UNIVERSITETET I AGDER

Tilgangsstyring av elektronisk pasientjournal

En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

Rune Hystad

Veileder
Rune Fensli

Masteroppgaven er gjennomført som ledd i utdanningen ved Universitetet i Agder og er godkjent som del av denne utdanningen. Denne godkjenningen innebærer ikke at universitetet innestår for de metoder som er anvendt og de konklusjoner som er trukket.

Universitetet i Agder, 2014
Fakultet for helse- og idrettsfag
Institutt for helse- og sykepleievitenskap

Tilgangsstyring av elektronisk pasientjournal

En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

MASTEROPPGAVE I HELSE- OG SOSIALINFORMATIKK

Universitetet i Agder, 2014

Fakultet for helse- og idrettsvitenskap

Institutt for helse- og sykepleievitenskap

Antall ord: 17848

Sammendrag

I helsetjenesten er tilgang til sensitive opplysninger om pasienter en nødvendighet for å kunne yte helsehjelp til pasienten, og ivareta pasientsikkerheten. Samtidig må opplysningene beskyttes mot urettmessig tilegnelse, for å ivareta pasientens personvern. I elektronisk pasientjournal (EPJ) er tilgangsstyring en essensiell funksjonalitet for å ivareta både pasientsikkerhet og personvern ved at autoriserte personer får tilgang til informasjon knyttet til pasientbehandlingen. Behandlingsprosesser er imidlertid ofte uforutsigbare, og pasientbehandling skjer på tvers av organisasjonsenheter i virksomheten de er ansatt i. Som en følge av dette er det vanskelig å sette opp strenge regler for tilgangsstyring, og unntaksmekanismer må benyttes.

I spesialisthelsetjenesten benyttes i hovedsak rollebasert tilgangsstyring (RBAC), og det har siden 2001 vært formulert krav om at tilgang til opplysninger i EPJ skal gis på bakgrunn av beslutninger om helsehjelp, såkalt beslutningsstyrt tilgang. Innføring av beslutningsstyrt tilgang vil innen få år være gjennomført i samtlige helseforetak. Litteratursøk viser en rekke utfordringer med tilgangsstyring i EPJ, men empiri over erfaringer med bruk og oppsett av beslutningsstyrt tilgang, er nærmest ikkeeksisterende.

Formålet med denne oppgaven har derfor vært å kartlegge hva sluttbrukere og systemforvaltere erfarer som de viktigste utfordringene ved bruk av beslutningsstyrt tilgang, og hva de anser som viktige faktorer for forbedring av tilgangsstyringen. For å få svar på dette er det utført en Delphiundersøkelse, og det er tatt ut rapporter fra en EPJ-database. Funnene viser at en rekke av utfordringene avdekket i tidligere studier fremdeles er til stede. Tilgangsstyring er i for liten grad tilpasset behandlingsprosesser, og utstrakt bruk av unntaksmekanismer er nødvendig for å ivareta pasientsikkerheten, som så genererer lange hendelsesregistre som ikke blir fulgt systematisk opp, og derfor går kan gå på bekostning av pasientenes personvern. Mulige forbedringer av utfordringene som er avdekket går blant annet på mer opplæring, standardisering av tilgangsstyring, enklere bruk av unntaksmekanismer og en mer prosessorientert tilgangsstyring.

Nøkkelord

Tilgangsstyring, Tilgangskontroll, Delphi, Elektronisk pasientjournal, Informasjonssikkerhet, Spesialisthelsetjeneste, Pasientsikkerhet

Abstract

In health care, access to sensitive information about patients is a necessity in order to offer care to the patient, and maintain patient safety. At the same time it is important that the information is protected against unauthorized access, to ensure patient privacy. Access control is an essential function in electronic health records (EHR) to maintain the duality between patient safety and patient privacy by ensuring that authorized personnel are allowed access to information they need. However, care processes are often unpredictable, and a number of end users can be involved in treatment across organizational units in the same health enterprise. As a consequence, it is hard to implement strict access control rules, and exception mechanisms must be used.

In the specialist care, role based access control (RBAC) is mainly used as access control model, and it has since 2001 been a requirement in Norway that access control in EHR must be given on the basis of decisions about health care, so called decision based access. Within few years, this will be used in all Norwegian health enterprises. Literature shows a number of challenges with access control in EHR, but empirical data on experiences with the use and setup of decision based access, is almost nonexistent.

The purpose of this study was therefore to identify what the end users and system administrators are experiencing as the most important challenges using decision based access, and what they consider important factors for the improvement of the access control. To answer this, a Delphi survey was conducted, and it is taken out reports from an EHR database. The survey and reports show that a number of challenges that have been identified in previous studies are still present. The access control is not sufficiently tailored to treatment processes, and extensive use of exception mechanisms is necessary to protect patient safety, which generates long event records that are not followed up systematically, and therefore may go at the expense of patient privacy. Possible improvements of the challenges uncovered include more education, standardization of access control, easier use of exception mechanisms and a more process oriented access control.

Keywords

Access Control, Delphi, Electronic Health Records, Information security, Patient safety

Forord

Å skrive denne masteroppgaven har på mange måter vært en ensom affære. Oppgaven hadde imidlertid ikke blitt ferdig om ikke en rekke mennesker både i og utenfor mine omgivelser hadde støttet meg på ulike måter. Jeg har hatt kontakt med, og fått hjelp av mange mennesker i løpet av prosessen, som har gitt meg både inspirasjon og ny kunnskap. Tusen takk skal dere ha, alle sammen!

Først vil jeg takke min veileder Rune Fensli for hans konstruktive og konkrete tilbakemeldinger gjennom dette året.

Elisabeth Holen-Rabbersvik skal ha takk for deling av sine erfaringer med utførelsen av en Delphistudie, og takk til Henry Langseth for god hjelp med oppsett av spørreskjema i SurveyXact.

Takk til Øystein Nytrø og Per Håkon Meland for nyttig innsikt i prosjektet iAccess, som to av doktorgradene det henvises til i oppgaven har vært del av.

Trond Elde, Løsningsarkitekt og FoU-koordinator i DIPS ASA skal ha takk for hans behjelpelighet angående informasjon rundt beslutningsstyrt tilgang i DIPS.
Leif Rune Rørvik, regional tjenesteansvarlig for DIPS i Sykehuspartner, og Kirsti Jangaard Loe, prosjektleder for Regional standardisering klinisk dokumentasjon (RSKD) i Helse Sør-Øst, skal ha takk for nyttige innspill i den initiale fasen med valg av problemområde.

Torbjørn Nystadnes, forfatter av EPJ-standarden, skal ha takk for essensielle avklaringer rundt begrepet beslutningsstyrt tilgang og dens bruk i standarden.

Sørlandet Sykehus Helseforetak skal ha en stor takk for tillatelser til gjennomføring av undersøkelsen, og behjelpelighet med uttrekk fra DIPS-databasen.

Sist men ikke minst må jeg takke min kone, sønn og mine svigerforeldre for raushet i tålmodighet og omtenksomhet gjennom de siste tre år, uten dere hadde jeg fremdeles vært en stakkars ungkar.

Rune Hystad
Grimstad, mai 2014

Innhold

FIGURLISTE

TABELLISTE

1.0 INNLEDNING

Tilgangsstyring er en viktig funksjon i helsevesenets elektroniske pasientjournalsystemer, og handler om å håndheve lover og regler for å sikre at bare autoriserte brukere får tilgang til taushetsbelagt informasjon. I helsevesenet betyr dette å beskytte pasientens personvern, samtidig som pasientsikkerheten ivaretas. Dette krever på sin side at helsepersonell har tilgang til den informasjonen de trenger for å kunne gjøre de mest informerte beslutningene om omsorg og behandling av pasienten (Røstad, 2009). Behandlingsprosesser kan imidlertid være uforutsigbare, og gjør det vanskelig å implementere gode regler for tilgangsstyring, som i tilstrekkelig grad ivaretar både personvern ved å minimere muligheten for urettmessig tilegnelse av taushetsbelagte opplysninger (snoking), og pasientsikkerhet.

Det finnes mange modeller for tilgangsstyring, men det er publisert lite forskning angående helsetjenestens krav til tilgangsstyring. Litteratursøk viser at de fleste modellene for tilgangsstyring i helsevesenet, er studier eller prototyper hvor helsepersonell ikke har deltatt i utviklingen av hverken retningslinjer, modeller eller mekanismer for tilgangsstyring (Ferreira, Cruz-Correia, Antunes og Chadwick, 2007).

Beslutningsstyrt tilgang, som er en videreutvikling av tradisjonell rollebasert tilgangsstyring, er i bruk i store deler av spesialisthelsetjenestens EPJ-systemer, da det på bakgrunn av lovverk konkretisert gjennom EPJ-standarden (Nystadnes, 2007), og Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren (Normen) (Helsedirektoratet, 2013) er pålagt å benytte dette. I løpet av få år vil beslutningsstyrt tilgang sannsynligvis være innført i alle regionale helseforetak med hvert sitt sett med standardiserte prinsipper for tilgangsstyring. Det eksisterer imidlertid lite empiri rundt denne modellen blant de som til daglig jobber med den; sluttbrukerne og systemforvalterne.

Denne oppgaven har søkt å kartlegge hva sluttbrukere og systemforvaltere anser som viktige utfordringene og mulige forbedringer av tilgangsstyringen, gjennom en Delphistudie og data fra EPJ-databasen ved sluttbrukernes helseforetak.

Forfatter har bakgrunn som både helsepersonell og systemforvalter, og har deltatt i implementering av beslutningsstyrt tilgang ved flere helseforetak, og ble derfor inspirert til å skrive denne masteroppgaven.

1.1 Oppgavens oppbygging

I neste kapittel vil tilgangsstyring i helsetjenesten bli nærmere beskrevet. Det vil bli presentert hvorfor tilgangsstyring kan være et problem, hva som påvirker tilgangsstyring, hvilke konsekvenser det kan ha, hvem det angår, og hva som foreligger av relevant forskning på området. Gjennomgangen fører frem til presentasjon av problemformuleringen med tilhørende forskningsspørsmål. Den teoretiske modellen som benyttes til å belyse funnene i oppgaven blir presentert til slutt.

Tredje kapittel redegjør for valg av metode, utvalg, gjennomføring av undersøkelsen, og analyse, metodekritikk, etiske overveielser og kildekritikk.

I fjerde kapittel oppsummeres funnene fra Delphiundersøkelsen, og uttrekk fra EPJ-databasen.

Kapittel fem inneholder diskusjonen av funnene, som leder til konklusjonen i kapittel seks.

2.0 TEORETISK FORANKRING

Kapitlet gir en oversikt over sentrale begreper innen tilgangsstyring i helsetjenesten som har betydning for denne oppgaven. Hvordan tilgangsstyring er implementert i DIPS EPJ fra leverandøren DIPS ASA (Distribuert Informasjons og Pasientdatasystem i Sykehus) utdypes da det er dette journalsystemet funnene i oppgaven baseres på. I tillegg beskrives InfoSec-modellen som skal gi en forståelse av informasjonssikkerhet og dets innhold relatert til tilgangsstyring. Til slutt i dette kapitlet presenteres problemformuleringen med tilhørende forskningsspørsmål, og avgrensninger.

2.1 Tilgangsstyring/Tilgangskontroll

Termene tilgangsstyring og tilgangskontroll er begge innarbeidede fellesbetegnelser for metoder, teknologiske prinsipper og verktøy for kontroll av tilgang til opplysninger. Formålet med tilgangsstyring er å i samspill med andre elementer sørge for å ivareta virksomheters informasjonssikkerhet, og består ifølge Andresen (2010) av fire hovedaktiviteter:

- Administrasjon (Rutiner og praktisk arbeid med behandling av brukeres handlingsmuligheter)
- Autentisering (Mekanismene som sørger for at brukere kan individuelt identifiseres)
- Autorisasjon (De fullmaktene en bruker har, og de tekniske mekanismene som sørger for samsvar mellom brukerens fullmakter og handlingsmuligheter i IT-systemer)
- Revisjon (Retrospektiv kontroll av brukeres autorisasjon)

Innenfor helsetjenesten skal tilgangsstyring sikre at helsepersonell har tilgang til tilgjengelig informasjon som er nødvendig for å gi pasienter en forsvarlig helsehjelp, samtidig som det er en forutsetning at informasjonen bare gjøres tilgjengelig innenfor rammene av lovbestemt taushetsplikt, for å beskytte pasientenes personvern (Helsedirektoratet, 2010).

EPJ-systemer kan defineres som sikkerhetskritiske systemer, sammen med f.eks. signalanlegg til jernbane, kontrollsystem for kjernefysiske anlegg, flytrafikk og banksystemer. Tilgangsstyring er en viktig funksjon i alle disse systemene, men EPJ-system avviker fra de andre i et viktig aspekt. I de fleste sikkerhetskritiske systemer er standardregelen for tilgangsstyring «ved tvil, nekt tilgang», men i helsetjenesten vil det alltid være «ved tvil, tillat tilgang» (Røstad, 2009). Beskyttelse av pasientens personvern er viktig, men det later til å

være enighet i litteraturen om at ved vekting av personvern og pasientsikkerhet, veier pasientsikkerhet tyngst (Andresen, 2010; Røstad, 2009; Åhlfeldt, 2008).

Samtidig som pasientsikkerheten ivaretas, må man så godt det praktisk lar seg gjøre, ha mekanismer som ivaretar personvernet, da brudd på pasienters personvern kan resultere i tapt tillit og frykt for at opplysninger skal bli misbrukt (Økland, Haumann og Christiansen, 2011). Frykt og mangel på tillit kan føre til at pasienter holder tilbake informasjon relevant for behandling som resulterer i økt fare for feilbehandling. Datatilsynet (2008) presenterte i 2008 en undersøkelse som viser i hvor stor grad nordmenn har tillit til at ansatte i blant annet sykehus, ikke ser på personopplysninger uten saklig grunn. Ved hjelp av en fempunkts Likert-skala, svarte 17 % av respondenten at de har «ingen tillit» til at sykehusansatte ikke ser på personopplysninger uten saklig grunn.

Mangelen på tillit kan se ut til å være berettiget. Det er sparsomt med litteratur som omhandler omfang av urettmessig tilegnelse av taushetbelagte opplysninger fra EPJ-system, men det som foreligger viser at dette forekommer. Andresen og Aasland (2008) utførte en spørreskjemaundersøkelse blant 395 leger, helsesekretærer og radiografer, hvor ett av spørsmålene gikk ut på om respondenten selv har lest opplysninger om pasienter av nysgjerrighet eller av andre grunner som respondenten selv ikke anser som faglig eller etisk aktverdige. Totalt 17,6 % av respondentene oppgav at de hadde lest i pasientjournaler uten faglig begrunnelse minst én gang. I Sverige ble det ved et universitetssykehus gjort en kvalitativ studie hvor 40 av 41 intervjuobjekter oppgav at kolleger urettmessig tilegnet seg taushetsbelagt informasjon (Wester, 2007). I en undersøkelse utført av tre masterstudenter deltok 264 helsepersonell ved Oslo Universitetssykehus, og 13,6 % av respondentene svarte at de hadde lest taushetsbelagte opplysninger om pasienter uten faglig grunn (Økland et al., 2011).

Det på mange måter motstridende hensyn til både pasientsikkerhet og personvern er hva som gjør tilgangsstyring i helsetjenesten så utfordrende. I tillegg er behandlingsprosesser ofte uforutsigbare, og gjør det dermed vanskelig å ha strenge regler for tilgangsstyring (Røstad, 2009). Dette har ført til at relativt «åpne» eller «vide» tilganger har blitt gitt ved sykehus i blant annet Norge (Helsetilsynet, 2008), Sverige (Wester, 2009) og Finland (European Court of Human Rights, 2008). Når det gjelder Norge, så forekommer det samtidig også at helsepersonell ikke får tilgang til alle pasienter de har et reelt behov for, da tilgangsstyringen er for statisk og i liten grad er knyttet til pasientenes dynamiske behandlingsforløp (Røstad,

2009; Andresen, 2010). Dette vises i Andresen og Aasland (2008) sin undersøkelse, der 26,5 % av respondentene (n=395) oppgir at de blir forhindret fra å gjøre oppgaver pga. manglende tilgang. Forfatterne skriver at de bare har tall for hvor mange som har opplevd så stramme tilganger at det er et reelt hinder i arbeidet, og at spørsmål direkte til helsepersonell ikke gir svar på om de også har unødvendig vide tilganger. Studien til (Økland et al., 2011) søker imidlertid å gi svar på dette, og i deres undersøkelse svarte 51,9 % av respondentene (n=264) at de er litt eller helt enig i at de har tilgang til taushetsbelagte opplysninger om pasienter de ikke har pleie, behandlings- eller administrativt ansvar for, og 14,9 % svarte eksplisitt at de var helt eller litt enig i at de hadde for vide tilganger.

En annen studie gjennomførte spørreskjemaundersøkelser blant helsepersonell for blant annet å undersøke hvordan tilgangsstyring påvirket bruk av EPJ. Respondentene var helsepersonell ved sykehus (n=206) og sykehjem (n=239). Forfatterne fant at helsepersonell utsatte dokumentering, og endret atferd i forhold til lesing av andres dokumentasjon som følge av tilgangsstyringen. Blant respondentene som var ansatt ved sykehus, svarte 37 % at arbeid ble utsatt, og 25 % svarte at pasientens journal ikke ble undersøkt før de skulle yte omsorg for pasientene. Studien gir imidlertid ingen forklaring på hva som er årsaken til disse funnene, annet enn at pålogging tar for mye tid ifølge helsepersonell, og derfor kan være én faktor (Faxvaag, Johansen, Heily, Melby og Grimsmo 2011, s. 605). Det er ikke gjort usabilitytesting av EPJ-systemene i denne studien så langt forfatterne kjenner til. Det er heller ikke beskrevet hvem som er leverandør av EPJ-et på sykehuset, og hvordan tilgangsstyringen er satt opp.

Utfordringer med tilgangsstyring kan ha sin årsak i en rekke faktorer, og Helsetilsynet (2008) har på bakgrunn av tilsyn sammen med Datatilsynet, ved Helse Bergen HF, pekt på seks bakenforliggende årsaker til manglende tilgangsstyring:

- Kunnskaper – Manglende kunnskaper om hva taushetsplikten etter helselovgivningen innebærer.
- Holdninger og respekt – Tilgangsstyringen er hovedsakelig innrettet etter helsepersonells behov for informasjon, og ikke pasienters behov for diskresjon. «Vide» tilganger gis for å unngå å benytte unntaksmekanismer og ingen tidsbegrensning gis etter endt pasientkontakt.

- Teknokratene styrer – Tilgangsstyring innrettes etter hva som datateknisk er lettvint, og hva ledere og rådgivere uten klinisk erfaring anser som viktig. Brukere og linjeledere har liten innflytelse.
- Leverandører – EPJ-system er i for liten grad utviklet i henhold til lovkrav for ivaretakelse av taushetsplikt.
- Lav risiko for å bli avslørt og straffet for snoking – Et høyt antall journaloppslag sammen med manglende teknologi for å avdekke snoking gir lav risiko for å oppdage urettmessig tilegnelse av taushetsbelagte opplysninger, i tillegg til utilstrekkelig preventiv effekt.
- Risikovurdering – Mangelfulle risikovurderinger av helseforetakene fører til manglende oversikt over systemenes sårbarhet.

Tiltak for å bedre dette er ifølge Helsetilsynet å forbedre kunnskapen om, og respekten for taushetsplikten. I tillegg må helseforetakene stille større krav til EPJ-leverandørene om videreutvikling av tilgangsstyring, og helseforetakene må så selv sørge for å sette opp tilgangsstyringen slik at behandlernes behov for tilgjengelighet, og pasientenes behov for personvern balanseres på en bedre måte (Helsetilsynet, 2008). Denne oppfatningen deles også av Datatilsynet (2009) som avdekket avvik ved tilgangsstyringen hos samtlige helseforetak de hadde tilsyn med i perioden 2005 – 2009.

En rekke helseforetak ser ut til å ha imøtegått noe av kritikken fra Helsetilsynet og Datatilsynet ved blant annet å bygge på funksjonalitet for beslutningsstyrt tilgang i eksisterende tilgangskontroll, slik at tilgang til opplysninger i journaler i større grad gis på bakgrunn av beslutninger om helsehjelp til pasienten, og ikke bare organisatorisk tilhørighet. Noe oppfølging, nye tilsyn eller annen litteratur som kan si noe om effekten av tiltakene ble ikke avdekket gjennom litteratursøk. Etter kontakt med Datatilsynet fikk imidlertid forfatter som svar:

> «Vi har en hypotese om at det fortsatt gjenstår mye hva gjelder tilgangsstyring i helsesektoren. Vi har imidlertid ingen data om dette. Datatilsynet skal gjennomføre tilsyn med tilgangsstyringen i helsesektoren i løpet av våren»[1].

