, W., Polk, W. & Smid, M. (2019). *Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations* (NIST Special Publication 800-57 Part 2 Revision 1). NIST. Hentet fra https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf

Bekkevik, F. M., Holm, O. R., Vassilakopoulou, P. & Hustad, E. (2018). Information Security Practices in Organizations: A Literature Review on Challenges and Related Measures. *MCIS*.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly: Management Information Systems, 34*(SPEC. ISSUE 3), 523-548. Hentet fra https://www.jstor.org/stable/25750690?seq=1#metadata_info_tab_contents

Chang, S. E. & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management and Data Systems, 106*(3), 345-361. https://doi.org/10.1108/02635570610653498

Creswell, J. W. (2014). *A concise introduction to mixed methods research* Sage Publications.

Culnan, M., Foxman, E. & W. Ray, A. (2008). Why IT Executives Should Help Employees Secure Their Home Computers. *MIS Quarterly Executive, 7*. Hentet fra https://aisel.aisnet.org/misqe/vol7/iss1/6/

da Veiga, A. & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers and Security, 70*, 72-94. https://doi.org/10.1016/j.cose.2017.05.002

De nasjonale forskningsetiske komiteene. (2016b). Generelle forskningsetiske retningslinjer. Hentet 29.05.2019 2019 fra https://www.etikkom.no/forskningsetiske-retningslinjer/Generelle-forskningsetiske-retningslinjer/

Direktoratet for e-helse. (2018a). *Faktaark 9 - Opplæring av ledere og medarbeidere*. Hentet fra https://ehelse.no/normen/faktaark/faktaark-09-opplaering-av-ledere-og-medarbeidere

Direktoratet for e-helse. (2018b). *Faktaark 14 - Tilgangsstyring*. Hentet fra https://ehelse.no/normen/faktaark/faktaark-14-tilgangsstyring

Direktoratet for e-helse. (2018c). *Faktaark 31 - Passord og passordhåndtering*. Hentet fra https://ehelse.no/normen/faktaark/faktaark-31-passord-og-passordhandtering

Faxvaag, A., Johansen, T. S., Heimly, V., Melby, L. & Grimsmo, A. (2011). Healthcare professionals' experiences with EHR-system access control mechanisms. I *Studies in Health Technology and Informatics* (Vol. 169, s. 601-605). Hentet fra http://ebooks.iospress.nl/publication/14239

Ferreira, A., Antunes, L., Chadwick, D. & Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics, 79*(4), 268-283. https://doi.org/10.1016/j.ijmedinf.2010.01.009

Hou, Y., Gao, P. & Nicholson, B. (2018). Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital. *Technological Forecasting and Social Change, 126*, 64-75. https://doi.org/10.1016/j.techfore.2017.03.023

Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. Kristiansand: Høyskoleforlaget.

Justis- og beredskapsdepartementet. (2018). Lov om behandling av personopplysninger (personopplysningsloven). Hentet 29.05.2019 2019 fra https://lovdata.no/dokument/NL/lov/2018-06-15-38

Kisekka, V., Sharman, R., Rao, H. R., Upadhyaya, S. & Gerber, N. (2015). Investigating the antecedents of healthcare workers' perceptions of organizational resilience in hospitals. *2015 International Conference on Information Systems: Exploring the Information Frontier, ICIS 2015*. Hentet fra https://www.scopus.com/inward/record.uri?eid=2-s2.0-84964653248&partnerID=40&md5=48016865386f7ba944a8672e565ee2cd

Kvale, S., Brinkmann, S., Anderssen, T. M. & Rygge, J. (2009). *Det kvalitative forskningsintervju* (2. utg. utg.). Oslo: Gyldendal akademisk.

Kvale, S., Brinkmann, S., Anderssen, T. M. & Rygge, J. (2015). *Det kvalitative forskningsintervju* (3. utg., 2. oppl. utg.). Oslo: Gyldendal akademisk.

Luethi, M. & Knolmayer, G. F. (2009). Security in health information systems: An exploratory comparison of U.S. and Swiss Hospitals. *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*. https://doi.org/10.1109/HICSS.2009.381

Microsoft. (i.d.). Office 365 Education. Hentet 29.05.2019 2019 fra https://www.microsoft.com/nb-no/education/products/office/default.aspx

Nemati, H. R. & Church, M. (2009). A human centered framework for information security management: A healthcare perspective. *15th Americas Conference on Information Systems 2009, AMCIS 2009* (s. 4883-4890). Hentet fra https://aisel.aisnet.org/amcis2009/591/

Nieles, M., Dempsey, K. & Pillitteri, V. Y. (2017). *An Introduction to Information Security*. NIST. Hentet fra https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Norwegian National Security Authority. (2016, 06.06.2016). NSM Cryptographic Requirements. Hentet 03.06.2019 2019 fra https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/ncr3.1.pdf

NSD. (i.d.-a). Kontroll av anonymitet. Hentet 29.05.2019 2019 fra https://nsd.no/arkivering/kontroll_av_anonymitet.html

NSD. (i.d.-b). Personidentifiserende data. Hentet 29.05.2019 2019 fra https://nsd.no/arkivering/personidentifiserbare_data.html

Oates, B. J. (2006). *Researching Information Systems and Computing*. London: SAGE Publications Ltd.

Rahimli, A. & Masrom, M. (2015). *Overview of Data Security Issues in Hospital Information Systems*.

Ransbotham, S. & Mitra, S. (2009). Choice and chance: A conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139. https://doi.org/10.1287/isre.1080.0174

Straub, D. W. & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly, 22*(4), 441-469. https://doi.org/10.2307/249551

Susanto, H. & Almunawar, M. N. (2018). *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard* Apple Academic Press.

Sørlandet sykehuset HF. (i.d.). Våre organisasjonskart. Hentet 03.06.2019 2019 fra http://ek.sshf.no/docs/pub/dok02935.pdf

UiA. (i.d.-e). Tilgang til Office 365. Hentet 29.05.2019 2019 fra https://www.uia.no/student/office-365/tilgang-til-office-365

Universitetet i Sørøst-Norge. (2018). Last ned norske EndNote-stiler. Hentet 03.06.2019 2019 fra http://bibliotek.usn.no/last-ned-norske-endnote-stiler/category31450.html

Van Devender, M. S., Campbell, M., Glisson, W. B. & Finan, M. A. (2016). Identifying opportunities to compromise medical environments. *AMCIS 2016: Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems*. Hentet fra

https://www.scopus.com/inward/record.uri?eid=2-s2.0-84987643744&partnerID=40&md5=02dc25ad055f55f80913e99721469ae7

Venkatesh, V., A. Brown, S. & Bala, H. (2013). *Bridging the Qualitative-Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems*.

Whitman, M. E. & Mattord, H. J. (2018). *Principles of information security* (6th ed. utg.). Boston, Mass: CENGAGE Learning.

Wiercioch, A., Teufel, S. & Teufel, B. (2018). The Authentication Dilemma. *Journal of Software, 13*(5), 277-286. https://doi.org/10.17706/jsw.13.5.277-286

Zhang, W. & Creswell, J. (2013). The use of mixing procedure of mixed methods in health services research. *Medical Care, 51*(8), e51-e57. https://doi.org/10.1097/MLR.0b013e31824642fd

# 8. Vedlegg

## 8.1: Spørreskjema

Velkommen til denne spørreundersøkelsen!

Vi takker på forhånd for at du deltar i denne undersøkelsen og dermed bidrar til økt bevissthet rundt ansattes forhold til teknologiske arbeidsverktøy i SSHF.