[1] (M. E. Pellerud, rådgiver i Datatilsynet, personlig kommunikasjon, 31. mars, 2014).

Når man skal utforme systemer for tilgangsstyring bør man starte med definering av strukturerte og formelle retningslinjer for tilgangsstyringen, og så velge en passende modell. En virksomhets retningslinjer for tilgangsstyring må beskrive reglene som skal håndheves for å tilfredsstille kravene til informasjonssikkerhet i organisasjonen. Deretter må det velges en passende modell for tilgangsstyring for å kunne modellere reglene som er definert i retningslinjene (Ferreira et al. (2007).

Det finnes en rekke modeller for tilgangsstyring, der den mest utbredte ser ut til å være rollebasert tilgangsstyring, eller Role-Based Access Control på engelsk (RBAC), da en eller annen form for RBAC er implementert i de fleste EPJ-system i dag (Alemán, Señor, Lozoya og Toval, 2013; Ferreira et al., 2007; Røstad, 2009). RBAC ble introdusert i 1992, og den sentrale idéen med denne modellen for tilgangsstyring er at brukere ikke gis direkte tilgang til objekter, men roller i applikasjonen. Det er i selve rollene det gis, eller fjernes tilganger (Ferraiolo og Kuhn, 1992).
Et problem med tidligere RBAC modeller som brukes i helsevesenet er deres statiske natur, som ikke fanger opp de dynamiske behovene til helsepersonell (Røstad, 2009).

Beslutningsstyrt tilgang har sitt opphav i den første versjonen av EPJ-standarden som ble publisert i 2001 (KITH, 2001). Det er en videreutvikling av, eller påbygning på den tradisjonelle rollebaserte tilgangsstyringen (Nystadnes, 2007), og er i større grad forløpsbasert, hvilket innebærer at muligheten for tilgang oppstår og forsvinner igjen når opplysninger om behandlingsforløpet tilsier at behovet er der (Andresen, 2010). Beslutningsstyrt tilgang går ut på at tilgang knyttes til beslutninger som gjelder behandling av pasienten, og ikke utelukkende organisasjonstilhørighet. I utgangspunktet treffes det en rekke ulike typer beslutninger innen et behandlingsforløp, for eksempel en henvisning eller et behov for å avlegge en bestemt prøve, som åpner tilgangen for de som skal utføre det som beslutningen gjelder. Beslutningene som berettiger tilgang treffes av den aktuelle behandler når situasjonen tilsier det, og behandleren får tilgang til pasientens journal enten automatisk, eller ved å manuelt oppgi årsak for journalinnsynet (Andresen, 2010). Av den grunn kan beslutningsstyrt tilgang sies å være en skjønnbasert tilgangsstyring da den ikke reguleres fullstendig fra virksomhetens side (Andresen, 2010).

Beslutningsstyrt tilgang er i dag i bruk i store deler av helsetjenestens EPJ-system i Norge. P.t. benytter hele Helse-Vest beslutningsstyrt tilgang (DIPS, 2011), Helse-Nord skal gjennom

FIKS-prosjektet sørge for at det blir innført innen 2016 (Helse Nord, 2014) og i Helse Sør-Øst har man et lignende prosjekt kalt Digital Fornying der alle helseforetak i løpet av 2016 skal ha innført EPJ fra DIPS, og beslutningsstyrt tilgang (Helse Sør-Øst, 2014). Helse Midt-Norge benytter p.t. EPJ fra Siemens (DocuLive) som ikke har beslutningsstyrt tilgang, men ifølge IT-sjef for Helse Midt-Norge er de i en prosess med å skifte ut EPJ-systemet, og i det nye journalsystemet vil kravet om beslutningsstyrt tilgang gjelde.[2]

Litteratursøk på modeller for tilgangsstyring viser at forskningen tenderer mot en teoretisk tilnærming da det finnes et høyt antall vitenskapelige artikler som presenterer ulike modeller for tilgangsstyring. Selv om mange av dem bruker helsetjenesten og EPJ som eksempel, er det få som baseres på empiriske studier som understøtter den valgte modellen, eller forklarer i detalj hvorfor modellene er egnet for helsetjenesten. Dette samsvarer med litteratursøk omtalt i andre studier (Røstad, 2009; Faxvaag et al. 2011).

I perioden 2005-2009 foregikk det imidlertid et forskningsprosjekt ved navn iAccess, som var et samarbeid mellom Universitetet i Oslo, Norges teknisk-naturvitenskapelige universitet, og Sintef. Prosjektet var finansiert av Norges Forskningsråd og omhandlet kontroll med tilgang til og bruk av helseopplysninger om pasienter (Norges teknisk-naturvitenskapelige universitet, 2014). Prosjektet hadde flere delprosjekter, blant annet én doktorgrad rettet mot tekniske muligheter og problemstillinger (Røstad, 2009), og én doktorgrad rettet mot juridiske muligheter og problemstillinger (Andresen, 2010).

I sin doktorgradsavhandling beskriver Andresen (2010) tretten prinsipper for hvordan tilgang kan reguleres, slik at helsepersonell får tilgang til de opplysninger de trenger i sitt arbeid i og på tvers av virksomheter. Beslutningsstyrt tilgang er ett av prinsippene som skårer jevnt høyt på vurderingskriteriene, men det konkluderes ikke med en klar «vinner» da hvert av prinsippene har sterke og svake sider ifølge Andresen. Da doktorgraden ble levert var beslutningsstyrt tilgang bare delvis i drift i mindre skala i enkelte virksomheter (Andresen, 2010), og ingen av disse var gjenstand for undersøkelser.

I sin doktorgradsavhandling presenterer Røstad (2009) et av hovedfunnene som at tilgangsstyring i fremtiden bør skreddersys mer opp mot behandlingsforløp, slik at man får

[2] (A. Pedersen, IT-sjef Helse Midt-Norge, personlig kommunikasjon, 1. april, 2014).

tilgang på bakgrunn av behandling, og ikke utelukkende organisasjonstilhørighet. Beslutningsstyrt tilgang søker å ivareta dette, men Røstad ser i større grad for seg tilgang gjennom predefinerte behandlingsforløp.

Ved Sørlandet sykehus Helseforetak ble beslutningsstyrt tilgang innført i 2012. Sluttrapporten for innføringen viser at det eksisterer avvik fra både helseforetaket og det regionale helseforetakets prinsipper for tilgangsstyring[3]. Årsakene til dette oppgis å være utfordringer med funksjonalitet i DIPS EPJ som gjør at tilgangsstyring ikke kan tilpasses behandlingsprosesser for alle sluttbrukerne, i tillegg til tilbakemelding fra sluttbrukere om at utstrakt bruk av unntaksmekanismer oppfattes som tungvint. Dette har ført til at videre tilganger enn initialt ønskelig er gitt, for å ivareta pasientsikkerheten og sluttbrukeres ønske om mindre bruk av unntaksmekanismer.
Situasjonen er dermed den at beslutningsstyrt tilgang innen få år vil være innført ved alle landets helseforetak, men empiri angående denne modellens suksess i forhold til ivaretakelse av pasientsikkerhet og personvern eksisterer praktisk talt ikke.

2.2 EPJ-standarden for tilgangsstyring

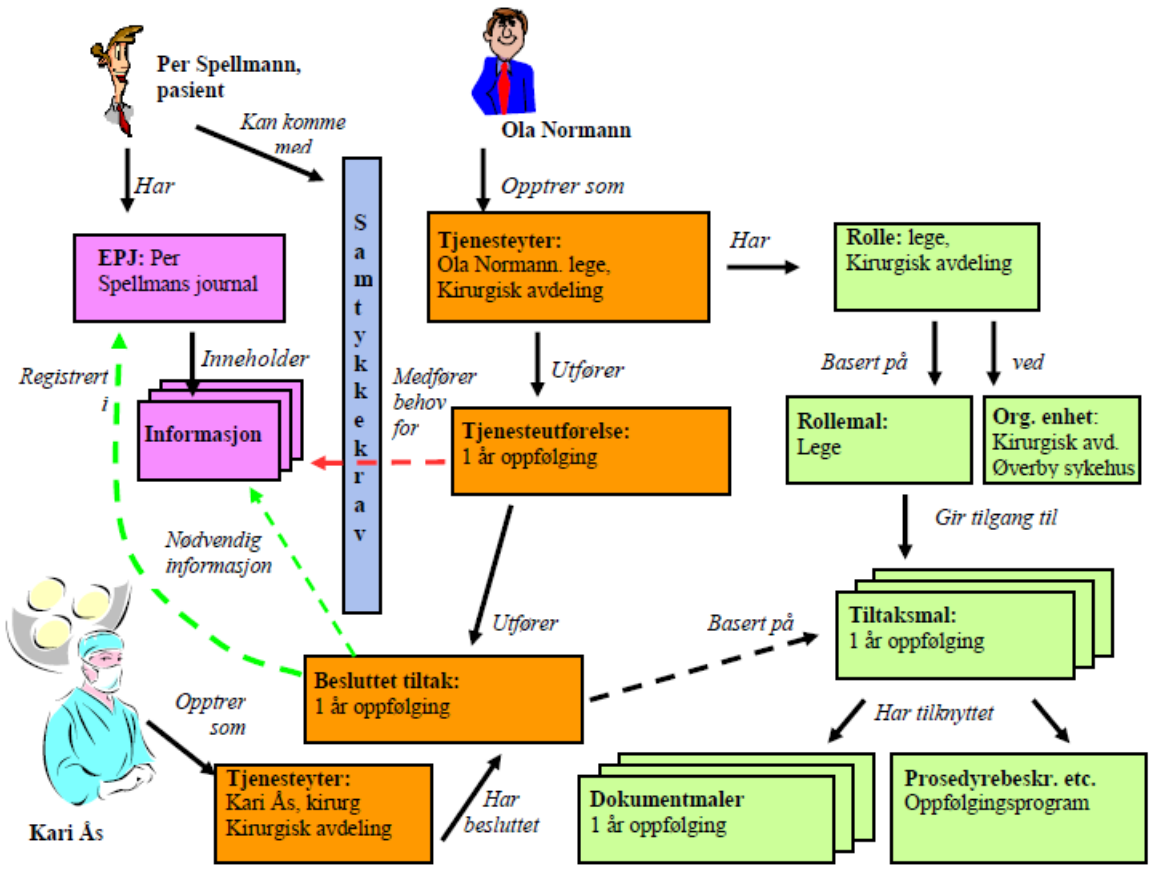
Det har i en årrekke eksistert internasjonale standarder for elektroniske pasientjournaler, men ifølge Helse- og omsorgsdepartementet var det behov for en nasjonal standard (NOU, 2006:5, 2006). På bakgrunn av dette startet Kompetansesenter for IT i helsevesenet (KITH AS, som nå er overført til Helsedirektoratet) på midten av 1990-tallet med et nasjonalt standardiseringsarbeid som resulterte i den første EPJ standarden, som ble publisert i 2001. EPJ standarden har siden da gjennomgått revideringer, blant annet da erfaring har vist at standarden har vært «vanskelig tilgjengelig for de fleste» (Nystadnes, 2007, s. 9), og er for tiden under revisjon på grunn av en rekke lov- og forskriftsendringer siden forrige utgave ble publisert (Helsedirektoratet, 2014).

Standarden har som mål å danne en felles plattform for alle leverandører av EPJ-system til det norske helsevesenet, og inneholder krav som skal bidra til å sikre at tilgangsstyring i EPJ skjer

[3] (N. D. Halseide, IKT-rådgiver og prosjektleder for innføring av beslutningsstyrt tilgang ved Sørlandet sykehus HF, personlig kommunikasjon, 18. desember 2013).

i henhold til gjeldende lovverk (KITH, 2010). EPJ standarden består av seks deler. Andre del av standarden omhandler blant annet arkitektur for tilgangsstyring i EPJ-systemer og definerer tekniske og generelle funksjonelle krav til innhold i tillegg til prinsipp for beslutningsstyrt tilgangskontroll (Nystadnes, 2007).

Beslutningsstyrt tilgang beskrives i detalj i standarden. Det er verdt å merke seg at kapitlet om tilgang og utlevering i del 2 av EPJ-standarden ikke bare heter «Tilgang og utlevering», men har fått innlemmet begrepet beslutningsstyrt, og derfor heter «Beslutningsstyrt tilgang og utlevering». Dette kan sees i sammenheng med at en målsetning er at autorisering for tilgang til journalopplysninger skal knyttes til beslutninger om helsehjelp som medfører behov for opplysninger. EPJ-standarden er også tydelig på at tilgangsstyringen skal sikre at helsepersonell med legitimt behov får tilgang til nødvendige helseopplysninger, men blir nektet tilgang til andre helseopplysninger. Det må ifølge EPJ-standarden være etablert en konkret relasjon mellom tjenesteyter og pasient for at det skal kunne gis tilgang til opplysninger i journalen (Nystadnes, 2007). Et eksempel som illustrerer sentrale deler av beslutningsstyrt tilgang, slik de beskrives i EPJ-standarden, er vist i figur 1.



Figur 1 Eksempel på beslutningsstyrt tilgang (Nystadnes, 2007)

Per Spellmann gjennomgikk i fjor en operasjon ved Øverby sykehus og det finnes derfor en journal (EPJ: Per Spellmanns journal) inneholdende dokumentasjon av denne operasjonen og eventuell annen helsehjelp Per Spellmann har mottatt fra sykehuset. Kirurgen som hadde ansvar for operasjonen, Kari Ås, besluttet at Per Spellemann skulle innkalles til kontroll et år etter operasjonen og registrerte derfor et *Besluttet tiltak* om oppfølging etter et år. Registreringen ble basert på *Tiltaksmalen* "1 år oppfølging" og til denne var det også tilknyttet en *Prosedyrebeskrivelse* for det aktuelle oppfølgingsprogram, samt relevante *dokumentmaler*. Ved registrering av det besluttete tiltaket ble det også angitt hvilken informasjon som kirurgen anså som nødvendig for å kunne gjennomføre oppfølgingstiltaket. Når Per Spellmann etter innkalling møter opp et år etter operasjonen, er det Ola Normann som skal gjennomføre den oppfølging som Kari Ås besluttet året før. Ola Normann er lege og når han er på jobb, opptrer han som *Tjenesteyter* i *Rollen* lege ved kirurgisk avdeling, en *Organisatorisk enhet* ved Øverby sykehus. *Rollen* er basert på en *Rollemal* for Lege som gir tilgang til et sett av *Tiltaksmaler* som dekker de oppgaver en lege ved

kirurgisk avdeling skal kunne utføre. Når Ola skal forberede seg til oppfølgingen av Per Spellmann, benytter han seg av de rettighetene som følger av tiltaket "1 års oppfølging" som kirurgen registrerte i journalen et år tidligere. Han åpner Per Spellmanns journal, og angir at han skal utføre tjenester relatert til "1 års oppfølging". Det registreres dermed (automatisk) en *Tjenesteutførelse* som dokumenterer at han har hatt tilgang til journalen i forbindelse med gjennomføring av dette tiltaket. Dersom ikke Per Spellmann har kommet med spesielle restriksjoner når det gjelder bruk av journalinformasjonen, vil Ola få tilgang til den informasjon han har behov for. Har derimot Per Spellmann krevd at tilgang til (deler av) informasjonen i journalen kun skal gis etter eksplisitt samtykke, må slik samtykke innhentes og registreres først. EPJ-systemet skal i så fall gi Ola Normann beskjed om at han må kontakte journalansvarlig som da må vurdere det konkrete behovet for opplysninger i det aktuelle tilfellet og om nødvendig kontakte pasienten slik at samtykke kan innhentes (Nystadnes, 2007, s. 28-29).

EPJ-standarden sier altså at tilgang må innebefatte et behandlerforhold til pasienten, men den sier derimot ikke noe om at tilgangsstyringen skal være rollebasert (Strømmen, 2013). Dette kan forklares med at et utsagn om krav til rollebasert tilgangskontroll, lett kunne blitt feiltolket ettersom en tradisjonell rollebasert tilgangskontroll ikke er tilstrekkelig for å oppfylle de krav som følger av bestemmelser i lov[4].

2.3 Unntaksmekanismer

Den generelle modellen for tilgangsstyring er som tidligere nevnt basert på rollebasert tilgangsstyring, sentrert rundt enheter (brukere, pasienter, organisasjonsenheter), mens i realiteten er arbeidet i helsetjenesten prosessorientert og dynamisk av natur. Behandlingsprosesser er ofte uforutsigbare, og det kan være vanskelig ha strenge regler for tilgangsstyring. Som et resultat av dette, må brukere i nødstilfeller og andre uventede situasjoner kunne overstyre tilgangsstyringen ved hjelp av unntaksmekanismer (Alemán et al. 2013; Andresen, 2010; Røstad, 2009).

[4] (T. Nystadnes, seniorrådgiver i Helsedirektoratet og forfatter av EPJ-standarden, personlig kommunikasjon, 3. april, 2014).

Det er i hovedsak to unntaksmekanismer for tilgang i EPJ-system i spesialisthelsetjenesten; aktualisering, og nødrettstilgang. Disse kan ha ulike navn avhengig av leverandør, og i DIPS kalles disse henholdsvis grønnlys- og blålystilgang som er beskrevet i kapittel 2.5.
Nødrettstilgang betegner en straffrihetsgrunn, slik at man i prinsippet ikke kan straffes for en forbudt handling, hvis den etter omstendighetene er nødvendig (Andresen, 2010). Ifølge EPJ-standarden bør behovet for å benytte en slik tilgang være svært lite og begrenset til reelle nødstilfeller. Nødrettstilgang er for øvrig også beskrevet i Normen, og ifølge den skal hvert enkelttilfelle hvor en slik tilgang benyttes, følges opp som et avvik (Helsedirektoratet, 2013).

For å minimere misbruk av nødrettstilgang er det laget noen ekstra sikkerhetstiltak, og tiltakene kan variere noe fra ett system til et annet, men de mest vanlige innebærer at bruker må oppgi grunn for bruk av nødrettstilgang, må skrive inn sitt passord, ikke får tilgang til hele journalen, men må gjenta nødrettstilgangen for å få tilgang til ulike deler av journalen, og tidsbegrensning av tilgang til journal ved bruk av nødrettstilgang (Røstad, 2009).

Noen EPJ inneholder andre unntaksmekanismer for å kunne håndtere ulike situasjoner hvor behovet for tilgang er reelt, men det ikke er snakk noen nødssituasjoner. Disse unntaksmekanismene minner mye om nødrettstilgang/blålystilgang. Hovedforskjellen er at mens blålysfunksjonen kun er ment for å brukes i nødstilfeller, er den «generelle» unntaksmekanismen konstruert for å håndtere all tilgang som er lovlig og normal fra en brukers synspunkt, men som tilgangsstyringen ikke har vært i stand til å håndtere (Røstad, 2009). I DIPS er grønnlysfunksjonen/eksplisitt tilgang en slik generell unntaksmekanisme.

Dette eksemplet illustrerer hva som ofte skjer med pasienter: de blir først gitt en diagnose, som kan endre seg flere ganger før det virkelige problemet er identifisert. Etter hvert som diagnose, tester og behandling endres, overføres de frem og tilbake, og blir ofte bedt om å gjengi sin sykehistorie og behandling så langt. Mekanismene for å overstyre tilgangsstyringen brukes ofte for å håndtere vanlige, gjentakende hendelser, som ikke er tillatt som følge av tilgangsstyringen, og man velger årsak fra en liste over tilgjengelige grunner (Røstad, 2009).

Man bør allikevel ha som målsetning å minimere behovet for unntaksmekanismer. Sett fra et informasjonssikkerhetsperspektiv er unntaksmekanismer en dårlig løsning da det resulterer i tap av kontroll over informasjonsflyten. Eventuelle nødvendige unntak bør behandles som del av den normale tilgangsstyringen, for å ha størst mulig kontroll. Det er nok ikke mulig å ikke

ha noen unntak i det hele tatt, men en mer egnet modell for tilgangsstyring kan redusere behovet for unntak (Røstad, 2009).