**Hvor lenge har du vært ansatt ved intensiv enhet?**

(1) ❑ 0-3 år
(2) ❑ 4-8 år
(3) ❑ 9-14 år
(4) ❑ 15-20 år
(5) ❑ 21+ år

**Hvordan er ditt forhold til passordbytter?**

(2) ❑ 1 = Svært utilfreds
(3) ❑ 2
(4) ❑ 3
(5) ❑ 4
(6) ❑ 5
(7) ❑ 6 = Svært tilfreds
(8) ❑ Jeg har ikke vært med på passordbytte enda

**Har du noen tanker om ting som kan gjøres annerledes når det gjelder bytting av passord?**

_____
_____
_____

Vi vil nå stille deg noen spørsmål angående inn- og utlogging. Legg merke til at vi i denne sammenhengen skiller mellom datamaskin (PC) og system (DIPS).

**Hvor ofte logger du av PC manuelt når du forlater den?**

(1) ❑ 1 = Aldri
(2) ❑ 2 = En gang i måneden eller sjeldnere
(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Alltid

**Hvor ofte logger du av DIPS når du forlater PC?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Alltid

**Hvor ofte må du logge ut andre kolleger fra PC før egen bruk?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Alltid

**Hvor ofte må du logge ut andre kolleger fra DIPS før egen bruk?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Alltid

**Får du tilgang til pasientdata innen rimelig tid?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = For hver 10. pasient eller sjeldnere

(3) ❑ 3 = For hver 7.-9. pasient

(4) ❑ 4 = For hver 4.-6. pasient

(5) ❑ 5 = For hver 2.-3. pasient

(6) ❑ 6 = Alltid

**Hvorfor logger du aldri av PC?**

_____

_____

_____

**Kan du nevne spesifikke situasjoner hvor du ikke logger av PC?**

_____

_____

_____

**Hvordan opplever du tilgangen på PC-er ved arbeidsplassen?**

(1) ❑ 1 = Svært dårlig

(2) ❑ 2

(3) ❑ 3

(4) ❑ 4

(5) ❑ 5

(6) ❑ 6 = Svært bra

**Hvordan opplever du responstiden for PC-er ved arbeidsplassen?**

(1) ❑ 1 = Svært dårlig

(2) ❑ 2

(3) ❑ 3

(4) ❑ 4

(5) ❑ 5

(6) ❑ 6 = Svært bra

**Hvordan opplever du brukervennligheten til kjernesystemet DIPS?**

(2) ❑ 1 = Svært dårlig

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

(6) ❑ 5

(7) ❑ 6 = Svært bra

**Hvordan opplever du brukervennligheten til prosedyreoppslagsverket EK-Web?**

(2) ❑ 1 = Svært dårlig

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

(6) ❑ 5

(7) ❑ 6 = Svært bra

(8) ❑ Jeg bruker ikke EK-Web

**For behandling av pasient mener jeg elektronisk rapportering er...**

(2) ❑ 1 = Negativt

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

(6) ❑ 5

(7) ❑ 6 = Positivt

**For sikring av pasientdata mener jeg elektronisk rapportering er...**

(1) ❑ 1 = Negativt

(2) ❑ 2

(3) ❑ 3

(4) ❑ 4

(5) ❑ 5

(6) ❑ 6 = Positivt

**Har du noen forslag til hva som kan gjøres annerledes i DIPS?**

_____

_____

_____

**Har du noen forslag til hva som kan gjøres annerledes i EK-Web?**

_____

_____

_____

**Hvordan opplever du opplæringen innen informasjonssikkerhet?**

(2) ❑ 1 = Svært dårlig

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

(6) ❑ 5

(7) ❑ 6 = Svært bra

(8) ❑ Jeg har ikke fått noen opplæring

**Hvordan opplever du opplæringen innen bruk av systemer?**

(2) ❑ 1 = Svært dårlig

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

(6) ❑ 5

(7) ❑ 6 = Svært bra

(8) ❑ Jeg har ikke fått noen opplæring

**Hvor ofte må du føre data over fra papir til system og omvendt?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Flere ganger om dagen

**Hvor ofte må du føre data over fra et system til et annet?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Flere ganger om dagen

**Bruker du privat mobiltelefon i arbeidssammenheng?**

(1) ❑ 1 = Aldri

(2) ❑ 2 = En gang i måneden eller sjeldnere

(3) ❑ 3 = 2-4 ganger i måneden

(4) ❑ 4 = 2-4 ganger i uken

(5) ❑ 5 = Hver dag

(6) ❑ 6 = Flere ganger om dagen

**For arbeidet vårt mener jeg bruk av privat mobiltelefon er...**

(2) ❑ 1 = Negativt

(3) ❑ 2

(4) ❑ 3

(5) ❑ 4

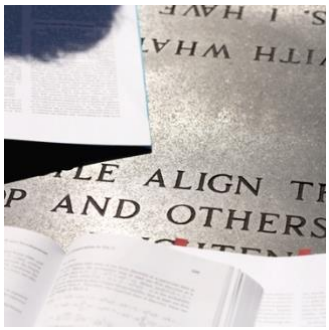
(6) ❑ 5

(7) ❑ 6 = Positivt

Takk for at du deltok i vår undersøkelse!

Eventuelle spørsmål kan sendes på mail: jorgeb13@student.uia.no / rickyo13@student.uia.no

Mvh
Jørgen Bjørnstad & Ricky Omland
Masterstudenter innen informasjonssystemer v/UiA



## 8.2: Liste over artikler med journaler

| # | Forfatter | Tittel | Pub. | Journal / Konferanse |
|---|---|---|---|---|
| 1. | Hou et al. | Understanding organisational responses to regulative pressures in information security management: The case of a Chinese hospital | 2017 | **?** (Technological Forecasting & Social Change, January 2018, Vol.126, pp.64-75) |
| 2. | Bekkevik et al. | Information Security Practices in Organizations: A Literature Review on Challenges and Related Measures | 2017 | **MCIS** (The 12th Mediterranean Conference on Information Systems) |
| 3. | McLaughlin et al. | Challenges and Best Practices in Information Security Management | 2018 | **MISQE** (MIS Quarterly Executive) |
| 4. | Tu & Yuan | Critical Success Factors Analysis on Effective Information Security Management. Information Systems Security, Assurance, and Privacy Track | 2014 | **AMCIS** (Twentieth Americas Conference on Information Systems, Savannah, 2014) |
| 5. | Faxvaag et al. | Healthcare Professionals' Experiences With EHR-System Access Control Mechanisms | 2011 | **EFMIS** (European Federation for Medical Informatics, 2011) |
| 6. | Smaradottir | Security Management in Health Care Information Systems: A literature review | 2018 | N/A |
| 7. | Anderson et al. | Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information | 2017 | **MIS** (Journal of Management Information Systems, 34(4), 1082–1112) |
| 8. | Huson & Hewitt | Would Increased Regulation Reduce the Number of Information Breaches? | 2016 | **HICSS** (49th Hawaii International Conference on System Sciences) |
| 9. | Hedström et al. | Value conflicts for information security management | 2011 | **JSIS** (The Journal of Strategic Information Systems, 20(4), 373–384) |
| 10. | Hassan et al. | Information security culture in health informatics environment: A qualitative approach | 2017 | **ICRIIS** (International Conference on Research and Innovation in Information Systems) |
| 11. | Stahl et al. | Information security policies in the UK healthcare sector: A critical evaluation | 2012 | **ISJ** (Information Systems Journal 22(1), 77–94) |
| 12. | Ferreira et al. | Grounding information security in healthcare | 2010 | **IJMI** (International Journal of Medical Informatics, 79(4), 268–283) |
| 13. | Luethi et al. | Security in health information systems: An exploratory comparison of U.S. and Swiss Hospitals | 2009 | **HICSS** (Proceedings of the 42nd Annual Hawaii International Conference on System Sciences) |
| 14. | Sunyaev et al. | Characteristics of IS security approaches with respect to healthcare | 2009 | **AMCIS** (15th Americas Conference on Information Systems, 2009) |
| 15. | Van Devender et al. | Identifying opportunities to compromise medical environments | 2016 | **AMCIS** (Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems, 2016) |
| 16. | Nemati et al. | A Human Centered Framework for Information Security Management: A Healthcare Perspective | 2009 | **AMCIS** (15th Americas Conference on Information |