Grimsmo (2007) påpeker også at unntaksmekanismer blir brukt i større utstrekning enn tiltenkt. En undersøkelse i et prosjekt om aktualisering ved Rikshospitalet viser at aktualisering utgjorde ca. 15 % av alle åpnede (leste eller skrevne) dokumenter ved Rikshospitalet, og 1/3 del av de som aktualiserer oftest, gjør ikke et bevisst valg av årsaksalternativ (Engum, 2008). I samme prosjekt ble det utfør intervjuer av 17 helsepersonell som aktualiserte «mye». Resultatet viser at ca. 50/50 mener at aktualisering er «irriterende», eller «dette blir man vant til».

En studie utført av Røstad (2009) har analysert bruk av aktualisering og nødrettstilgang ved åtte sykehus i Helse Midt-Norge som benyttet Siemens DocuLive sitt EPJ. Resultatene viste at i løpet av én mnd. ble aktualisering benyttet 54096 ganger, som er 17 % av totalt antall journalinnsyn). Nødrettstilgang ble derimot kun benyttet 67 ganger, 0,07 % av totalt antall journalinnsyn. Ut i fra denne studien benyttes aktualisering så hyppig at det knapt kan kalles en unntaksmekanisme. Når man ser dette i sammenheng med at de som aktualiserer oftest ikke gjør et bevisst valg av årsaksalternativ (Engum, 2008), og at det ofte oppgis uklare fritekstbegrunnelser (Andresen, 2010) er det betimelig å stille spørsmål om dette er en ønskelig situasjon.

Å gi tilgang til å kunne overstyre tilgangsstyringen innebærer som tidligere nevnt at man har en funksjonalitet i et system som kan misbrukes, og for å minimere sikkerhetsrisikoen loggføres bruk av unntaksmekanismer slik at man kan utføre retrospektive kontroller, altså en gjennomgang av hvilke brukere som har vært inne på hvilke pasienters journal osv. (Røstad, 2009).

2.4 Hendelsesregister/logger

Hendelsesregister er i Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren definert som registrering av hendelser i et informasjonssystem, med det formål å forebygge, avdekke og hindre gjentagelse av sikkerhetsbrudd (Helsedirektoratet, 2013). Den alminnelige samlebetegnelsen for hendelsesregistre er imidlertid «logger» (Andresen, 2010).

Krav om bruk av hendelsesregistre kan man utlede av personopplysningsforskriften § 2-11 der det står at det skal treffes tiltak mot uautorisert innsyn i personopplysninger der konfidensialitet er nødvendig, og i § 2-8 står det uttrykkelig at autorisert bruk av informasjonssystemet skal registreres (Personopplysningsforskriften, 2000). I tillegg forutsetter helseregisterloven § 13 at pasienter har rett til innsyn i logg for hvem som har hatt tilgang til helseopplysninger om ham eller henne (Helseregisterloven, 2001).

EPJ-systemer generer flere typer logger, blant annet tidligere nevnt logg for bruk av unntaksmekanismer som nødrettstilgang og aktualisering (Andresen, 2010). EPJ-standarden stiller også krav til at det skal finnes kontrollrapporter som skal kunne avsløre om noen har åpnet en journal ved å opprette et fiktivt besluttet tiltak/aktualisering, eller nødrettstilgang (Nystadnes, 2007).

Hendelsesregistre benyttes derfor i hovedsak til etterkontroll av tilganger, men kan også forebygge urettmessig tilegnelse av taushetsbelagte opplysninger, da brukerne vet at oppslag, endring eller sletting i en journal blir loggført og kan spores til brukeren som har utført handlingen (Økland et al. 2011). Selvsensuren har som oftest ønsket effekt, men kan også ha utilsiktede virkninger. I tidligere nevnte studie utført av Andresen og Aasland (2008) oppgir 5,1 prosent av respondentene at de minst én gang har latt være å lese opplysninger de burde ha lest, fordi handlingen kan spores i hendelsesregistre. I studiene til Økland et al. (2011) sa totalt 14,7 % av respondentene seg litt eller helt enig i at tanken på at det blir ført logg har stoppet dem i å lese taushetsbelagte opplysninger som de faglig sett burde ha lest.

Ifølge Datatilsynet (2008) argumenterer virksomheter for at hendelsesregistre gir tilstrekkelig personvern, slik at man kan ha en «vid» tilgangsstyring, da det vil være for omfattende å kartlegge hva sluttbrukere trenger tilgang til. Å gjennomgå hendelsesregistre kan imidlertid være meget tid- og ressurskrevende, slik at det i hovedsak gjøres ved stikkprøver, etter forespørsel fra pasienter (Datatilsynet, 2009), eller kontroll av profilerte personer (Innomed, 2012).

I oktober i 2010 ble det gjort over én million oppslag i journalsystemet på Rikshospitalet. Å manuelt sjekke hvert eneste oppslag er derfor ikke gjennomførbart da det ville blitt altfor tidkrevende. Helseforetakene er derfor avhengig av å ha holdepunkter for å velge ut oppslag

som skal sjekkes. Dette gjøres ofte ved å bare kontrollere logger for bruk av aktualisering og nødrettstilgang (Datatilsynet, 2009; Rogstad, 2011). Selv om bare disse loggene undersøkes, så virker oppgaven fremdeles uhåndterlig, da undersøkelser viser at aktualisering har stått for 14-17 % av totalt antall journaloppslag (Engum, 2008; Røstad, 2009).

2.4.1 Mønstergjenkjenning

Ifølge Normen skal hendelsesregistrene enkelt kunne analyseres ved hjelp av analyseverktøy, for å kontrollere tilgangsstyring, og oppdage brudd på tilgang til helse- og personopplysninger (Helsedirektoratet, 2013). Hva som er enkelt, og hvilke krav det er til analyseverktøyet er imidlertid ikke nærmere beskrevet i Normen.

Mønstergjengkjenningsprogrammer er en type analyseverktøy som er designet for å lettere kunne kontrollere hendelsesregistre (Røstad, 2009). Kort fortalt går mønstergjenkjenning ut på å automatisere prosessen med å avdekke urettmessige oppslag i pasientjournaler, ved å analysere store mengder data, lete etter mønstre, og rapportere funn som defineres som mistenkelige oppslag i pasientjournaler (Rogstad, 2011). Urettmessige oppslag mistenkes når det oppdages avvik fra vanlig bruk, som er representert av bruksmønstrene (Røstad, 2009). Mønstergjenkjenningsprogram har blitt pilotert, men er imidlertid ikke i bruk i produksjon i EPJ-system i Norge (Økland et al. 2011).

Pilotstudier har vært utført i Ullevål sykehus og Helse Nordmøre og Romsdal HF (Innomed, u. å), og på bakgrunn av disse pilotstudiene ble enda en pilotstudie utført ved OUS, Ullevål og Rikshospitalet, som ble avsluttet i 2012.

Sluttrapporten for prosjektet konkluderer med at stikkprøver av hendelsesregister ikke er en tilstrekkelig metode for reell kontroll av urettmessig tilegnelse av taushetsbelagte opplysninger, grunnet det enorme antall oppslag som gjøres hver dag ved sykehuset. Rutinen ved OUS er at kontroll av oppslag i hovedsak gjøres på profilerte personer og pasienter som har bedt om innsynslogg. I forprosjektet ble det utarbeidet 17 scenarioer med avvikende oppslagsmønstre som kan indikere urettmessig tilegnelse av informasjon, og åtte av scenarioene ble testet. På bakgrunn av scenarioene ble hvert journaloppslag gitt en score, der høy score indikerer avvik fra normalt oppslagsmønster. Ca. 7,3 millioner journaloppslag ble

analysert, og av disse fikk 150 en spesielt høy score, og av disse ble 29 håndtert videre i linjen av klinikklederne (Innomed, 2012).

Mønstergjenkjenningsprogrammet som ble benyttet i disse pilotene var ikke utviklet av EPJ-leverandøren, men levert av firmaet SAS (Innomed, 2012). Implementering av et slikt verktøy vil selvsagt medføre kostnader, og på generelt grunnlag vil kostnader ved å innføre dette bestå av en rekke komponenter:[5]

- Arbeidsmøter med kunden for å fastlegge en mønsterinstruks
- Utarbeide krav for tilgang til pasient-, ansatt- og loggdata (journaloppslagene)
- Fysisk tilrettelegging av tilgang til utvalgte produksjonsdata
- Programvare for mønstergjenkjenning
- Kjøpe tjenester av en driftsorganisasjon for kjøring av systemet
- Kompetanseoppbygging og løpende ajourhold av deteksjonssystem og målsetninger

Styringsgruppen i Nasjonal IKT vedtok 5. juni 2013 å starte tiltaket 'Etablering av nasjonal standard for statistisk analyse av logger fra oppslag i behandlingsrettede helseregistre' på bakgrunn av pilotstudien ved OUS. Målet er å etablere en nasjonal metode og rammeverk for gjennomgang av logger fra behandlingsrettede helseregistre basert på statistisk analyse og mønstergjenkjenning (Nasjonal IKT, 2013).

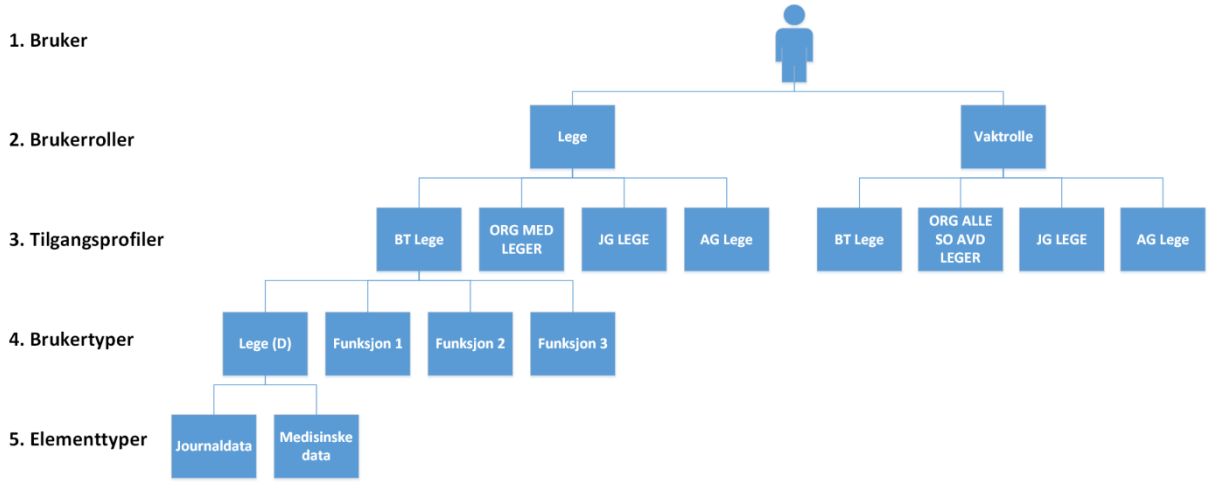
2.5 Tilgangsstyring i DIPS

DIPS ASA er Norges største leverandør av EPJ for spesialisthelsetjenesten i Norge (Ellingsen og Monteiro, 2012), og deres løsning for EPJ brukes av Helse Sør-Øst RHF, Helse Vest RHF og Helse Nord RHF i tillegg til flere private sykehus. Respondentene i denne oppgavens studie benytter, eller skal til å benytte DIPS, og av den grunn utdypes deres modell for tilgangsstyring i dette underkapitlet.

DIPS har funksjonalitet for både tradisjonell rollebasert tilgangsstyring, og beslutningsstyrt tilgang slik andre del av EPJ-standarden definerer. Tradisjonell og beslutningsstyrt tilgang er i hovedsak bygget opp på samme måte, men det som omtales i denne oppgaven gjelder

[5] (I. Krogstad, seniorrådgiver i Health Care SAS Institute Nordic, personlig kommunikasjon, 26. mars, 2014)

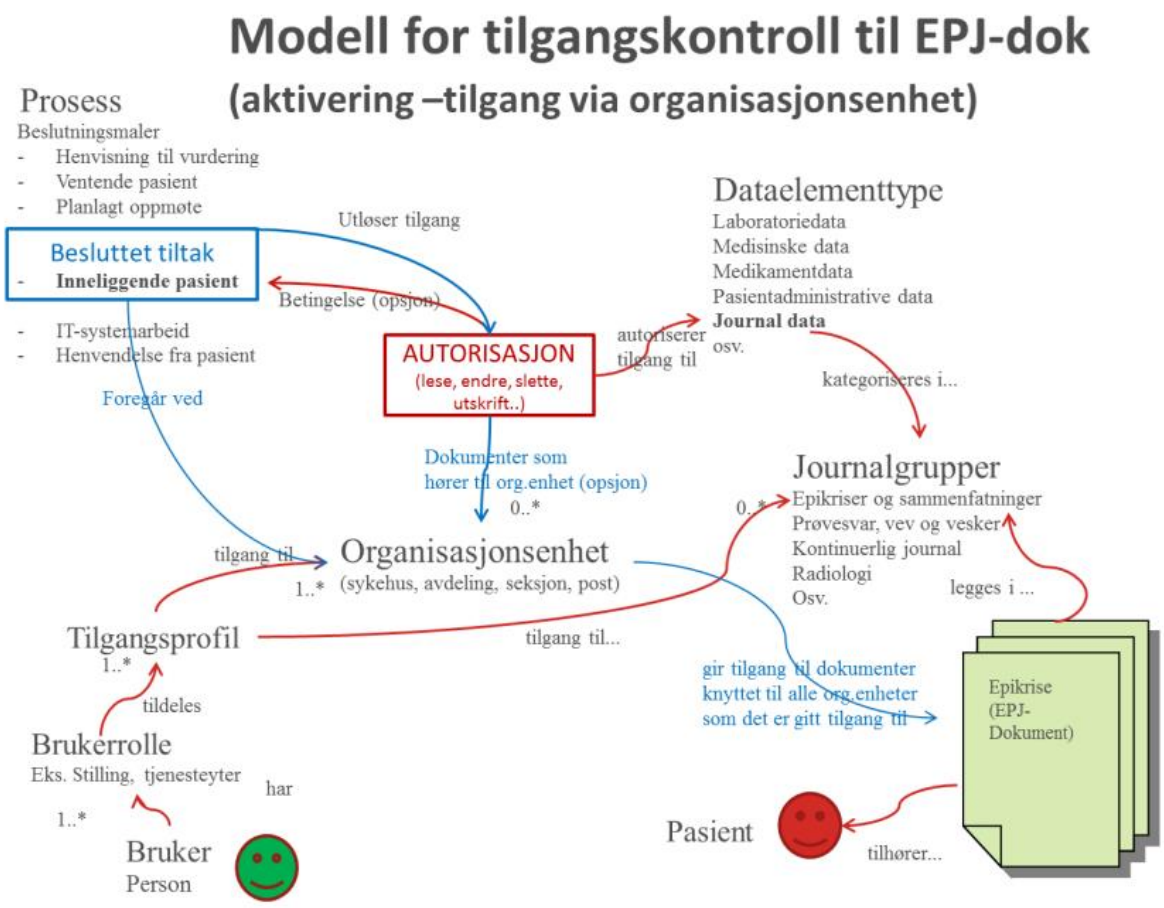
spesifikt for beslutningsstyrt tilgang da det er krav om bruk av dette, og funnene i oppgaven er basert på beslutningsstyrt tilgang. Figur 2 viser hierarkisk hvordan en bruker tildeles tilgang i DIPS. En bruker tildeles én eller flere brukerroller. Hver enkelt brukerrolle blir så tildelt et antall tilgangsprofiler, som gir tilgang til brukertyper (rollemaler iht. EPJ-standarden), organisasjonsenheter innad i virksomheten, journalgrupper som gir tilgang til dokumenttyper, og arbeidsgrupper som gir tilgang til arbeidsoppgaver. Brukertyper er et navngitt sett med autorisasjoner som inneholder én eller flere elementtyper. Elementtyper gir så tilgang til funksjoner og data i DIPS EPJ. Et eksempel på elementtype kan være «Journaldata», som må tildeles en brukertype for å få tilgang til data i journalen (Strømmen, 2013).



Figur 2 Oppsett av tilganger i DIPS [6]

Den beslutningsstyrte tilgangen i DIPS er i praksis en enda mer finkornet tilgangsstyring enn den som beskrives i EPJ-standarden, ved at det må foreligge et besluttet tiltak og baseres på beslutningsmaler, som tilsvarer tiltaksmaler i EPJ-standarden (Strømmen, 2013). DIPS har implementert modellen for beslutningsstyrt tilgang som vist i figur 3, hvor det eksemplifiseres hvordan tilgang gis ved beslutning om helsehjelp til en inneliggende pasient.

[6] (T. Elde, Løsningsarkitekt og FoU-koordinator i DIPS ASA, personlig kommunikasjon, 8. januar, 2013)



Figur 3 Modell for tilgangskontroll i DIPS [7]

Å forklare denne modellen i detalj, på en kortfattet måte lar seg vanskelig gjøre, til det er modellen for kompleks. Det er derfor bare gitt et eksempel, hvor begreper fra EPJ-standarden er inkludert. Når bruker opptrer som en brukerrolle (EPJ-standard: tjenesteyter) med tilhørende tilgangsprofil (EPJ-standard: Rolle), med tilgang til aktuell organisasjonsenhet aktiverer en pasient, og åpner skjermbilder der det er tilknyttet pasientdata, vil DIPS sjekke at det foreligger et besluttet tiltak basert på en beslutningsmal (tiltaksmal iht. EPJ-standarden) knyttet til den aktuelle organisasjonsenheten. Beslutningsmalen, i dette tilfellet «Inneliggende pasient» vil sjekke brukers tilgang til organisasjonsenhet, og gir tilgang til pasientens journal, og viser aktuelle journalgrupper som bruker har tilgang til. Sagt på en enklere måte; helsearbeider er involvert i pasientbehandlingen fordi behandling foregår ved samme organisasjonsenhet som helsearbeider er tilknyttet, og hvis så er tilfelle sjekkes det hvilke opplysninger helsearbeider kan åpne, gitt ved dataelementtyper og journalgrupper.

[7] (T. Elde, Løsningsarkitekt og FoU-koordinator i DIPS ASA, personlig kommunikasjon, 8. januar, 2013)

2.5.1 Implisitt tilgang

DIPS sin implementasjon av beslutningsstyrt tilgang består av to typer overordnede beslutningsmaler, og skiller da mellom implisitt og eksplisitt tilgang. Med implisitt tilgang menes de tilganger en bruker automatisk får som en del av det naturlige pasientforløpet og bruk av systemet, og er formalisert i form av tiltaksmaler som illustreres her:

- Bruker er informasjonsansvarlig for pasienten
- Bruker er journalansvarlig for pasienten
- Bruker er pasientansvarlig for pasienten
- Bruker er pasientens primærkontakt
- Bruker har behandlingsansvar for pasienten
- Dokument i arbeidsflyt
- Henvisning til vurdering
- Vurdert henvisning
- Inneliggende pasient
- Planlagt oppmøte
- Poliklinisk besøk
- Pasienten finnes på operasjonsoversikten
- Ventende pasient
- Åpen henvisningsperiode
- Åpen konsultasjonsserie
- Inneliggende ledsager

2.5.2 Eksplisitt tilgang/grønnlystilgang

I de tilfeller en bruker ikke har gyldig implisitt tilgang, altså da ingen av de ovennevnte tiltaksmalene slår til, men tilgang er ønskelig, må bruker benytte/beslutte eksplisitt tilgang, også benevnt grønnlystilgang. Dette for å kunne dokumentere hvorfor det var nødvendig for tilgangen. DIPS har da følgende eksplisitte tiltaksmaler:

- Bestilling av dokumenter fra offentlige og juridiske instanser og forsikringsselskap
- Eksternt prøvesvar/notat til vurdering
- Etterarbeide

- Forskning
- Henvendelse fra pasienten
- Henvendelse fra pasientens behandler
- Henvendelse fra pasientens pårørende
- Internkontroll/Kvalitetssikring
- IT-Systemarbeid
- Meldt pasient
- Pasientinnsyn
- Tilsyn med helsepersonellets virksomhet
- Tilsyn på annen avdeling.
- Undervisning
- Åpne sperret journal i nødverge

Listen ovenfor viser alle tilgjengelige tiltaksmaler som leveres som standard i DIPS, og hvilke maler en bruker har tilgang til avhenger av virksomheten sine retningslinjer for hvilke rollmaler som skal ha tilgang til hvilke tiltaksmaler. Bruk av grønnlys loggføres i et eget hendelsesregister.