| | | | | |
|---|---|---|---|---|
| | | | | Systems, 2009) |
| 17. | Sedlack | Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting | 2016 | **AMCIS** (Surfing the IT Innovation Wave - 22nd Americas Conference on Information Systems, 2016) |
| 18. | Kisekka et al. | Investigating the Antecedents of Healthcare Workers' Perceptions of Organizational Resilience in Hospitals | 2015 | **ICIS** (International Conference on Information Systems: Exploring the Information Frontier, 2015) |
| 19. | Martin et al. | Information security and insider threats in small medical practices | 2014 | **AMCIS** (20th Americas Conference on Information Systems) |
| 20. | Elmrabit et al. | Insider threats in information security categories and approaches | 2015 | **ICAC** (21st International Conference on Automation and Computing, 2015) |

## 8.3: Intervjuguide i TEH

# Intervjuguide – *"ISM og klinisk arbeidsflyt i helsesektoren"*

For datainnsamlingen vår ønsker vi å utføre semi-strukturerte dybdeintervjuer. Målet vårt med intervjuguiden er å samle store deler av informasjonen på respondentens/informantens eget initiativ. Dette vil vi gjøre gjennom å lede intervjupersonen gjennom kategoriserte temaer som er relevant i forhold til det vi ønsker å undersøke. For å påse at gjennomførelsen av intervjuet genererer den informasjonen vi er ute etter, har vi satt opp noen strukturerende spørsmål som vi vil ta opp ved behov.

**1. Bakgrunn** *(Type tjeneste, avdeling, rolle…)*:

**Introduksjon**:

*1.1 I hvilken tjeneste/avdeling er du ansatt?*

*1.2 Hvor lenge har du vært ansatt?*

*1.3 Hvilken rolle har du i organisasjonen?*

**2. Teknisk sikkerhetspraksis**

*2.1 Hvor mange systemer brukes av ansatte ved SSHF (Spesifikt kliniske avd.)?*

*2.1.1 Kan du gi noen eksempler på systemer ved SSHF? (Formål, bruksområde...)*

*2.1.2 Hvordan er systemene knyttet sammen? (Arkitektur)*

*2.1.3 Bruker avdelingene felles plattform?*

*2.2 Hvordan håndterer SSHF adgangskontrollmekanismer (tilgangsstyring – innlogging)?*

*2.2.1 Krav til passord?*

*2.2.2 Har systemene automatisk utlogging etter bestemt tid? (Timeouts)*

*2.2.3 Tror du det utvikles «workarounds» blant ansatte? (e.g. gule lapper med passord)*

**3. Formell sikkerhetspraksis**

*3.1 Har du noen kjennskap til retningslinjene for informasjonssikkerhet som dere må følge?*

*3.2 Hvilke rutiner må ansatte forholde seg til iht. informasjonssikkerhet?*

*3.3 Hvordan håndterer organisasjonen ansattes kunnskap om sikker bruk av systemene?*

*3.3.1 Føler du det settes av nok tid og ressurser til kursing og opplæring?*

*3.4 Har du noen tanker om ting som kan gjøres annerledes?*

**4. Uformell sikkerhetspraksis**

*4.1 Hva er ditt inntrykk av ansattes holdninger til endring?*

*4.1.1 Tror du holdningene kan være basert på kultur?*

*4.2 Hvordan opplever du at prosessrutiner blir håndtert av de ansatte i organisasjonen?*

*4.2.1 Tror du det tidvis kan oppstå dobbeltarbeid som følger av rutinene?*

*4.2.2 Tror du det kan utvikles «workarounds» for andre prosessrutiner enn innlogging?*

**5. Avslutning**

*5.1 Mulighet for å ta kontakt igjen senere for å få klarhet i noen av spørsmålene?*

# Intervjuguide – *"ISM og klinisk arbeidsflyt i helsesektoren"*

For datainnsamlingen vår ønsker vi å utføre semi-strukturerte dybdeintervjuer. Målet vårt med intervjuguiden er å samle store deler av informasjonen på respondentens/informantens eget initiativ. Dette vil vi gjøre gjennom å lede intervjupersonen gjennom kategoriserte temaer som er relevant i forhold til det vi ønsker å undersøke. For å påse at gjennomførelsen av intervjuet genererer den informasjonen vi er ute etter, har vi satt opp noen strukturerende spørsmål som vi vil ta opp ved behov.

**1. Bakgrunn** *(Type tjeneste, avdeling, rolle…)*:

**Introduksjon**:

*1.1 I hvilken tjeneste/avdeling er du ansatt?*

*1.2 Hvor lenge har du vært ansatt?*

*1.3 Hvilken rolle har du i organisasjonen?*

**2. Teknisk sikkerhetspraksis**

*2.1 Kan du ta oss gjennom en vanlig arbeidsdag?*

*2.2 Hvor mange systemer bruker du gjennom en vanlig arbeidsdag?*

*2.2.1 Kan du gi noen eksempler på systemer du bruker?*

*2.2.2 Bruker dere mobile enheter i jobbsammenheng?*

*2.2.3 Hvordan opplever du å bruke systemene?*

*2.2.2 Hvor mange ganger må du logge inn og ut av systemer og PC/Utstyr gjennom dagen?*

*2.2.2.1 I typisk hvilke situasjoner må dette gjøres?*

*2.3 Hvordan forholder du deg til passord?*

**3. Formell sikkerhetspraksis**

*3.1 Har du noen kjennskap til retningslinjene for informasjonssikkerhet som dere må følge?*

*3.2 Hvilke rutiner må du som ansatt forholde deg til iht. informasjonssikkerhet?*

*3.2.1 Føler du at du har tilstrekkelig kunnskap om sikker bruk?*

*3.2.2 Føler du det settes av nok tid og ressurser til kursing og opplæring? (Bruk av verktøy og systemer, sikkerhet...)*

**4. Uformell sikkerhetspraksis.**

*4.1 Hvordan er din holdning til endring? (eks. System byttes ut)*

*4.1.1 Hvordan opplever du at endringer blir håndtert av organisasjonen?*

*4.2 Hvordan opplever du IT- og sikkerhetskulturen blant ansatte?*

*4.2.2 Opplever du at det oppstår dobbeltarbeid?*

**5. Avslutning**

*5.1 Har du noen tanker om ting som kan gjøres annerledes?*

*5.2 Mulighet for å ta kontakt igjen senere for å få klarhet i noen av spørsmålene?*

# Vil du delta i forskningsprosjektet

## *"ISM og klinisk arbeidsflyt i helsesektoren"*?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å komme med forslag til innovasjon og effektivisering av arbeidsflyten i norsk helsesektor. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

### Formål

Vårt mål i utredelsen er å – gjennom utforskende/eksplorative intervjuer – gjøre funn på spesifikke aspekter innenfor informasjonssikkerhet som kan påvirke klinikernes flyt i arbeidsprosesser (arbeidsflyt).

Problemstillingen vår er som tittelen: ***"ISM og klinisk arbeidsflyt i helsesektoren"***. På bakgrunn av problemstillingen har vi konstruert følgende forskningsspørsmål: ***"Hvilke aspekter ved ISM kan påvirke klinisk arbeidsflyt?"***.

Studien gjennomføres i forbindelse med vår masterutredning, våren 2019.

**Hvem er ansvarlig for forskningsprosjektet?**

Universitetet i Agder / Institutt for informasjonssystemer er ansvarlig for prosjektet.

**Hvorfor får du spørsmål om å delta?**

Vi ønsker deltakere som sitter på ulike erfaringer og bakgrunner, som resultat av at de besitter ulike roller i populasjonen, som i denne sammenhengen er Sørlandet Sykehus HF (SSHF). Spesifikt ønsker vi å strukturere utvalget i tre rollebaserte grupperinger:

1. Klinikere – sykepleier, helsefagarbeider, o.l.
2. Leder – informasjonssikkerhet, informasjonsteknologi
3. Mellomleder – typisk avdelingsleder

### Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du deltar i et personlig intervju. Det vil ta deg ca. 45 minutter. Intervjuguiden inneholder hovedsakelig spørsmål om prosessrutiner i organisasjonen, deres kultur og retningslinjer, samt helseinformasjonssystemers funksjonalitet. Svarene du oppgir under intervjuet blir tatt opp gjennom lyd i tillegg til notater underveis.