2.5.3 Nødrettstilgang/blålystilgang

Funksjonaliteten for nødrettstilgang i DIPS kalles blålystilgang. Når man benytter denne funksjonen (om bruker har tilgang til den), får man opp et skjermbilde der man er nødt til å fylle inn en fritekstbegrunnelse for årsak til tilgang. Alle journaloppslag loggføres, men bruk av blålys havner i likhet med grønnlys i en egen logg. Ved bruk av blålys får man i hovedsak tilgang til alle medisinske data på aktuell pasient, men det kan imidlertid finnes unntak. Hver virksomhet kan sette opp hvilke type dokumenter man får tilgang til ved bruk av blålys, og hvilke typer psykiatriske journaldokumenter brukere i somatiske avdelinger kan få tilgang til.

2.5.4 Sperrefunksjon

Pasienter har i henhold til lovverket rett til å kreve sperring av hele eller deler av sin journal iht. Pasient- og brukerrettighetsloven § 5-3 (1999) og Helsepersonelloven § 25 og 45 (1999).

For å etterleve lovverket, er det i DIPS funksjonalitet for å sperre alle pasientopplysninger, deler av journalen eller enkelte journaldokumenter til en valgt pasient, for én eller flere brukere, for all tid, eller for en bestemt tidsperiode.

Sperrefunksjonen overstyrer tilgangsstyringen som er beskrevet i 2.3.1 og 2.3.2. Av pasientsikkerhetsårsaker er det likevel mulig for virksomheten (helseforetaket) å gi enkelte brukere tilgang til å åpne sperrede journaldokumenter.

2.6 Oppsummering og presisering av problemet

I dette kapittelet har det blitt presentert teori som anses relevant for oppgaven. Utfordringer med tilgangsstyring kan inntreffe når en person benytter en EPJ for å tilegne seg taushetsbelagte opplysninger. Litteratursøk viser at det finnes lite vitenskapelig dokumentasjon på erfaringer med bruk og forvaltning av tilgangsstyring i EPJ på generelt grunnlag, og ingen som spesielt tar for seg beslutningsstyrt tilgang. Litteraturen på området omhandler i hovedsak forslag til tilgangsmodeller som kan være egnet til bruk i EPJ. På bakgrunn av dette ble denne oppgaven konsentrert rundt å gjøre en undersøkelse av utfordringer med bruk og forvaltning av tilgangsstyring med beslutningsstyrt tilgang.

2.7 Problemformulering og forskningsspørsmål

På bakgrunn av den teoretiske forankringen er nedenstående problemformulering og forskningsspørsmål valgt.

2.7.1 Problemformulering

Hvilke utfordringer er det med tilgangsstyring av elektronisk pasientjournal i spesialisthelsetjenesten, og hvordan kan den forbedres?

2.7.2 Forskningsspørsmål

1. Hva anser sluttbrukere og systemforvaltere som de viktigste utfordringene med tilgangsstyring med beslutningsstyrt tilgang?
2. Hva er viktige faktorer for at tilgangsstyringen kan forbedres for å ivareta pasientsikkerhet og pasienters personvern?

2.8 Studiens avgrensninger

Forskningsområdet for denne oppgaven befinner seg i skjæringspunktet mellom informasjonssikkerhet og helsetjenesten. Helsetjenesten styres av lover og forskrifter som ofte er unike for hvert enkelt land, selv om mange land har liknende lover. Denne oppgaven er i hovedsak basert på den norske helsetjenesten, og lovene og forskriftene som regulerer den, konkretisert gjennom EPJ-standarden.

Videre avgrenses studien til kun å omhandle EPJ i spesialisthelsetjenesten. Studien vil ikke utforske problematikk rundt tilgangsstyring på tvers av virksomheter. Tekniske betraktninger vi ikke diskuteres i dybden, og studien omhandler heller ikke pasienters tilgang til egen journal, og problematikk rundt dette.

2.9 Teoretisk rammeverk

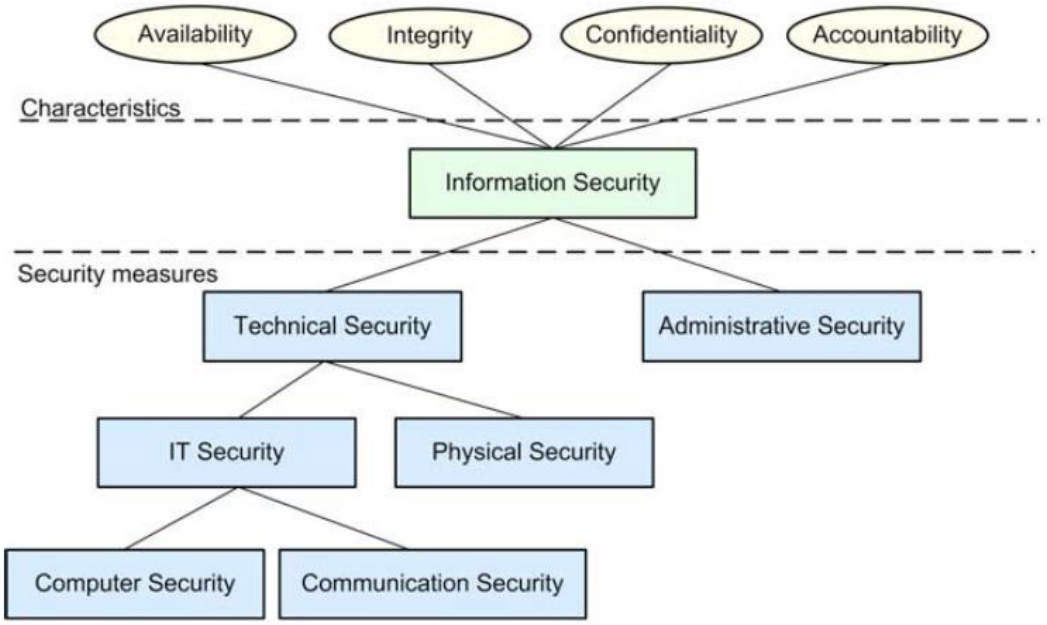
Teorier benyttes for å uttrykke noe allment, noe som gjelder for hele befolkningen eller for grupper av befolkningen, eller avgrensede områder. Teorier forenkler fenomener, ved at de viser til essensen i det fenomenet som teoretiseres. Vitenskapelige teorier viser til regelmessige mønstre som mulig vil ha gyldighet i en overskuelig framtid (Johannesen, Tufte og Kristoffersen, 2010).

I første del av oppgaven er det beskrevet problemstillinger knyttet til tilgangsstyring av taushetsbelagte opplysninger i EPJ. For å undersøke sluttbrukere og systemforvalteres utfordringer med tilgangsstyring blir Åhlfeldt (2008) sin Extended InfoSec model for informasjonssikkerhet i helsetjenesten brukt som teorigrunnlag. Modellen er utviklet med det formål å beskrive på en enkel måte hva informasjonssikkerhet representerer, og kan uttrykke hvor problemer og behov innen informasjonssikkerhet eksisterer. I denne oppgaven blir modellen brukt

for å synliggjøre innen hvilke områder respondentenes faktorer for utfordringer og forbedringer med tilgangsstyring kan plasseres.

2.9.1 The Information Security Model

Åhlfeldt utviklet som del av et doktorgradsarbeid en modell for informasjonssikkerhet i helsetjenesten kalt Information Security Model. Modellen er en kombinasjon av fire anerkjente kjennetegn for å oppnå informasjonssikkerhet; tilgjengelighet, integritet, konfidensialitet og ansvarlighet, og SIS-modellen (Swedish Standards Institute) for sikkerhetstiltak. Sistnevnte benyttes for å dele opp sikkerhetstiltakene fra et informasjonssikkerhetsperspektiv (Åhlfeldt, 2008). Modellen presenteres i figur 4.



Figur 4 InfoSec-modellen

Hovedbegrepet informasjonssikkerhet er presentert i midten. De fire kjennetegnene som står øverst representerer sammen informasjonssikkerhet. For at informasjonssikkerhet i en organisasjon skal oppnås, må alle disse egenskapene være oppfylt. Den nederste delen av modellen presenterer de forskjellige sikkerhetsforanstaltningene, fordelt i en hierarkisk orden. Modellens komponenter forklares på følgende måte:

- **Tilgjengelighet** refererer til forventet ressursbruk innenfor en tidsramme
- **Integritet** omhandler beskyttelse mot uønskede endringer
- **Konfidensialitet** handler om å beskytte data fra uautorisert tilgang
- **Ansvarlighet** handler om muligheten til å spore utførte aktiviteter til en enkeltperson

- **Informasjonssikkerhet** dekker problemstillinger knyttet til alle typer informasjonsbehandling og kan bli sett på som en prosess med å beskytte informasjonsressurser, med det formål å oppnå tilgjengelighet, konfidensialitet, integritet og ansvarlighet. Både tekniske og administrative sikkerhetstiltak er nødvendig for å oppnå disse fire kjennetegnene.

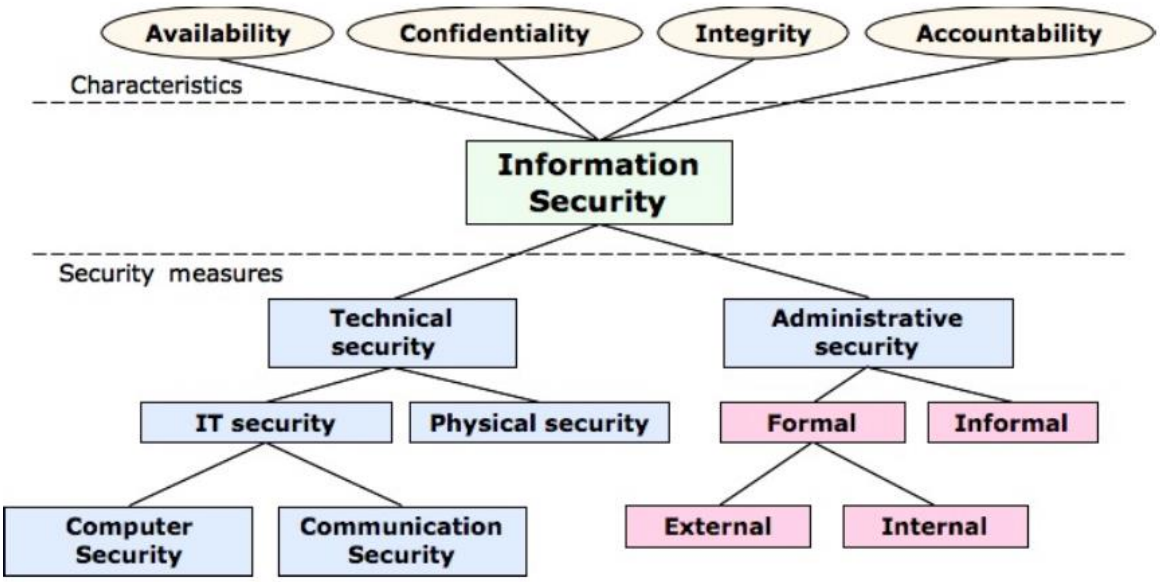
- **Administrativ sikkerhet** omhandler forvaltning av informasjonssikkerhet; strategier, retningslinjer, risikovurderinger, opplæring osv. Planlegging og implementering av sikkerhet krever en strukturert måte å jobbe på. Denne delen av den totale sikkerheten er på et organisatorisk nivå og angår virksomheten som helhet.

- **Teknisk sikkerhet** omhandler tiltak som skal treffes for å nå de overordnede kravene, og skal derfor understøtte det som inngår i aspektet administrativ sikkerhet. Teknisk sikkerhet deles videre inn i fysisk sikkerhet og IT-sikkerhet.
- **Fysisk sikkerhet** omhandler fysisk beskyttelse av for eksempel datalagringsenheter og alarmer
- **IT-sikkerhet** omhandler informasjonssikkerhet i tekniske informasjonssystemer, og kan deles inn i data- og kommunikasjonssikkerhet
- **Datasikkerhet** omhandler beskyttelse av maskinvare og dets innhold, for eksempel sikkerhetskopiering og kryptering
- **Kommunikasjonssikkerhet** innebærer beskyttelse av nettverk og andre medier som kommuniserer informasjon mellom datamaskiner

Da modellen manglet en utdyping av det administrative sikkerhetsaspektet, ble modellen videreutviklet ved å legge til elementene formell og uformell (Formal og Informal) fra TFI-modellen, som viser et informasjonssystem som bestående av tekniske (T), formelle (F) og uformelle (I) elementer. TFI-modellen ble valgt da den er en semiotisk modell, som fokuserer på kontekstrelaterte aspekter som organisasjonskultur og menneskelig

adferd i stedet for teknologi. Dette gjør det mulig å forstå kontekstspesifikke aspekter som ellers kan være vanskelige å analysere.

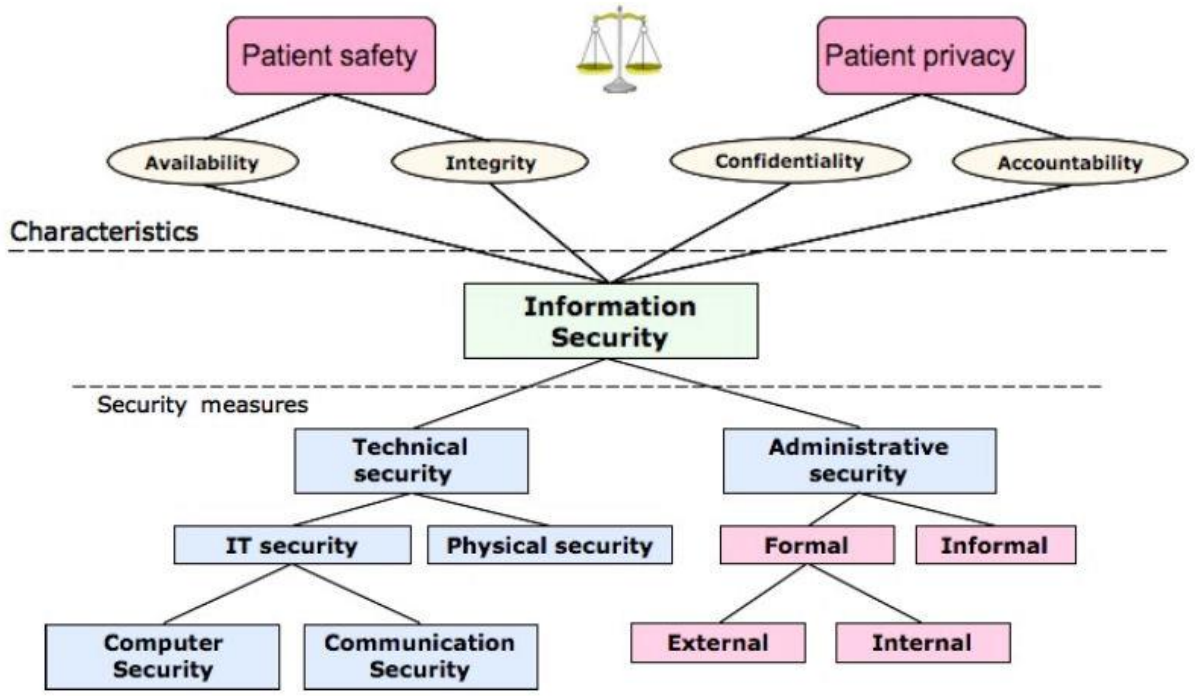
Administrativ sikkerhet omhandler styring av informasjonssikkerhet, som kan være både formell og uformell. Det formelle elementet omfatter retningslinjer, regler, kontroller, standarder osv. som tar sikte på å definere et grensesnitt mellom teknologiske delsystemer, mens det uformelle elementet omhandler aspekter relatert til menneskelig oppførsel. Det formelle aspektet er videre underinndelt i et eksternt og internt nivå. Dette da organisasjoner må forholde seg til eksterne reguleringer rundt informasjonssikkerhet, f.eks. lover, forskrifter og avtaler med andre organisasjoner. Videre er det interne regler og retningslinjer for informasjonssikkerhet som IT-strategier, sikkerhetsrutiner, opplæring og informasjon osv. På bakgrunn av disse nye aspektene ble InfoSec-modellen utvidet, som vist i figur 5.



Figur 5 Den utvidede InfoSec-modellen

Modellen er ytterligere utvidet ved å inkludere aspektene som angir hovedmålet med informasjonssikkerhet i helsetjenesten; pasientsikkerhet og personvern. Pasientsikkerhet defineres her som muligheten for å kunne gi best mulig omsorg med riktig informasjon til rett tid. Personvern defineres som å beskytte taushetsbelagte opplysninger fra å bli distribuert til uautoriserte personer. Pasientsikkerhet er derfor direkte knyttet til tilgjengelighet og integritet, mens personvern er direkte knyttet til konfidensialitet og ansvarlighet, som vist i figur 6.

Det understrekes imidlertid at disse knytningene ikke er absolutte da det kan oppstå tilfeller hvor konfidensialitet og ansvarlighet er nødvendig for å oppnå pasientsikkerhet, og tilgjengelighet og integritet er nødvendig for å oppnå pasientens personvern (Åhlfeldt, 2008).



Figur 6 Den utvidede InfoSec-modellen med pasientsikkerhet og personvern

Tilgangsstyring i EPJ bidrar til informasjonssikkerhet ved å ivareta pasienters personvern, samtidig som det ikke skal gå på bekostning av pasientsikkerhet, og er avhengig av både administrative og tekniske aspekter for å kunne lykkes med oppgaven. På bakgrunn av dette anses den utvidede InfoSec-modellen som egnet til å visualisere utfordringer og potensielle forbedringer av tilgangsstyring.

3.0 METODE OG UTVALG

Dette kapittelet beskriver fremgangsmåten for å besvare de forskningsspørsmålene som er formulert. Det redegjøres for metodevalg, gjennomførelsen av studien, og bakgrunn for de valg som er tatt vil bli belyst. Videre beskrives utvalg, gjennomføring av spørreundersøkelsene, analyse av spørsmålsrundene, metodekritikk, etiske overveielser og litteratursøk og kildekritikk.

Valg av metode ble basert på problemstillingen som skulle undersøkes, og mangel av empiri på dette problemområdet. På bakgrunn av dette falt valget på å benytte Delphimetoden. Målet med undersøkelsen er å få frem sluttbrukere og systemforvalteres meninger om hva som er dagens utfordringer med, og mulige forbedringer av tilgangsstyringen i EPJ for spesialisthelsetjenesten. For å finne svar på dette var det naturlig å gjennomføre en Delphiundersøkelse med disse to gruppene, fordelt på hvert sitt ekspertpanel.

I tillegg har det blitt tatt ut rapporter med data fra DIPS-databasen ved helseforetaket sluttbrukerne er ansatt i, som kan bidra til å belyse utfordringer rundt dagens tilgangsstyring.

En pilotstudie ble gjennomført både for å teste hvordan spørreskjemasystemet SurveyXact som Universitet i Agder har lisens på, fungerer som verktøy til en Delphistudie, og generell test av formatering og spørsmålsstilling. Det ble inkludert 13 respondenter i piloten; syv sluttbrukere og seks systemforvaltere, og studien ble gjennomført over fire runder. På bakgrunn av pilotstudien ble det gjort endringer i formatering, og teknisk oppsett for validering av svar i de to siste rundene.

3.1 Delphimetoden

Delphimetoden ble utviklet av Rand Corporation på begynnelsen av 1950-tallet da luftforsvaret i USA ønsket å estimere hvor mange atombomber Sovjetunionen ville avfyre mot USA i en tenkt krigssituasjon. Måten dette ble gjennomført på var at et ekspertpanel bestående av syv respondenter; fire økonomer, én ekspert innen fysisk sårbarhet, én systemanalytiker, og én elektronikkingeniør deltok i en studie bestående av fem spørreskjemaer som ble sendt ut med en ukes mellomrom. Forfatterne konkluderte med at

metoden er meget gunstig for å fremstille en foreløpig innsikt i et problemområde, som videre forskning kan bygge på (Dalkey og Helmer, 1962).
Delphimetoden har siden da blitt mye brukt innen forskning på bl.a. informasjonssystemer, som en iterativ prosess for å samle inn og destillere eksperter innen et område sine meninger (snarere enn objektive fakta), ved hjelp av en rekke spørreskjemaer og tilbakemeldinger (Skulmoski, Hartman og Krahn, 2007).
En undersøkelse kan utføres på ulike måter, men det er allikevel fire grunnleggende kjennetegn ved Delphimetoden (Rowe og Wright, 2001):

- Anonymitet
- Iterasjon
- Kontrollerte tilbakemeldinger
- Statistisk grupperespons

Respondentene i en Delphistudie kjenner normalt ikke hverandre og anonymitet overfor de andre respondentene oppnås ved at prosessen koordineres av en moderator. Spørreskjemaene fylles ut av respondentene og returneres til moderatoren som så analyserer grupperesponsen. Ivaretakelse av anonymitet har noen fordeler fremfor andre metoder med gruppedynamikk, som f.eks. fokusgruppeintervju, ved at anonymitet reduserer påvirkning av dominante personer, respondentene kan lettere endre mening uten å «tape ansikt», og anonymitet fører vanligvis til en høyrere svarprosent. Det andre kjennetegnet ved en Delphistudie er at undersøkelsen gjennomføres gjennom flere iterasjoner/runder. Dette sammen med at respondentene får tilbakemelding, kan bidra til læring og endring av tidligere vurderinger, og økt enighet blant respondentene. Nye runder gjennomføres vanligvis frem til man oppnår stabilitet i respondentenes svar, og ikke nødvendigvis når konsensus er oppnådd. Tilbakemeldingene er kontrollerte da moderatoren analyserer svarene og kontrollerer og omarbeider svarene før tilbakemelding gis til respondentene i neste runde. Statistisk grupperespons presenteres enten grafisk eller numerisk, med sentraltendens og spredning, og i enkelte tilfeller gjengis kommentarer fra respondentene. Avhengig av antall runder kan man i tillegg til å måle grad av konsensus, også påvise endring og utjevning av meninger (Gracht, 2012).