Tatt i betraktning at intervjuene vi ønsker å gjennomføre vil være semi-strukturerte, vil vi bruke samme intervjuguide for intervjuene i hver av grupperingene som ble nevnt under forrige punkt.

**Det er frivillig å delta**
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

**Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Våre to veiledere ved instituttet (nevnt i andre punkt) vil ha tilgang til opplysningene vi innhenter fra deg.
- Datamaterialet vil lagres i en mappe gjennom tjenesten Office 365 som kun vi har tilgang til. Tjenesten leveres gjennom universitetets egen infrastruktur, og vi er derfor trygge på at dataene er lagret på en sikker måte. I tillegg vil vi påse at ingen sensitiv data kan kobles til navn eller kontaktinformasjon, ved at vi holder denne informasjonen adskilt fra det innsamlede datamaterialet.

Det kan tenkes at en person som har god kjennskap til organisasjonen og de ansatte vil kunne gjenkjenne deg som deltaker i vår publikasjon, på bakgrunn av at vi ønsker å inkludere en presentasjon av respondentenes ulike roller, erfaringer og bakgrunner.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes i juni 2019. Ved prosjektets avslutning vil vi påse at all data blir anonymisert og lydopptak fjernes permanent fra disken.

**Dine rettigheter**
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

**Hva gir oss rett til å behandle personopplysninger om deg?**
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Agder / Institutt for informasjonssystemer har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

**Hvor kan jeg finne ut mer?**
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
- Universitetet i Agder / Institutt for informasjonssystemer ved student Jørgen Bjørnstad, på epost (jorgeb13@uia.no) eller telefon: 466 77 806. Evt. prosjektansvarlig/veileder Devendra B. Thapa, på epost (devinder.thapa@uia.no) eller telefon: 38 14 14 19.

- Universitetets personvernombud: Ina Danielsen, på epost (personvernombud@uia.no) eller telefon: 45 25 44 01.
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 55 58 21 17.

Med vennlig hilsen

Devendra B. Thapa
(Forsker/veileder)

Jørgen Bjørnstad / Ricky L. Omland
(Student)

---

## Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet ***"ISM og klinisk arbeidsflyt i helsesektoren"***, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i personlig intervju
- ☐ at opplysninger om meg publiseres slik at jeg kan gjenkjennes (ved at funnene fra intervjuet kobles til min rolle, bakgrunn og mine erfaringer i organisasjonen)

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. midten av juni 2019.

---

(Signert av prosjektdeltaker, dato)

## 8.6: Informasjonsskriv for kvantitativ datainnsamling

# Vil du delta i forskningsprosjektet

## *"ISM og klinisk arbeidsflyt i helsesektoren"*?

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å komme med forslag til innovasjon og effektivisering av arbeidsflyten i norsk helsesektor. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

### Formål

Vårt mål i utredelsen er å – gjennom spørreskjema – undersøke i hvilken grad aspekter innenfor informasjonssikkerhet kan påvirke klinikernes flyt i arbeidsprosesser (arbeidsflyt).

Problemstillingen vår er som tittelen: ***"ISM og klinisk arbeidsflyt i helsesektoren"***. På bakgrunn av problemstillingen har vi konstruert følgende forskningsspørsmål: ***"I hvilken grad kan aspekter ved ISM påvirke klinisk arbeidsflyt?"***.

Studien gjennomføres i forbindelse med vår masterutredning, våren 2019.

**Hvem er ansvarlig for forskningsprosjektet?**

Universitetet i Agder / Institutt for informasjonssystemer er ansvarlig for prosjektet.