Det finnes ikke noen standard prosedyre for gjennomførelse av en Delphistudie da ulike studier kan ha nytte av ulike tilnærminger, men en typisk Delphistudie består av følgende

stadier: Først utformes forskningsspørsmål, deretter velges metode. Både kvalitative og kvantitative metoder kan benyttes i en Delphiprosess. Deretter velger man informanter/eksperter. Så kommer selve undersøkelsesfasen som i hovedsak kan bestå av tre faser (Okoli og Pawlowski, 2004; Schmidt, 1997):

- Idémyldring
- Innsnevring
- Rangering

Før selve undersøkelsen starter, kan det være hensiktsmessig å utføre en pilotstudie for å avdekke eventuelle svakheter ved undersøkelsen (Skulmoski et al., 2007).

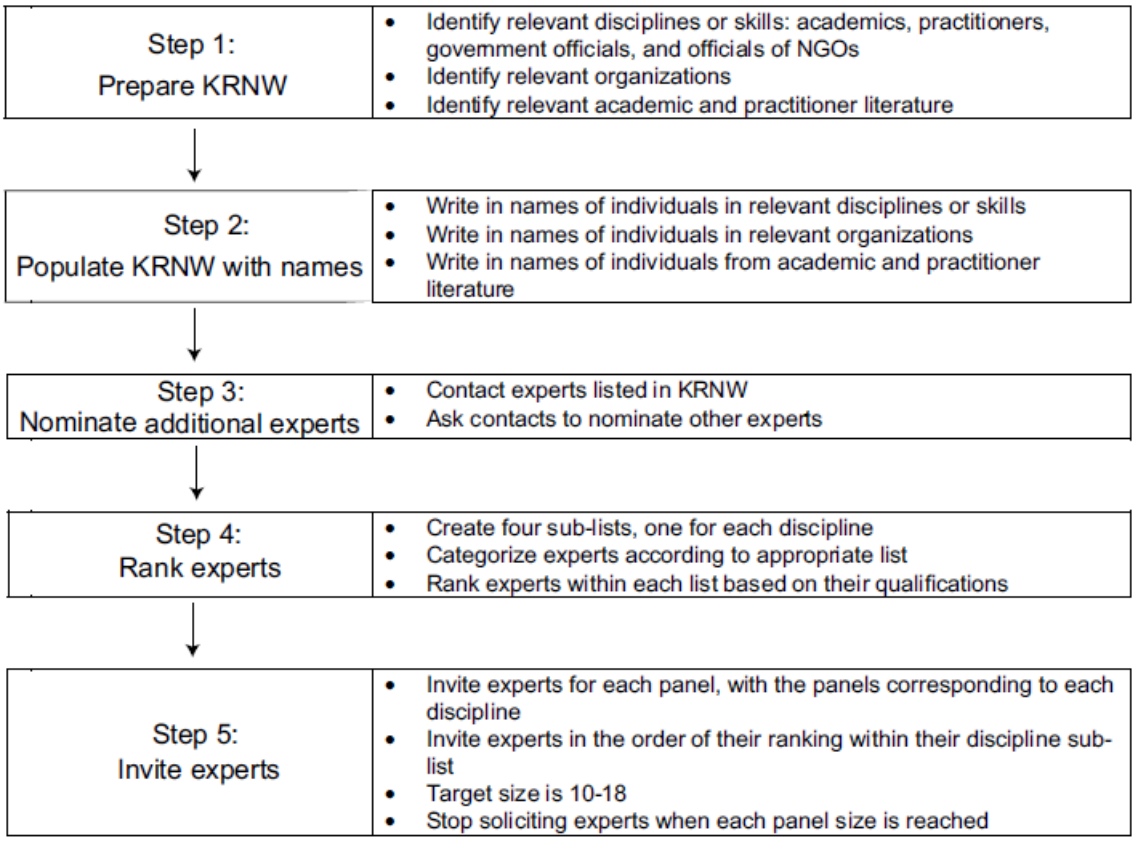
3.2 Bakgrunn for valg av metode

Delphimetoden innebærer, som andre metoder, både styrker og svakheter. Metoden er valgt på bakgrunn av at bruk av tilgangsstyring er et lite undersøkt fenomen som krever kunnskap fra personer som har erfaring med de forskjellige aspektene knyttet til bruk og forvaltning av dette. Det er forfatters oppfatning at problemområdet ikke i tilstrekkelig grad er utforsket slik at man har belegg for hvilke variabler man skulle bygget opp et tradisjonelt spørreskjema med. Å benytte en Delphimetode med ekspertpanel vil også kunne svare bedre på forskningsspørsmålene enn ved intervju av enkeltpersoner, det kan avdekkes flere faktorer, og de kan lettere kvantifiseres. I tillegg er det en fordel at ekspertene slipper å møtes, med tanke på tidligere nevnte fordelere med anonymitet, og logistikk da det ene ekspertpanelet består av respondenter fra flere landsdeler, og det andre panelet består av klinikere som man kan tenke seg at ikke med letthet ville fått aksept for å dras ut av produksjonen i større grad enn de har i denne undersøkelsen. Det er også en fordel at antall respondenter per panel gjerne kan være fra 10 til 18, selvsagt avhengig av studie, og tilgjengelige eksperter innen aktuelt område (Okoli og Pawlowski, 2004).

Denne oppgavens undersøkelse baseres på en rangordningsbasert tilnærming av Delphimetoden, som beskrevet av Schmidt (1997), med en kvalitativ innledende runde, en runde med validering av konsolidering av kvalitative svar, og deretter reduksjon av faktorer, og konsensusprosess med rangering av faktorer.

3.3 Utvalg

I en Delphistudie søker man ikke et utvalg som skal være representativt for en populasjon, man søker i stedet én eller flere grupper med kvalifiserte eksperter som har inngående forståelse og kunnskap om temaet for studien (Okoli og Pawlowski, 2004). Denne masteroppgaven har en praktisk tilnærming til tilgangsstyring i helsetjenesten. Fokuset har vært på økt innsikt i erfaringer med bruken og forvaltningen av beslutningsstyrt tilgang i EPJ i spesialisthelsetjenesten, for å avdekke utfordringer, og kunne komme med anbefalinger for forbedringer av tilgangskontrollen. Det er kun når man har en bedre forståelse av sluttbrukere og systemforvalteres arbeidshverdag at det gir mening å foreslå forbedringer av tilgangsstyring i EPJ. Sluttbrukerne og systemforvalterne ble fordelt til hvert sitt panel, og utvelgelse av eksperter baseres på Okoli og Pawloski (2004) sine anbefalinger om utarbeidelse av et knowledge resource nomination worksheet (KRNW) som vist i figur 7, men i en forenklet og modifisert utgave.



Figur 7 Utarbeidelse av Knowledge Resource Nomination Worksheet (KRNW) (Okoli og Pawlowski, 2004)

3.3.1 Sluttbrukere

Ett av punktene i første steget i prosedyren for utvelgelse av eksperter er å identifisere aktuelle organisasjoner respondentene befinner seg i. Kriteriene for organisasjon var at det måtte være en organisasjonsenhet i spesialisthelsetjenesten, og et helseforetak i Helse Sør-Øst som benytter EPJ fra DIPS, og beslutningsstyrt tilgang. Valget falt da på SSHF (Sørlandet sykehus Helseforetak).

Det ble så gjort en vurdering på hvilke kriterier som skulle stilles til aktuelle respondenter i dette panelet. Ett av kriteriene var at brukerne i størst mulig grad skulle benytte aktualisering (grønnlysfunksjonen i DIPS), altså tilfeller der ordinær tilgangsstyring ikke dekker behovet og gir tilgang. For å identifisere aktuelle stillinger ble det derfor tatt ut rapport fra DIPS på bruk av aktualisering som presenteres i tabell 9 i kapittel 4.3. I tillegg ble sykepleiere invitert da de er den største brukergruppen, og tilbakemeldinger fra dem anses derfor som viktig. Det var også et kriterium at sluttbrukerne skulle ha fått ekstra opplæring i, og ha vært med på testing av beslutningsstyrt tilgang da dette ble innført ved SSHF. Sistnevnte kriterium ble satt for å øke sannsynligheten for at sluttbrukerne i studien var innforstått med begreper som beslutningsstyrt tilgang og relaterte begrep og problemstillinger som ville komme frem i løpet av spørsmålsrundene i undersøkelsen. Forfatter fikk hjelp av IKT-avd. ved SSHF til å få oversikt over hvilke brukere som tilfredsstilte disse kriteriene, og på bakgrunn av dette ble et skjema for nominasjon utarbeidet.

Tredje steg i prosessen ble utelatt da man på bakgrunn av de foregående stegene hadde opparbeidet tilstrekkelig antall navn. Aktuelle respondenter ble så rangert på bakgrunn av tidligere nevnte kriterier, men måltallet for respondenter ble ca. doblet fra 10-18 til 35, da informantene første gang ble kontaktet med forespørsel om deltakelse sammen med første spørreskjema, og for å ta høyde for frafall slik at man etter siste runde skulle sitte igjen med mellom 10 og 18 respondenter.

Sluttbrukerne som samtykket til å delta i undersøkelsen, og gjennomførte første runde vises i tabell 1. Samlekategorien «andre stillinger» er benyttet av anonymitetshensyn.

Tabell 1 Sluttbrukerpanel

Stilling	Antall eksperter
Enhetsleder	**1**
Overlege	**1**
Rådgiver	**1**
Sekretær	**4**
Sykepleier	**4**
Andre stillinger	**7**
Sum	**18**

3.3.2 Systemforvaltere

Da antall personer med kompetanse innen forvaltning av tilgangsstyring i EPJ i spesialisthelsetjenesten er relativt sett lavt i forhold til sluttbrukere, var det nødvendig å inkludere respondenter fra flere organisasjoner. Kriteriene for organisasjon var at det måtte være en organisasjonsenhet i spesialisthelsetjenesten som benytter EPJ fra DIPS ASA. Det ble derfor valgt å nominere aktuelle respondenter fra de tre regionale helseforetakene som benytter DIPS; Helse Nord, Helse Vest, og Helse Sør-Øst.

Det ble så gjort en vurdering på hvilke kriterier som skulle stilles til aktuelle respondenter i dette panelet. For å få en bredde i panelet ble det inkludert eksperter med kompetanse i både direkte forvaltning av EPJ (lokale systemforvaltere ved hvert helseforetak, og regionale systemforvaltere, som f.eks. ansatte i Helse Vest IKT og Sykehuspartner), og personer med kompetanse innen personvern og lovverk knyttet til tilgangsstyring. En rekke eksperter ble nominert på bakgrunn av forfatters kjennskap til personer i fagmiljøet i Sykehuspartner som forvalter EPJ for hele Helse Sør-Øst. Andre eksperter under Helse Vest og Helse Nord ble nominert på bakgrunn av deres deltakelse i prosjekter og arbeidsgrupper for tilgangsstyring. Enkelte av de nominerte ekspertene ble så kontaktet for nominering av flere eksperter. Ekspertene ble så rangert, og 20 av ekspertene ble formelt invitert til å delta i studien. Tallet er lavere enn i det andre panelet da det ble forventet lavere frafall på grunn av kontakt med enkelte av ekspertene før formell invitasjon ble sendt sammen med første runde av spørreundersøkelsen.

Systemforvalterne som samtykket til å delta i undersøkelsen, og gjennomførte første runde, vises i tabell 2.

Tabell 2 Systemforvalterpanel

Stilling	Antall eksperter
Systemforvalter regionalt	**10**
Systemforvalter lokalt	**5**
Spes. komp. personvern og jus	**2**
Sum	**17**

3.4 Gjennomføring

Studien ble gjennomført i løpet av fire runder. For distribusjon av spørsmålene og innsamling av data, ble spørreskjemasystemet SurveyXact benyttet. Dette foregikk ved at en lenke til spørreskjemaet ble sendt via e-post til respondentene. Svarfristen ble satt til tre arbeidsdager med en påminnelse fjerde virkedag for de av respondentene som ikke hadde besvart aktuelt spørreskjema.

Analysen ble gjennomført i løpet av to til fire dager, og deretter returnert til ekspertene. Respondenter som ikke besvarte en runde, ble ekskludert fra resten av undersøkelsen.
De to første rundene ble respondenten behandlet som ett panel, men ble så delt opp i to panel i runde tre og fire på bakgrunn av sin stilling og kompetanse. Tabell 3 viser en oversikt over respondentenes deltakelse i spørreskjemarundene.

Tabell 3 Deltakelse

	Sluttbrukere	Systemforvaltere	Totalt
Runde én (%)	**18 (100)**	**17 (100)**	**35 (100)**
Runde to (%)	**18 (100)**	**17 (100)**	**35 (100)**
Runde tre (%)	**16 (89)**	**16 (94)**	**32 (91)**
Runde fire (%)	**13 (72)**	**15 (88)**	**28 (80)**

3.5 Analyse

I denne undersøkelsen ble det gjort en kvalitativ innholdsanalyse av første runde med spørreskjema, der det ble valgt å benytte Directed Content Analysis, beskrevet av Hsieh og Shannon (2005) som tar utgangspunkt i at man har et teoretisk rammeverk som grunnlag for koding av utsagn. Respondentenes utsagn ble derfor forkortet og kategorisert i henholdt til de predefinerte kategoriene i InfoSec-modellen. I fjerde runde ble grad av konsensus analysert i SPSS ved å beregne Kendall's W.

3.5.1 Første runde

I den første runden besvarte ekspertene følgende spørsmål:

Spørsmål 1: *Hvilke utfordringer opplever du knyttet til beslutningsstyrt tilgang (tilgangsstyringen i DIPS)? Du bør nevne punktvis (i stikkordsform) minst fem utfordringer du kommer på.*

Spørsmål 2: *Hvordan kan tilgangsstyringen i DIPS etter din mening forbedres? Du bør nevne punktvis (i stikkordsform) minst fem faktorer du kommer på.*

I e-posten med forespørselen om deltakelse i undersøkelsen, fikk respondentene en kortfattet informasjon om problemområdet rundt tilgangsstyring for å sikre at de hadde en felles forståelse av begrepet tilgangsstyring, og beslutningsstyrt tilgangskontroll. De kvalitative dataene ble så konsolidert slik at svar med lik betydning ble slått sammen, og svar ble sortert under overordnede kategorier, og en rekke svar ble reformulert for å tydeliggjøre utfordringen eller forbedringsforslaget.

På bakgrunn av spørsmål 1 ble totalt 56 unike utfordringer identifisert etter konsolidering av like svar.

På bakgrunn av spørsmål 2 ble totalt 44 unike forbedringsforslag identifisert etter konsolidering av like svar.

3.5.2 Andre runde

Ekspertene fikk etter første runde automatisk tilsendt en e-post med svarene de hadde oppgitt, og ble i andre runde stilt følgende forespørsler relatert til spørsmålene fra første runde:

Spørsmål 1: *Jeg spurte: Hvilke utfordringer opplever du knyttet til beslutningsstyrt tilgang (tilgangsstyringen i DIPS)? Du bør nevne punktvis (i stikkordsform) minst fem utfordringer du kommer på. Svarene som kom inn er oppsummert nedenfor (men ikke nødvendigvis ordrett). Se igjennom listen, og dersom du ikke finner ditt svar, sett det opp i feltet nedenfor i stikkordsform.*

Spørsmål 2: *Jeg spurte: Hvordan kan tilgangsstyringen i DIPS etter din mening forbedres? Du bør nevne punktvis (i stikkordsform) minst fem utfordringer du kommer på. Svarene som kom inn er oppsummert nedenfor (men ikke nødvendigvis ordrett). Se igjennom listen, og dersom du ikke finner ditt svar, sett det opp i feltet nedenfor i stikkordsform.*

Tre av respondentene kom med tilbakemeldinger i denne runden, og som et resultat av dette ble tre nye faktorer under spørsmål 1 inkludert i runde tre, og det ble gjort en tilføyelse på en av faktorene under spørsmål 2.

3.5.3 Tredje runde

I den tredje runden ble ekspertene behandlet som to selvstendige panel, og bedt om å velge ut minst 10 av de viktigste utsagn/faktorer knyttet til hvert av de to initiale spørsmålene. Utsagnene/faktorene ble arrangert i tilfeldig rekkefølge for å unngå bias som følge av kontekseffekter. Faktorene kan ses i sin helhet i vedlegg 6.

Spørsmål 1: *Velg minst 10 utsagn/faktorer som du mener er viktige utfordringer knyttet til beslutningsstyrt tilgang. Dine svar skal være basert på den kompetansen du har i din stilling. Utfordringene trenger ikke å forholde seg til dine egne erfaringer.*

Spørsmål 2: *Velg minst 10 utsagn/faktorer som du mener er viktige faktorer for at tilgangsstyringen skal forbedres. Dine svar skal være basert på den kompetansen du har i din stilling. Forbedringsforslagene trenger ikke å forholde seg til dine egne erfaringer.*

For panelene med sluttbrukere ble utsagn/faktorer som var valgt av over 30 % av ekspertene beholdt, mens det i systemforvalterpanelet ble satt et cut-off point på 35 % for spørsmål én, og 40 % for spørsmål to. Dette ble gjort for å redusere listene til en håndterbar størrelse på rundt 10 faktorer, og samtidig sikre at viktige faktorer ikke ble avvist i denne runden.

3.5.4 Fjerde runde

I den fjerde runden ble ekspertene bedt om å rangere utsagn/faktorene fra den reduserte listen etter forrige runde, knyttet til hvert spørsmål. Utsagnene/faktorene ble arrangert i tilfeldig rekkefølge for å unngå bias som følge av kontekseffekter.
I tillegg kunne ekspertene spørreskjemaet legge inn kommentarer for å forklare eller rettferdiggjøre sine rangeringer.

Spørsmål 1: *I hvilken grad anser du følgende utsagn/faktorer som utfordringer i tilgangsstyringen?*

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-10[8] *i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-10, der 1 = viktigst*

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

Spørsmål 2*: I hvilken grad tror du følgende utsagn/faktorer kan forbedre tilgangsstyringen?*

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-9[9] *i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-9, der 1 = viktigst.*

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

[8] Sluttbrukerne rangerte fra 1-10, mens systemforvalterne rangerte fra 1-9
[9] Sluttbrukerne rangerte fra 1-9, mens systemforvalterne rangerte fra 1-8

Enighet om rangeringen blant ekspertene ble så analysert ved hjelp av Kendall's W i IBM SPSS Statistics 19.

I tillegg ble skalaen invertert for økt lesbarhet ved presentasjon av resultatene, og gjennomsnittlig rangering for hver faktor beregnet.

Kendall's W var < 0,3 for alle spørsmålene, hvilket indikerer meget svak enighet (Schmidt, 1997). Undersøkelsen ble likevel avsluttet av praktiske årsaker, og for ikke å belaste respondentene ytterligere da det ble antatt at flere runder ikke ville føre til sterk grad av enighet blant ekspertene. Dissensus, eller mangel på enighet kan også være et gyldig funn for en Delphistudie (Gracht, 2012; Skulmoski et al., 2007). Panelene hadde blitt enige om de viktigste faktorene, mangel på sterk konsensus var på rangeringen av disse faktorene.

3.6 Metodekritikk

Ifølge litteraturen er det vanlig å sette et cut-off point i runden med redusering av viktige faktorer på >50 % for å oppnå et håndterlig antall faktorer, maksimalt 20-23 (Okoli og Pawlowski, 2004; Schmidt, 1997). I denne studien ble det satt cut-off point på 30-40 % for å få rundt 10 faktorer under hvert spørsmål. Dette medførte at flere faktorer som ikke ble ansett som viktige av hovedvekten av respondenten kom med til runden med rangering av faktorene.

I runde fire ble respondentene bedt om å rangere faktorene slik Schmidt (1997) anbefaler. En svakhet ved denne rangeringsmetoden er at man kan «tvinge frem» irrelevante faktorer. For eksempel kan noen respondenter finne to kriterier svært viktige, mens de resterende er irrelevante. Da vil en faktor uten relevans bli rangert som nummer tre, mens eksperten i prinsippet mener det har lik relevans som faktoren rangert som f.eks. nummer åtte. Et alternativ kunne ha vært å be respondentene angi viktigheten av hver faktor ved hjelp av en Likertskala, og så beregne grad av konsensus ved hjelp av Fleiss kappa analyse. På denne måten er det mulig at respondentene kunne oppnådd konsensus rundt noen av faktorene.
Det kunne også blitt utført flere runder for å enten oppnå en sterkere grad av konsensus, evt. bekrefte deres svake konsensus.

Alle respondentene benytter EPJ fra DIPS ASA, og svarer på bakgrunn av sine erfaringer med dette systemet. Det kan føre til at det er vanskelig å skille mellom prinsipp- og systemnivå, for beslutningsstyrt tilgang. Samtidig anses det for relevant å få frem faktorer som går direkte på utfordringer med det aktuelle EPJ-systemet, da begrepet beslutningsstyrt tilgang ikke eksisterer i et vakuum, men må tas i bruk i et system, og DIPS ASA er den suverent største leverandøren av EPJ til spesialisthelsetjenesten i Norge, og alle Helseforetak i Norge har, eller har planlagt å ta i bruk beslutningsstyrt tilgang.
Det kunne med fordel blitt gjort en triangulering av funn ved å supplere med dybdeintervju, eller ved utførelse av en spørreundersøkelse på bakgrunn av funnene etter Delphistudien.

3.7 Etiske overveielser

På grunnlag av Helsinkideklarasjonen fra 1964, som bygger på Nürnbergkodeksen utformet etter 2. verdenskrigs forskningsetiske overtramp mot svake grupper, eksisterer det forskningsetiske retningslinjer (Førde, 2013).

Tre områder som tradisjonelt diskuteres innen forskningsetiske retningslinjer er; informert samtykke, fortrolighet og konsekvenser (Kvale og Brinkmann, 2009). Informert samtykke går ut på at informantene informeres om undersøkelsens overordnede formål, hovedtrekkene i designen, risikoer og fordeler ved å delta, sikring av at de involverte deltar frivillig, og informasjon om rett til å trekke seg (Kvale og Brinkmann, 2009). Fortrolighet går ut på at private data som identifiserer informantene ikke skal avsløres (Kvale og Brinkmann, 2009).

Data som kan identifisere informantene skal ikke avsløres, av hensyn til deres konfidensialitet. I selve oppgaven vil det derfor ikke blitt tatt med informasjon som kan identifisere informantene, og dette er respondentene i studien informert om.

Konsekvenser innebærer at man bør forholde seg til mulig skade, og de fordeler informantene kan forventes å få ved å delta i undersøkelsen (Kvale og Brinkmann, 2009). Informantene i denne oppgaven er sluttbrukere og systemforvaltere, og de vurderes ikke som sårbare. Spørsmålene omhandler ikke personlige temaer, og det vurderes derfor som lav sannsynlighet for etisk krenkelse av informantenes intimsfære. Spørsmålene er åpne og det anses som lite

trolig at respondentene har følt seg bundet, eller har følt at de kunne havne i konflikt med arbeidsgiver ved å svare på noen bestemt måte.

Studien var godkjent av Norsk samfunnsvitenskapelig datatjeneste (NSD) på bakgrunn av meldeskjema 36271, og fakultetets etikkomité ved Universitetet i Agder. Aksept for gjennomføring av undersøkelse med respondenter ansatt i SSHF, ble innhentet fra forskningsenheten, og aktuelle respondenters deltakelse i undersøkelsen var godkjent av vedkommendes ledere. Respondentene gav frivillig informert samtykke til å delta i studien ved svar på forespørsel om deltakelse i undersøkelse (vedlegg 4).

3.8 Litteratursøk og kildekritikk

Det er bestrebet å bruke primærkilder i oppgaven, og litteratur er i hovedsak innhentet etter søk initialt i Google Scholar, og videre i anerkjente internasjonale og skandinaviske databaser som Medline og Svemed+, via søkemotorene Ovid og Cinahl, i tillegg til søkemotoren Oria som er en søkemotor for universitetsbibliotekets samlede ressurser, da denne ble tilgjengelig. Søkeord omfattet bruk av norske, svenske, danske og engelske ord relatert til tilgangsstyring, EPJ, informasjonssikkerhet, og helsetjenesten.

Litteratursøk viste at det eksisterte få vitenskapelige artikler direkte knyttet til denne oppgavens problemområde, noe som verifiseres av andre studiers omtale av litteratursøk på området (Faxvaag et al. 2011; Røstad, 2009). Den mest relevante vitenskapelige litteraturen omfatter doktorgradene til Andresen (2010), Røstad (2009), og Åhlfeldt (2008) som går i dybden på tekniske, juridiske og generelle informasjonssikkerhetsmessige utfordringer rundt tilgangsstyring i helsetjenesten.

I tillegg har det vært nødvendig å benytte norske offentlige utredninger, og rapporter fra statlige organisasjoner som Helsedirektoratet, Helsetilsynet og Datatilsynet, og det antas at slike kilder er troverdige.

Det har også blitt benyttet personlig kommunikasjon som referanse flere steder i oppgaven. Dette kan selvsagt føre til bias, men det ble ansett som nødvendig å innhente ytterligere informasjon enn det litteratursøk avdekket. Blant annet har det blitt innhentet tillatelse til

innsyn i virksomhetsinterne dokumenter, som sluttrapporter for innføring av beslutningsstyrt tilgang, avviksdokumenter og leveransedokument for standardisering av tilgangsstyring i Helse Sør-Øst, og sluttrapport for prosjektet iAccess. Disse har også vært nyttige for økt forståelse av problemområdet.

Det er i liten grad benyttet utenlandske kilder i oppgaven med unntak av den svenske doktorgraden til Åhlfeldt (2008) som har undersøkt informasjonssikkerhet i helsetjenesten i Norge, Sverige, Finland og England. Dette har pragmatiske årsaker da lite utenlandsk litteratur på området eksisterer, i tillegg til at resultatene kunne vært vanskelige å overføre på grunn av ulik oppbygging av helsetjenesten og ulikt lovverk som regulerer tilgangsstyring (Åhlfeldt, 2008).

4.0 RESULTAT

I dette kapitlet presenteres funn fra Delphiundersøkelsen og rapporter fra SSHF sin DIPS-database med uttrekk av data som ble brukt til å nominere eksperter til sluttbrukerpanelet, og data som kan belyse utfordringer rundt dagens tilgangsstyring relatert til svarene i Delphiundersøkelsen.

4.1 Presentasjon av funn fra Delphiundersøkelsen

Her presenteres resultatene fra fjerde og siste runde av undersøkelsen hvor respondentene ble bedt om å rangere de viktigste faktorene fra foregående runde. I tabellene er skalaen invertert for lettere å vise rangeringen av faktorene, med de høyest rangerte øverst, og det er beregnet gjennomsnittlig rangering av faktorene som anbefalt av Schmidt, Lyytinen, Keil og Cule (2001). Se evt. vedlegg 5 og 6 for oversikt over alle faktorene som kom frem i undersøkelsen.

4.1.1 Sluttbrukere

4.1.1.1 Spørsmål 1

I hvilken grad anser du følgende utsagn/faktorer som utfordringer i tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-10 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-10, der 1 = viktigst.

Tabell 4 Rangering spørsmål 1 sluttbrukere

Faktor	**Gjennomsnittlig rangering (invertert)**
1. Ikke tilstrekkelig antall/dekkende implisitte beslutningsmaler	7
2. Det mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal	6,92
3. Bruker kan velge feil beslutningsmal	6,31
4. Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang	6
5. Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.	5,69
6. For lite opplæring i tilgangsstyring	5,62
7. Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang	5,46
8. Det kreves for mange tastetrykk for å beslutte seg tilgang	4,46
9. Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket	3,92
10. Når man beslutter tilgang har man automatisk bare tilgang i ett døgn	3,62

Kendall's W = 0,150

4.1.1.2 Spørsmål 2

I hvilken grad tror du følgende utsagn/faktorer kan forbedre tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-9 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-9, der 1 = viktigst

Tabell 5 Rangering spørsmål 2 sluttbrukere

Faktor	**Gjennomsnittlig rangering (invertert)**
1. Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen	6,31
2. Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til	5,92
3. Mulighet for selv å kunne opprette egendefinert beslutningsmal	5,85
4. Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon	5,85
5. Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang	5,31
6. Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn	4,77
7. Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang	3,77
8. Redusere antall klikk som trengs for å beslutte seg tilgang	3,62
9. Den besluttede tilgangen bør automatisk vare i mer enn én dag	3,62

Kendall's W = 0,158

4.1.2 Systemforvaltere

4.1.2.1 Spørsmål 1

I hvilken grad anser du følgende utsagn/faktorer som utfordringer i tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-9 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-9, der 1 = viktigst.

Tabell 6 Rangering spørsmål 1 systemforvaltere

Faktor	**Gjennomsnittlig rangering (invertert)**
1. Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig	6,47
2. Tilgangsstyringen er ikke integrert med personalsystemet	5,67
3. Definering av korrekte tilgangsprofiler	5,2
4. Lite standardisering av tilgangsstyring på tvers av helseforetakene	5
5. Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har	5
6. Det er for dårlig støtte for logganalyse	4,87
7. Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke	4,87
8. Utilstrekkelig funksjonalitet for sperring av journal	4,4
9. Tilpasninger til spesialtilganger er utfordrende for forvaltere	3,53

Kendall's W = 0,086

4.1.2.2 Spørsmål 2

I hvilken grad tror du følgende utsagn/faktorer kan forbedre tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-8 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-8, der 1 = viktigst

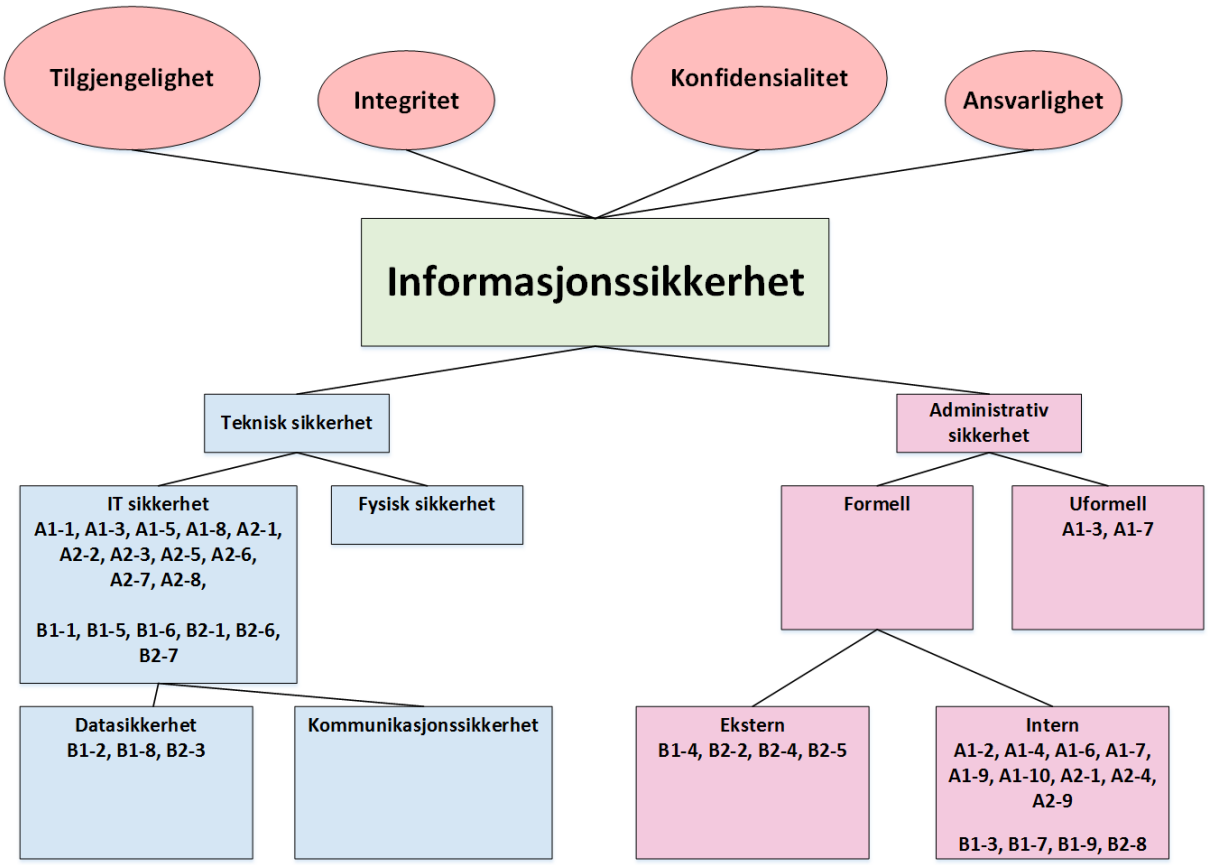
Tabell 7 Rangering spørsmål 2 systemforvaltere

Faktor	**Gjennomsnittlig rangering (invertert)**
1. Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS	5,13
2. Klarere retningslinjer fra nasjonale myndigheter i forhold til hvordan tilgangsstyringen skal legges opp	5,07
3. Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk	5,07
4. Felles retningslinjer for tilgangsstyring på regionalt eller nasjonalt nivå	4,93
5. Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperioder	4,4
6. Bedre oversikt over alt hva en bruker har tilgang til	4,4
7. Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til	3,73
8. Aktiv bruk av innsynslogg for kvalitetssikring	3,27

Kendall's W = 0,080

4.2 Sammenstilling av utfordringer og forbedringsforslag

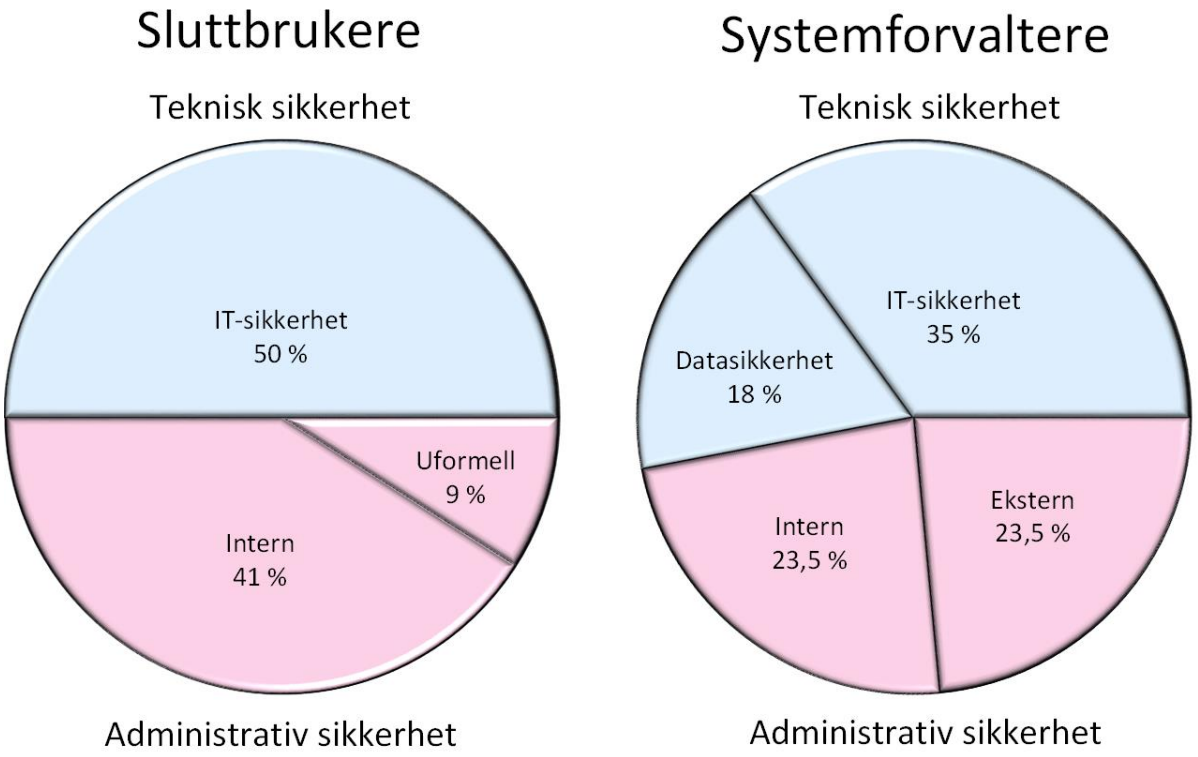
Figur 8 viser InfoSec-modellen med de sammenstilte faktorene for utfordringer og forbedringer av tilgangsstyringen. Bokstav- og nummerkodene i figuren er notert i henhold til ekspertpanel, spørsmål og faktor, hvor A = sluttbruker, og B = systemforvalter (f.eks. viser kode A2-4 til panelet med sluttbrukere, spørsmål 2, faktor 4).



Figur 8 InfoSec-modellen med faktorer fra Delphiundersøkelsen

Enkelte faktorer er plassert i flere bokser, f.eks. faktoren A1-3; «Bruker kan velge feil beslutningsmal». Denne er inkludert i kategorien Uformell, da bruker ved feiltakelse, mangel på kunnskap om hvilken mal som skal velges, eller det kan være en kultur for å velge «den første og beste», selv om bruker vet at aktuell mal ikke samsvarer med årsaken til åpningen av journalen. Faktoren er også inkludert i kategorien Datasikkerhet, da det ideelt sett ikke burde være teknisk mulig for sluttbrukerne å åpne en journal, og oppgi en årsak som ikke er korrekt. Det er ikke identifisert noen faktorer som kan plasseres i kategoriene Integritet, Fysisk sikkerhet, og kommunikasjonssikkerhet. Dette betyr selvsagt ikke at det ikke eksisterer problemer knyttet til disse aspektene, men i denne studien er ingen av de viktigste faktorene rundt tilgangsstyring knyttet til nevnte kategorier i modellen.

For tydeligere å visualisere de to ekspertpanelenes fordeling av faktorer (både utfordringer og forbedringer) i henhold til InfoSec modellen, presenteres faktorene sortert for hvert panel, i figur 9.



Figur 9 Prosentvis fordeling av faktorer per kategori fra InfoSec modellen

Man ser av sektordiagrammene at fordelingen mellom teknisk og administrativ sikkerhet er tilnærmet lik for de to panelene. Forskjellen er i underkategoriene, som viser at bare sluttbrukerne har ansett uformelle faktorer, som f.eks. feil valg av beslutningsmal som en av de viktigste utfordringene. Videre viser figuren at systemforvalterne har oppgitt viktige faktorer under datasikkerhet, som f.eks. logganalyse. I tillegg har de et ønske om mer eksterne (regionale og nasjonale) føringer for tilgangsstyring.

4.3 Rapporter

Ved Sørlandet Sykehus Helseforetak gikk man den 27.10.12 over fra tradisjonell rollebasert tilgangsstyring, til beslutningsstyrt tilgang. Per 27.10.12 var det 6 576 unike antall brukere i

DIPS EPJ ved SSHF. De største gruppene er sykepleiere (2401), leger (731) og sekretærer (588), som til sammen utgjør 56,5 % av det totale antall brukere[10].

Systemansvarlig for DIPS ved SSHF har tatt ut rapporter med anonymisert uttrekk av blålys- og grønnlyslogg. Uttrekkene er for perioden 01.08.13-30.09.13. Disse datoen er fra og med, og til og med. Basert på dette er det mulig å identifisere noen mønstre mht. yrkesgrupper og hyppighet når det gjelder bruk av blålys- og grønnlysfunksjonalitet.

Tabell 8 nedenfor viser de tolv stillingsbetegnelsene som hyppigst må benytte unntaksmekanismer for å få tilgang til journaler. Resterende stillingsbetegnelser er ikke tatt med av anonymitetshensyn. Betegnelsen «annen stilling» i tabellen er også benyttet av anonymitetshensyn.