**Hvorfor får du spørsmål om å delta?**

Vi ønsker deltakere som sitter på ulike erfaringer og bakgrunner, som resultat av at de besitter ulike roller i populasjonen, som i denne sammenhengen er Sørlandet Sykehus HF (SSHF). Spesifikt ønsker vi å strukturere utvalget i tre rollebaserte grupperinger:

1. Klinikere – sykepleier, lege, o.l.
2. Leder – informasjonssikkerhet, informasjonsteknologi, seksjon/avdeling

### Hva innebærer det for deg å delta?

Hvis du velger å delta i prosjektet, innebærer det at du deltar i en spørreundersøkelse. Det vil ta deg ca. 4-6 minutter, noe avhengig av hvor mye du legger i svarene. Spørreskjemaet inneholder hovedsakelig spørsmål om program- og maskinvare, inn- og utlogging, samt noe om opplæring, doble føringer og bruk av mobiltelefon som arbeidsredskap. Dine svar fra spørreskjemaet registreres elektronisk.

Vi vil bruke samme spørreskjema for samtlige respondenter der deltakeren får mulighet til å definere sin fartstid i organisasjonen.

**Det er frivillig å delta**
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykke tilbake uten å oppgi noen grunn. Alle opplysninger om deg vil da bli anonymisert. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

**Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger**
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- En foreløpig ukjent veileder ved instituttet (nevnt i andre punkt) vil ha tilgang til opplysningene vi innhenter fra deg.
- Datamaterialet vil lagres i en mappe gjennom tjenesten Office 365 som kun vi har tilgang til. Tjenesten leveres gjennom universitetets egen infrastruktur, og vi er derfor trygge på at dataene er lagret på en sikker måte. I tillegg vil vi påse at ingen sensitiv data kan kobles til navn eller kontaktinformasjon, ved at vi holder denne informasjonen adskilt fra det innsamlede datamaterialet.

Det kan tenkes at en person som har god kjennskap til organisasjonen og de ansatte vil kunne gjenkjenne deg som deltaker i vår publikasjon, på bakgrunn av at vi ønsker å inkludere en presentasjon av respondentenes ulike roller, erfaringer og bakgrunner.

**Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?**

Prosjektet skal etter planen avsluttes i juni 2019. Ved prosjektets avslutning vil vi påse at all data blir anonymisert og spørreskjema med resultater fjernes fra plattformen vi bruker som verktøy for gjennomføringen av undersøkelsen.

**Dine rettigheter**
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- innsyn i hvilke personopplysninger som er registrert om deg,
- å få rettet personopplysninger om deg,
- få slettet personopplysninger om deg,
- få utlevert en kopi av dine personopplysninger (dataportabilitet), og
- å sende klage til personvernombudet eller Datatilsynet om behandlingen av dine personopplysninger.

**Hva gir oss rett til å behandle personopplysninger om deg?**
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Universitetet i Agder / Institutt for informasjonssystemer har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

**Hvor kan jeg finne ut mer?**
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

- Universitetet i Agder / Institutt for informasjonssystemer ved student Jørgen Bjørnstad, på epost (jorgeb13@uia.no) eller telefon: 466 77 806. Evt. prosjektansvarlig/veileder Devendra B. Thapa, på epost (devinder.thapa@uia.no) eller telefon: 3814 1419.
- Vårt personvernombud: Ina Danielsen, på epost (personvernombud@uia.no) eller telefon: 45 25 44 01.
- NSD – Norsk senter for forskningsdata AS, på epost (personverntjenester@nsd.no) eller telefon: 5558 2117.

Med vennlig hilsen

Prosjektansvarlig (Forsker/veileder) Jørgen Bjørnstad / Ricky L. Omland

---

## Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet ***"ISM og klinisk arbeidsflyt i helsesektoren"***, og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i spørreundersøkelsen
- ☐ at opplysninger om meg publiseres slik at jeg kan gjenkjennes (ved at funnene fra undersøkelsen kobles til min rolle, bakgrunn og mine erfaringer i organisasjonen)

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet, ca. midten av juni 2019.

---

(Signert av prosjektdeltaker, dato)