Tabell 8 Gj.snittl. antall aktualiseringer per stilling i perioden 01.08.13-30.09.13

Stilling	Antall
Fagarbeidere (n=19)	47,1
Konsulent (n=115)	43
Audiograf (n=16)	27,4
Legestudent m/lisens (n=5)	21
Sekretær (n=588)	19,9
Annen stilling (n=1)	17
Rådgiver (n=23)	13
Enhetsleder (n=131)	11,4
Overlege (n=452)	7,6
Lege LIS (n=278)	7
Ingeniør/teknisk stilling (n=4)	6,3
Avdelingsleder (n=32)	5,7

[10] (G. T. Berge, Systemansvarlig DIPS, IKT-avd. SSHF, personlig kommunikasjon, 27. oktober, 2013)

I en periode på to måneder, 01.08.13-30.09.13 er det benyttet unntaksmekanismer i 33577 tilfeller som tabell 9 viser nedenfor.

Tabell 9 Antall journaloppslag per beslutningsmal

Beslutningsmal	Antall journaloppslag
Internkontroll/kvalitetssikring	10031
Henvendelse fra pasientens behandler	6733
Etterarbeide	4844
Bestilling av dokumenter fra offentlige og juridiske instanser og forsikringsselskap	4375
Henvendelse fra pasienten	3091
Meldt pasient	1410
Eksternt prøvesvar/notat til vurdering	1315
Tilsyn på annen avdeling	591
Henvendelse fra pasientens pårørende	512
Forskning	362
Blålys	180
Pasientinnsyn	91
IT-systemarbeid	42
Totalt	33577

5.0 DISKUSJON

I diskusjonen oppsummeres og diskuteres funnene fra resultatkapitlet under hvert forskningsspørsmål, i lys av InfoSec-modellen og tidligere empiri presentert i teorikapitlet. Til slutt i kapitlet diskuteres ulikheter mellom ekspertpanelene, og øvrige funn.

5.1 Utfordringer med tilgangsstyring

5.1.1 Sluttbrukere

Av de viktigste utfordringene sluttbrukerne kom frem til, kan den ene halvparten plasseres i den generelle kategorien IT-sikkerhet, og den andre halvparten i administrativ sikkerhet, hvorav hovedparten i kategorien Intern, under formell administrativ sikkerhet.

De to høyest rangerte utfordringene omhandler mangel på relevante/dekkende implisitte og eksplisitte maler. Manglende implisitte maler er plassert i kategorien Teknisk sikkerhet da de er programmert av leverandør som standard for alle kunder, mens utfordringen med for få eksplisitte maler er plassert i kategorien Intern, da nye eksplisitte maler kan bestilles av kunden (HF-et). Disse to utfordringene henger logisk sammen da mangel på relevante implisitte maler vil si at man ikke automatisk får tilgang til journalen man har behov for, og dermed må beslutte tilgang via grønnlysfunksjonen. Når man så skal få tilgang via grønnlysfunksjonen får man opp en liste med beslutningsmaler, men ut i fra respondentenes svar, burde det vært flere beslutningsmaler, da reel grunn for åpning av journalen ikke alltid finnes i listen de har tilgang til. Disse utfordringene har dermed konsekvenser både for sluttbrukerne, som må bruke tid på unntaksmekanismer for å omgå normal tilgangsstyring, og de av systemforvalterne som skal gjennomgå logger for bruk av unntaksmekanismer. Sluttbrukerne mener også at det er en viktig utfordring at man må beslutte tilgang for ofte. Dette antyder at beslutningsstyrt tilgang slik det er utviklet av DIPS ASA, og slik det er implementert på det aktuelle HF-et ikke i tilstrekkelig grad er skreddersydd til å følge behandlingsprosesser, slik tidligere studier viser (Røstad, 2009). Delphiundersøkelsen forteller bare at respondentene anser dette som en viktig utfordring, men sier ikke noe om i hvilket omfang de må omgå den automatiske tilgangsstyringen. Det kan imidlertid rapporten for bruk av aktualisering ved det aktuelle HF-et si noe om, da det fremgår av den at grønnlysfunksjonen i gjennomsnitt blir brukt mer enn 16 000 ganger per måned (tabell 10) til

åpning av journaler i helseforetaket sluttbrukerne er ansatt i. Dette tallet tilsier at det må være vanskelig å følge opp hendelsesregisteret, noe som samsvarer med en intervjuundersøkelse av Andresen (2010) hvor det framkommer at bruken av unntaksmekanismer er for stor til at man systematisk kan følge dette opp. Når man i tillegg ikke kan stole på at beslutningsmalen som er brukt angir korrekt grunn for åpning av journal må man spørre seg hvilken verdi en logg over dette har. Disse utfordringene er tidligere beskrevet av Røstad (2009) som analyserte hendelsesregister i Siemens DocuLive, for hele Helse Midt-Norge, hvor unntaksmekanismer ble brukt til åpning av 17 % av det totale antallet journaler. Røstad avdekket også manglende predefinerte årsaker for aktualisering, og kom med anbefaling om seks nye aktualiseringsmaler:

• Physician referrals.
• Hand over patient information to other hospital/health personnel on request.
• Request for information from a patient or next of kin.
• Release information to other external entity: insurance, legal, complaints.
• Out-patient clinic patient encounters.
• Patient not registered correctly in admin system (results in access denied, even though patient is physically present at ward).

I DIPS er beslutningsmaler med tilsvarende årsak som de fire øverste av disse inkludert som standard for alle helseforetak som har beslutningsstyrt tilgang (se 2.5.2 og tabell 9), men man har altså fremdeles et behov for flere, ifølge sluttbrukerne. Beslutningsmalene som er tilgjengelig i det aktuelle helseforetaket er del av en «standardpakke» som leveres av DIPS ASA. Som tabell 10 viser, har ikke SSHF andre eksplisitte beslutningsmaler enn de som er standard. Dersom kunden (HF-et) definerer et behov for flere kan dette bestilles, og hvem som evt. skal ha tilgang til aktuell beslutningsmal settes opp iht. HF-et sine interne retningslinjer. Utfordringen med, og en evt. løsning på utfordringen med for få eksplisitte beslutningsmaler anses på bakgrunn av dette å ligge på det interne formelle nivået.

Når aktualiseringsmekanismer benyttes i så stor grad som det gjøres, bør prosessen med å gi seg selv tilgang være enkel og rask. Ut i fra faktor A1-8 «Det kreves for mange tastetrykk for å beslutte seg tilgang» kan det se ut til at dette ikke er tilfelle. Hvor mye tid sluttbrukere bruker på å beslutte tilgang i hvert enkelt tilfelle kan tenkes å variere fra bruker til bruker, ut i fra både ferdigheter, og hvor ofte de må beslutte tilgang, men det bør undersøkes nærmere

hvor mange tastetrykk som trengs for å beslutte tilgang, og om dette er noe leverandøren kan redusere. Sluttbrukeres oppfatning av at unntaksmekanismer for tilgangsstyring opptar for mye tid, og kan være «irriterende» er også beskrevet i tidligere undersøkelser (Faxvaag et al. 2011; Engum, 2008).

Den siste faktoren som går direkte på beslutningsmal er faktor A1-3; «Bruker kan velge feil beslutningsmal». Denne er inkludert i kategorien Uformell, da bruker ved feiltakelse, mangel på kunnskap om hvilken mal som skal velges, eller det kan være en kultur for å velge «den første og beste», selv om bruker vet at aktuell mal ikke samsvarer med årsaken til åpningen av journalen. Faktoren er også inkludert i kategorien Datasikkerhet, da det ideelt sett ikke burde være mulig for brukerne å åpne en journal, og oppgi en årsak som ikke er korrekt, da dette gir dårlig datakvalitet i forhold til oppfølging av hendelsesregister.

De resterende fem faktorene kan plasseres i kategorien Intern, og anses som utfordringer helseforetaket i hovedsak kan påvirke da de kan relateres til opplæring, eller manglende sådan av sluttbrukere. De aktuelle faktorene i rangert orden er:

- Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang
- For lite opplæring i tilgangsstyring
- Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang
- Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket
- Når man beslutter tilgang har man automatisk bare tilgang i ett døgn

Når man beslutter tilgang velger man først en beslutningsmal man har tilgang til, og så kan man om man ønsker, sette inn en fritekstbegrunnelse i tillegg til årsaken malen oppgir. Dette kan være hensiktsmessig som en utdypelse av årsaken til at man har åpnet aktuell journal, og kan beskytte sluttbruker mot evt. mistanke om urettmessig tilegnelse av taushetsbelagte opplysninger ved pasientinnsyn i logg, eller ved tilsyn. Det ser imidlertid ikke ut til at det er kommunisert ut til sluttbrukerne hvordan, og i hvilke tilfeller dette feltet skal brukes. De tre neste faktorene går direkte på at sluttbrukerne oppfatter at de har for lite kunnskap om tilgangsstyring, og derfor har manglende forståelse for bruken av beslutningsstyrt tilgang og lovverket som krever dette for å sikre pasientens personvern. At sluttbrukerne også anser det som en viktig utfordring at man føler man gjør noe ulovlig, er mistrodd og overvåket når man

beslutter tilgang, må også kunne antas å være et resultat av manglende opplæring og kunnskap, da beslutning av tilgang er legitimt når man har behov for det. Det tyder på at sluttbrukerne er for lite kjent med helseforetakets retningslinjer for tilgangsstyring, og ikke er kjent med hvordan hendelsesregisteret forvaltes og kontrolleres, noe som er avdekket i en tidligere studie (Åhlfeldt, 2008).

Den siste av de interne formelle faktorene «Når man beslutter tilgang har man automatisk bare tilgang i ett døgn», kan også tilskrives manglende opplæring og/eller kunnskaper, da hvor mange dager man har tilgang kan justeres av bruker selv.

At det synes å være en mangel på opplæring innen tilgangsstyring, sammenfaller med Åhlfeldt (2008) sine studier av informasjonssikkerhet i helsetjenesten i Norge, Finland og England, som påpeker at det mest neglisjerte området rundt informasjonssikkerhet, er opplæring av brukere (Åhlfeldt, 2008). Helseforetaket som har iverksatt prinsipper og retningslinjer rundt tilgangsstyring, har derfor tilsynelatende ikke kommunisert godt nok ut til sluttbrukerne hvordan de skal sette seg inn i, og forholde seg til disse i praksis.

Det er fire av faktorene som medfører økt tidsbruk for sluttbrukerne; A1-1, A1-5, A1-8, og A1-10. Dette indikerer at økt tidsbruk på grunn av tilgangsstyringsmekanismer er noe som anses som en viktig utfordring for sluttbrukere, og samsvarer med tidligere studier (Faxvaag et al., 2011; Røstad, 2009; Åhlfeldt, 2008).

Man ser fra listen over faktorer i tabell 4 at ingen av faktorene omhandler for «smal» tilgang til pasientopplysninger. Dette kan ha sin årsak i at alle sluttbrukerne har mulighet for aktualisering/beslutte tilgang til en journal de har behov for via grønnlysfunksjonen i DIPS.

5.1.2 Systemforvaltere

Av de viktigste utfordringene systemforvalterne kom frem til, er fem av faktorene relatert til teknisk sikkerhet, og fire til administrativ sikkerhet, og de fleste angår i hovedsak utfordringer rundt tildeling og vedlikehold av tilganger.

Av utfordringer relatert til teknisk sikkerhet finner vi den høyest rangerte faktoren: «Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig». Dette er ikke overraskende da administrasjonsdelen av DIPS ikke har blitt utviklet nevneverdig de siste årene, samtidig som det er arbeidsverktøyet til, og benyttes av de fleste i systemforvalterpanelet. At brukergrensesnittet ikke oppfattes som tilstrekkelig intuitivt og oversiktlig kan sammen med faktor B1-5; «Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har» tenkes å påvirke både personvern og pasientsikkerhet om for mye eller for lite tilganger gis, og man ikke har oversikt over hvilke tilganger en bruker faktisk er tildelt.

Det ser videre ut som om systemforvalterne anser tildeling av tilganger p.t. involverer for mange manuelle rutiner, da den nest høyest rangerte utfordringen er at tilgangsstyringen ikke er integrert med personalsystemet. En slik løsning kan tenkes å redusere, om ikke fjerne, manuell tildeling av tilganger, og således redusere menneskelige feil knyttet til tilgangstildeling. I tillegg vil dette kunne avhjelpe systemforvalterne med utfordringen de opplever med at interne formelle rutiner for bestilling og/eller avslutning av tilgang ikke etterleves (faktor B1-7). Mangel på etterleving av nevnte rutiner kan også tenkes å påvirke både pasientsikkerhet og personvern hvis feil tilgang er bestilt, tilgang ikke er bestilt, evt. for sent bestilt, og tilgang ikke avsluttes når bruker slutter eller ansettes i en annen organisasjonsenhet i samme virksomhet, og beholder tilgang fra tidligere arbeidsforhold.

Systemforvalterne mener at det er for dårlig støtte for logganalyse. Som tidligere nevnt kan hendelsesregistre inneholde et for høyt volum med oppføringer til at man kan gjennomgå all bruk av unntaksmekanismer. Det blir derfor stort sett bare tatt stikkprøver, eller innsynslogger tas ut på profilerte personer, eller innsynslogg utleveres etter ønske fra pasient (Andresen, 2010; Innomed, 2012). Uten en systematisk fremgangsmåte for logganalyse kan man i realiteten ikke oppnå et tilstrekkelig personvern ved utbredt bruk av unntaksmekanismer (Åhlfeldt, 2008). Som nevnt i teoridelen av oppgaven, kan programvare for mønstergjenkjenning benyttes som verktøy for å analysere hendelsesregistre for å avdekke mulige brudd på pasienters personvern, og bruk av dette vil klart være en forbedring fra dagens situasjon hvor det tilsynelatende ikke finnes noen automatikk i dette. Samtidig bør man også vurdere mønstergjenkjenning ut fra et nytte/kost-perspektiv. Pilotstudier har blitt utført, men mønstergjenkjenning er fremdeles ikke i bruk i et produksjonsmiljø innen EPJ i Norge. Den siste pilotstudien, som ble utført ved OUS, analyserte 7,3 millioner

journaloppslag, og av disse ble 29 ansett som mulige tilfeller av urettmessig tilegnelse av taushetsbelagte opplysninger, og håndtert videre av de ansattes klinikkledere (Innomed, 2012). Når man samtidig tar i betraktning at studier angående omfang av urettmessig tilegnelse av taushetsbelagte opplysninger viser at mellom 13,6 og 17,6 % av sluttbrukere har lest taushetsbelagte opplysninger uten faglig grunn (Andresen og Aasland, 2008; Økland et al., 2011), bør det undersøkes nærmere hvorfor mønstergjenkjenningsprogrammet har avdekket så få mulige tilfeller av såkalt snoking. Implementering av mønstergjenkjenning vil også medføre kostander både i innkjøp og drift[11], slik at man må vurdere bruken av dette fra en nytte/kost-perspektiv.

Den siste faktoren som kategoriseres under teknisk sikkerhet er B1-8; «Utilstrekkelig funksjonalitet for sperring av journal». Pasienter har i henhold til lovverket rett til å sperre hele eller deler av sin journal for en eller flere enkeltpersoner, eller for alle iht. Pasient- og brukerrettighetsloven § 5-3 (1999) og Helsepersonelloven § 25 og 45 (1999). Helsepersonelloven § 45 går konkret på tilgang til journal og journalopplysninger og er en pliktbestemmelse som pålegger databehandlingsansvarlig å gi nødvendige helseopplysninger til andre som yter helsehjelp, noe som typisk kan skje vha. tilgangsstyring til opplysninger i EPJ. Dersom pasienten motsetter seg at bestemte opplysninger gis, så må dette resultere i en sperring av de aktuelle opplysningene i EPJ slik at tilgangsstyringen kan ta hensyn til pasientens krav[12]. På hvilken måte funksjonaliteten ikke er tilstrekkelig kommer ikke frem i denne studien, og bør undersøkes videre, da sperring av journal kan medføre en risiko for feil i pasientbehandlingen hvis bruker ikke har tilgang til nødvendig informasjon, eller brudd på pasientens personvern, hvis informasjon ikke i tilstrekkelig grad blir sperret (Åhlfeldt, 2008).

Av utfordringer som kan kategoriseres under administrativ sikkerhet, kom systemforvalterne frem til tre faktorer blant de ni viktigste:

- Definering av korrekte tilgangsprofiler
- Lite standardisering av tilgangsstyring på tvers av helseforetakene
- Tilpasninger til spesialtilganger er utfordrende for forvalterne

[11] (I. Krogstad, Health Care SAS Institute Nordic, personlig kommunikasjon, 26. mars, 2014)
[12] (T. Nystadnes, seniorrådgiver i Helsedirektoratet og forfatter av EPJ-standarden, personlig kommunikasjon, 5. mai, 2014

Definering av korrekte tilgangsprofiler går i hovedsak ut på å sette opp hvilke standardtilganger brukere skal ha. Som det fremgår av InfoSec modellen må man forholde seg til interne og eksterne føringer, i form av lover, regler og forskrifter, og interne retningslinjer for tilgangsstyring. Utfordringen her er å forholde seg til alle disse føringene, og samtidig kunne opprette standardtilganger som ivaretar sluttbrukernes behov for tilgjengelighet til informasjon som skal sikre pasientsikkerheten, samtidig som pasientenes personvern ivaretas. De fleste ekspertene i systemforvalterpanelet jobber med forvaltning på regionalt nivå, og/eller har deltatt i arbeidsgrupper for standardisering av tilgangsstyring på tvers av et regionalt helseforetak. Det er derfor ikke overraskende at lite standardisering av tilgangsstyring på tvers av helseforetakene trekkes frem som en av de viktigste utfordringene. Norges lover og forskrifter, EPJ-standarden og norm for informasjonssikkerhet gjelder for alle helseforetak, men disse gir bare generelle føringer for tilgangsstyring. Prinsipper for tilgangsstyring på tvers av helseforetak i helseregionene har blitt utarbeidet, men disse er også av generell karakter, og ser i liten grad ut til å være harmonisert. Hvert helseforetak er selv ansvarlig for oppsett av tilgangsstyring. Dette kan vi blant annet se i Helse Sør-Øst, hvor OUS skal innføre DIPS høsten 2014, og har valgt å ikke ta i bruk blålys/nødrettstilgang (Oslo universitetssykehus, 2013), da helseforetakene selv kan definere om nødrettstilgang er en nødvendig funksjon[13].

For systemforvalterne som drifter tilgangsstyring på tvers av helseforetak er det derfor klart at det kan være en utfordring å forholde seg til hvert helseforetak sitt særegne oppsett, og retningslinjer for tilgangsstyring. Det virker også uheldig at standardiseringen bare har foregått på et regionalt, og ikke nasjonalt nivå. Direkte tilgang til journalopplysninger på tvers av virksomheter er fremdeles lovstridig, men med stortingsmeldingen «Én innbygger – én journal» (St. meld nr. 9 (2012-2013), og utredningen av ny helseregisterlov og pasientjournallov ser det ut til at det vil åpnes opp for dette (Prop. 72 L, 2013-2014). Om tilgangsstyringen vil være slik den er i dag, vet man ikke da løsningsalternativ ikke er utredet, men det virker noe tungrodd og lite ressursvennlig at hvert regionale helseforetak skal utarbeide sine standarder, når det om noen år kan bli nasjonale retningslinjer som det er krav om at må følges.

[13] (K. J. Loe, prosjektleder Regional standardisering klinisk dokumentasjon, personlig kommunikasjon, 16. september, 2013)

Samtidig er det klart at ikke alt kan standardiseres, hverken nasjonalt, regionalt eller lokalt, og målet med tilgangsstyring er heller ikke å gjøre jobben lett for dem som skal administrere dette, men å ivareta pasienters personvern. Det kan derfor være tilfeller hvor lokale tilpasninger må gjøres, og spesialtilganger må gis til enkeltansatte som har behov for dette i sitt arbeid. Den siste faktoren «Tilpasninger til spesialtilganger er utfordrende for forvalterne» setter søkelys på dette, og er en faktor det kan være hensiktsmessig å undersøke nærmere i videre studier. Dette for å klargjøre hvilke momenter som gjør det vanskelig å tilpasse spesialtilganger, det være seg administrative og/eller tekniske utfordringer.

5.2 Potensielle forbedringer

5.2.1 Sluttbrukere

Av mulige forbedringer sluttbrukerne anser som de viktigste, er hovedvekten (syv av ni faktorer) kategorisert under teknisk sikkerhet, og gås derfor gjennom først. Den høyest rangerte faktoren «Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen» er kategorisert både under teknisk og administrativ sikkerhet da både leverandør og helseforetak må ta stilling til dette. Etter kontakt med sluttbruker for utdyping av problemet som ligger bak forbedringsforslaget, bunner det ut i at journaldokumenter i DIPS er tilknyttet elektroniske henvisninger, og da ansatte i somatiske avd. ikke har tilgang til psykiatriske journaldokumenter, får mottaker åpnet den elektroniske henvisningen, men ikke det tilknyttede journaldokumentet, som kan inneholde nødvendig informasjon for behandler. For å omgås dette problemet er rutinen i dag at journaldokumentene manuelt sendes elektronisk til mottakers arbeidsgruppe i DIPS, slik at en implisitt beslutningsmal (Dokument i arbeidsflyt) aktiveres, og mottaker får da tilgang til dokumentet, selv om sluttbruker i utgangspunktet ikke har tilgang til denne journalgruppen. Å skulle gi tilgang til psykiatriske journaldokumenter vil løse problemet slik at de ansatte i somatiske avd. får tilgang, men er kanskje ikke en løsning som ivaretar personvernet da man på generelt grunnlag vil få tilgang til én eller flere typer psykiatriske journaldokumenter. Denne faktoren viser at definering av regler og standarder kan bli mer komplekse enn designet av tekniske systemer tillater (Åhlfeldt, 2008). Her er det forfatters oppfatning at leverandør og kunde sammen bør komme frem til en løsning som ikke baserer seg på manuelle rutiner som kan bli glemt, men en

løsning som automatisk gir tilgang til henvisningens tilknyttede journaldokumenter, slik at personvern og pasientsikkerhet blir ivaretatt.

De resterende seks faktorene under teknisk sikkerhet går i hovedsak ut på brukervennlighet, og kan karakteriseres som svar på utfordringene som ble avdekket av sluttbrukerne under spørsmålet om utfordringer. Dette gjelder f.eks. reduksjon av antall klikk som trengs for å beslutte tilgang, og inkludere eksempler for bruk av fritekstfelt ved manuell beslutning av tilgang. En faktor det imidlertid kan være interessant å bemerke seg er A2-5; «Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang». Det er delvis mulig å sette opp hva hver enkelt beslutningsmal skal kunne gi tilgang til, men tilgangsstyringen er implementert på det aktuelle HF-et slik at man i all hovedsak får tilgang til akkurat de samme pasientopplysninger ved bruk av eksplisitt, som ved implisitt tilgang. Det kan se ut som sluttbrukerne etterspør en enda mer finkorning av tilgangsstyringen ved at man f.eks. etter å ha valgt aktuell beslutningsmal, velger hva slags pasientinformasjon man ønsker å få tilgang til. Dette kan tenkes å være aktuelt hvis man f.eks. får en henvendelse fra pasientens behandler om hvilke medisiner hun eller han står på, og sluttbruker kan da beslutte tilgang til kun pasientens medikasjon. En slik funksjonalitet vil kunne ivareta pasientens personvern på et dypere plan enn dagens tilgangsstyring muliggjør. Samtidig må man ta i betraktning at innføring av en slik funksjonalitet vil medføre et betydelig kartleggings- og implementeringsarbeid for virksomheter som evt. vil ta dette i bruk.
De to unike faktorene under administrativ sikkerhet går på opplæring av brukere i tilgangsstyring og rutiner rundt dette. Faktor A2-9; «Den besluttede tilgangen bør automatisk vare i mer enn én dag» ses som et svar på faktor A1-10 «Når man beslutter tilgang har man automatisk bare tilgang i ett døgn», og kan som tidligere nevnt tilskrives manglende opplæring og/eller kunnskaper, da hvor mange dager man har tilgang kan justeres av bruker selv. En forbedring av denne utfordringen tolkes da til å fordre bedre opplæring av sluttbrukere, heller enn tekniske virkemidler.

5.2.2 Systemforvaltere

Av mulig forbedringer systemforvalterne anser som de viktigste, kan den ene halvparten kategoriseres under teknisk sikkerhet, og den andre under administrativ sikkerhet.

Under teknisk sikkerhet går to av faktorene (B2-1 og B2-6) på ønske om økt brukervennlighet angående tildeling og vedlikehold av tilganger, og henger naturlig sammen med tidligere nevnte utfordringer ang. dette (B1-1 og B1-5). Økt brukervennlighet kan tenkes å påvirke både personvern og pasientsikkerhet om brukergrensesnittet kan gjøres enklere og mer oversiktlig slik at man muligens kan redusere omfanget av feil tilganger som skyldes menneskelig svikt ved opprettelse og vedlikehold av tilganger. Faktor B2-3; «Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk», kan i enda større grad redusere menneskelig svikt ved opprettelse av brukertilganger, da alle standardtilganger kan gis automatisk når brukers leder registrerer den ansatte i personalsystemet. En slik løsning skal etter planen tas i bruk i OUS høsten 2014 (DIPS, 2013). Forhåpentligvis kan dette forenkle brukeradministrasjonen, og dermed tenkes å ha en ressursmessig gevinst, ved at ledere kan bruke mindre tid på å bestille og melde fra om avslutning av tilganger, og systemforvalterne kan bruke mindre tid på opprettelse og stenging av tilganger. Et viktigere poeng, sett fra et informasjonssikkerhetsperspektiv, er at dersom en slik integrasjon fungerer, vil den ha en positiv effekt på både pasientsikkerhet og personvern. Da vil man som nyansatt automatisk ha de riktige tilgangene i EPJ-et, og når man slutter vil tilgangene opphøre.

Det siste forbedringsforslaget under teknisk sikkerhet viser at de fleste av systemforvalterpanelet også forholder seg til brukersiden av DIPS. Faktor B2-7; «Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til» er den eneste faktoren både sluttbruker- og systemforvalterpanelet anser som blant de viktigste. En slik forbedring vil spare brukere for unødvendig tidsbruk, og ansvaret for gjennomføring av en slik endring ligger naturlig nok hos leverandør.

Av de fire forbedringsforslagene som kategoriseres under administrativ sikkerhet er tre av fire faktorer (B2-2, B2-4 og B2-5) i underkategorien formell ekstern, og disse faktorene viser at systemforvalterne tydelig ønsker en mer overordnet regional og nasjonal styring av hvordan tilgangsstyringen skal settes opp. Disse faktorene kan ses som et tilsvar til faktor B1-4 «Lite standardisering av tilgangsstyring på tvers av helseforetakene. Dette komme av at respondentene mener at hvert enkelt helseforetak ikke har forutsetninger for å ivareta tilgangsstyring iht. gjeldende lover og regler, da en kommentar fra Delphiundersøkelsen påpeker dette. I tillegg kan disse faktorene forklares med at flere av de regionale

helseforetakene har som målsetning å konsolidere EPJ-databasene sine, slik at det blir én database per regionale helseforetak for å imøtekomme visjonen Én innbygger – én journal, og realisere gevinster i form av forenkling av drift (Andersen, 2013; Finborud, 2014).
Den siste faktoren, B2-8; «Aktiv bruk av innsynslogg for kvalitetssikring» viser at systemforvalterne er opptatt av pasientens personvern, og samtidig ser at det er hensiktsmessig å forbedre bruken av hendelsesregister for å kvalitetssikre at sluttbrukerne ikke misbruker den tillit de er gitt, ved å urettmessig tilegne seg taushetsbelagte opplysninger.

5.3 Sammenlikning av panel og øvrig diskusjon

I dette underkapitlet vil enkelte ulikheter mellom ekspertpanelene diskuteres, i tillegg til øvrige momenter som ikke har sin naturlige plass i de foregående underkapitlene.

Figur 8, som er en sammenstilling av alle faktorene (både utfordringer og mulige forbedringer) for sluttbrukere og systemforvaltere, viser at de to panelene har en tilnærmet lik fordeling av faktorer under administrativ og teknisk sikkerhet, men den videre fordelingen i underkategorier viser tydelige ulikheter. Under administrativ sikkerhet er det bare sluttbrukerne som har uformelle faktorer som f.eks. manglende forståelse for bruken av beslutningsstyrt tilgang, med blant de viktigste faktorene. Samtidig er det bare systemforvalterne som har med eksterne faktorer, som f.eks. standardisering av tilgangsstyring på tvers av helseforetak. Videre er det kun systemforvalterne som har kommet med faktorer som iht. InfoSec-modellen kan kategoriseres som datasikkerhet, som kan eksemplifiseres i faktoren for integrasjon mellom personalsystem og EPJ for sikring av opprettelse og stenging av tilganger.

Dette, sammen med de andre faktorene, viser at både sluttbrukere og systemforvaltere i hovedsak er opptatt av faktorer som påvirker dem i det daglige. Sluttbrukerne er eksperter i selve bruken av tilgangsstyring, mens systemforvalterne er eksperter på administrasjonen av den. For at tilgangsstyring skal fungere bør det derfor være en god kommunikasjon mellom disse to gruppene på et lokalt, regionalt og nasjonalt plan (Åhlfeldt, 2008). Dette er spesielt viktig å tenke på når man går inn i en periode med økt fokus på standardisering av EPJ, og herunder tilgangsstyring på regionalt og muligens nasjonalt plan.

Sluttbrukerne anså manglende beslutningsmaler som en viktig faktor, uten at systemforvalterne gjorde det samme. Som tidligere nevnt kan nye maler bestilles av leverandør. For at nye maler skal bestilles, så må imidlertid noen faktisk bestille disse, og denne myndigheten ligger hos systemforvalterne. Det kan derfor se ut til at mangel på maler ikke kommuniseres til systemforvalterne. Dette virker svært uheldig da det resulterer i at brukere i visse situasjoner er nødt til å registrere uriktig årsak til åpning av journal, da det i DIPS ikke eksisterer en egen beslutningsmal for «andre årsaker», slik det gjør i DocuLive EPJ (Røstad, 2009).

Sluttbrukerne i Delphiundersøkelsen ønsker mulighet for å opprette egendefinerte beslutningsmaler (faktor A2-3). Selv om målet bør være minst mulig bruk av unntaksmekanismer, kan et slikt alternativ tenkes å være nyttig da systemforvalterne, eller andre i helseforetaket kan ta ut logg for bruken av dette. Loggen kan gjennomgås, og man kan kanskje være proaktive, og sørge for at ofte brukte årsaker kan bestilles som ny beslutningsmal hos leverandør, og tildeles de som har behov for malen slik Røstad (2009) delvis gjorde i sin studie av hendelsesregister for aktualisering.

I løpet av en periode på to måneder ble aktualisering/grønnlysfunksjonen benyttet 33397 ganger, mens nødrettstilgang/blålys bare ble brukt 180 ganger (tabell 10). I tillegg var det ingen av de viktigste faktorene som omhandler at man blir direkte hindret i pasientbehandlingen som følge av begrenset tilgang, og ingen av ekspertene mener at for vide tilganger er av de viktigste utfordringene med tilgangsstyring, selv om dette kom frem som en faktor fra en sluttbruker i første runde. Det kan tenkes at dette har sin årsak i at sluttbrukerne ved grønnlysfunksjonen i hovedsak får tilgang til det de har behov for. Dette samsvarer med en tidligere studie av Røstad (2009).

Som tidligere nevnt bør det være en målsetning å redusere bruken av unntaksmekanismer. Ut fra tabell 10 som viser hvilke predefinerte årsaker brukere har benyttet når de har besluttet seg tilgang, går en rekke av dem ut på utlevering av opplysninger til behandler, offentlige instanser, og henvendelser fra pasienten selv, samt pårørende. Tilgang på tvers av virksomheter og pasientens tilgang til egen journal er utenfor denne oppgavens omfang, men som man ser, påvirker mangel på tilgang på tvers av virksomheter og pasientens tilgang til egen journal tilgangsstyringen i en virksomhets EPJ, da det fører til økt bruk av unntaksmekanismer, som i prinsippet er uønsket.

6.0 KONKLUSJON

Dette er en studie av tilgangsstyringen i det dominerende EPJ-et som benyttes i spesialisthelsetjenesten i Norge. Å utføre denne studien av eksisterende tilgangsstyring var nødvendig for å forstå svakhetene med, og mulige forbedringer av hvordan beslutningsstyrt tilgangsstyring er implementert og i bruk i dag, sett fra både sluttbrukere og systemforvalteres ståsted.

Litteraturen viser at tilgangsstyring i EPJ er problematisk da man både må ta hensyn til pasientsikkerhet og pasientens personvern, som har gitt utslag i at vide tilganger har blitt gitt, tilgangsstyringen har vært for statisk ved at det er organisasjonstilhørighet som i hovedsak gir tilgang til en journal, og ikke en beslutning om helsehjelp. Det har i tillegg vært for høyt volum av tildeling og bruk av unntaksmekanismer som genererer lange innsynslogger, som i for liten grad blir fulgt opp.

Beslutningsstyrt tilgang er innført i en rekke av landets helseforetak, og vil snart være innført i alle, men en rekke av utfordringene som er avdekket i tidligere studier, er fremdeles tilstede. Tilgangsstyringen er ikke tilstrekkelig skreddersydd til å følge behandlingsprosesser, som fører til at sluttbrukerne må bruke unntaksmekanismer for å få tilgang man antar de har rettmessig behov for.

De predefinerte årsakene sluttbrukerne må oppgi når de benytter unntaksmekanismer er fremdeles ikke alltid dekkende for reel grunn for åpning av journal. Dette kan føre til at feil begrunnelse velges, slik at man ikke kan stole på årsaken for åpning av journalen i hendelsesregisteret for unntaksmekanismer. Bruk av hendelsesregister for avdekking av urettmessig tilegnelse av taushetsbelagte opplysninger er dessuten usystematisk, og verktøy som kan avhjelpe dette, f.eks. mønstergjenkjenning benyttes fremdeles ikke.

Både sluttbrukerne og systemforvalternes svar viser også at det foreligger mangler innen helseforetak sin etterleving av interne retningslinjer, og opplæring av sluttbrukere i forhold til tilgangsstyring.

I tillegg oppfattes aktualiseringsmekanismene som tungvinte av sluttbrukerne, og de ønsker at å tildele seg tilgang skal kunne utføres raskere og enklere.

Pasientsikkerheten ser ut til å være ivaretatt, da ingen av faktorene som anses som viktigst av sluttbrukerne omhandler mangel på tilgang til opplysninger de har behov for. Dette kan ha sin årsak i at man har muligheten for aktualisering ved hjelp av grønnlysfunksjonen, som innebærer at sluttbrukerne kan tildele seg selv tilgang til en journal de i utgangspunktet ikke har automatisk tilgang til.

Delphiundersøkelsen har også avdekket faktorer som tidligere studier ikke har avdekket.
For bedre å kunne ivareta pasientsikkerhet og pasienters personvern, bør brukergrensesnittet for både sluttbrukere og systemforvaltere bli mer brukervennlig.

På bakgrunn av teori, Delphiundersøkelsen og uttrekkene fra EPJ-databasen har følgende administrative og tekniske utfordringer og mulige forbedringer blitt belyst iht. de to hovedkategoriene administrativ og teknisk sikkerhet fra InfoSec-modellen:

Utfordringer innen administrativ sikkerhet:

- For lite kunnskap om, og forståelse for tilgangsstyring
- Rutiner for bestilling og stenging av tilganger etterleves ikke
- Manglende formidling av behov for nye beslutningsmaler
- Tilgangsstyring er satt opp ulikt på hvert helseforetak

Utfordringer innen teknisk sikkerhet

- Tilgangsstyringen er for lite skreddersydd ift. pasientforløp
- Tidkrevende og tungvint å beslutte tilgang
- For mye bruk av unntaksmekanismer

Forbedringer innen administrativ sikkerhet

- Opplæring av sluttbrukere i tilgangsstyring
- Kommunikasjon mellom sluttbrukere og systemforvaltere for avklaring av behov for nye beslutningsmaler
- Standardisering av tilgangsstyring på regionalt og nasjonalt nivå

Forbedringer innen teknisk sikkerhet

- Tilgangsstyringen bør knyttes mer opp mot behandlingsprosesser ved å få utviklet flere implisitte beslutningsmaler
- Systematisk oppfølging av hendelsesregistre, evt. ved bruk av mønstergjenkjenning
- Enklere grensesnitt for sluttbrukere ved bruk av unntaksmekanismer

- Enklere grensesnitt for systemforvaltere ift. tildeling og vedlikehold av tilganger
- Integrasjon mellom personalsystem og EPJ for automatisk opprettelse og stenging av brukertilganger

InfoSec-modellen har vært nyttig til å visualisere på hvilke områder utfordringer og forbedringer av tilgangsstyring kan plasseres, og viser at både administrative og tekniske utfordringer eksisterer. Både leverandør (DIPS ASA), kunde (helseforetak) og regionale (RHF) og nasjonale myndigheter har ansvar for en forbedring av de ulike utfordringene med tilgangsstyring Delphiundersøkelsen og uttrekkene fra EPJ-databasen har oppfanget. Det er iht. InfoSec-modellen essensielt at alle deler av modellen hvor utfordringer er avdekket må følges opp, for å oppnå informasjonssikkerhet i EPJ. Administrative tiltak både i og utenfor virksomheten som benytter et EPJ, må være utformet på en gjennomførbar måte, og de må videre etterleves ved hjelp av velfungerende tekniske sikkerhetstiltak.

6.1 Videre arbeid

Å bare utføre en Delhistudie (dog sammen med noe uttrekk fra EPJ-database) har sine begrensninger. En videreføring av arbeidet som er gjort i denne oppgaven kan være å triangulere funnene ved å supplere med dybdeintervju, og utførelse av en spørreundersøkelse på bakgrunn av funnene etter Delphiundersøkelsen. Intervju kan gi klarhet i detaljer rundt de av faktorene som ikke spesifikt beskriver hva som er den reelle utfordringen, f.eks. utfordringer rundt sperring av journal. Delphiundersøkelsen forteller *hvilke* faktorer som anses som viktige av ekspertene, men den sier ikke noe om i hvilket *omfang* en utfordring er et problem. På bakgrunn av Delphiundersøkelsen (og evt. intervju) kan man utforme spørreskjema som kan besvare i hvilket omfang utfordringene eksisterer, og forbedringsforslagene anses som nyttige.

Det kan med fordel også tas ut flere spørringer fra flere EPJ-databaser for å kartlegge bruk av unntaksmekanismer, da ulike virksomheter kan ha satt opp tilgangsstyring ulikt. Det kunne også vært interessant å få ut data for i hvor stor grad spesialtilganger gis sluttbrukere, altså tilganger som avviker fra det som er vanlig for ansatte ved en post eller poliklinikk osv. Dette kan bidra til å forklare faktorene i Delphiundersøkelsen som går på at tildeling av spesialtilganger er utfordrende, dersom det skjer i et stort omfang. Det kan også si noe om i

hvilken grad virksomheten har lykkes med å definere standardtilganger, og hvor lett det vil la seg gjøre å evt. implementere integrasjon mellom personalsystem og EPJ for automatisk tildeling av tilganger.

Stortingsmelding nr. 9 (2012-2013) "Én innbygger – én journal", har som mål å gjøre klinisk informasjon tilgjengelig på tvers av sted og omsorgsnivå. Dette vil sette nye krav til dagens EPJ-plattform med tanke på blant annet tilgangsstyring og endring av lovverk. Det kan derfor være av nytte å undersøke hvordan tilgangsstyring skal understøtte visjonen om én felles journal.

REFERANSER

Alemán JL, Señor IC, Lozoya PA, Toval A. (2013) Security and privacy in electronic health records: a systematic literature review. *J Biomed Inform, 46*(3), 541-562. doi: http://dx.doi.org/10.1016/j.jbi.2012.12.003

Andresen, H. (2010). *Tilgang til og videreformidling av helseopplysninger* (Doktorgradsavhandling, Universitetet i Oslo). Hentet fra https://www.duo.uio.no/bitstream/handle/10852/19000/HerbjoernAndresenAvhandling.pdf?sequence=1

Andresen, H. og Aasland, O. G. (2008). Helsepersonells håndtering av pasientopplysninger. *Tidsskrift for den Norske legeforening, 128*(24), 2823 – 7. Hentet fra http://tidsskriftet.no/article/1781321

Andresen, Ø. (2013) *Moglegheiter for kvalitetsregister gjennom ny IKT*. Hentet fra http://www.helse-bergen.no/fagfolk/forskning/Documents/kvalitetsregisterkonferansen%202013-%20postere%20foredrag/Registerkonferanse2013%20%C3%98rjan%20Andersen.pdf

Dalkey, N., og Helmer, O. (1962) *An Experimental Application of the Deplhi Method to the use of Experts*. Hentet fra http://www.rand.org/content/dam/rand/pubs/research_memoranda/2009/RM727.1.pdf

Datatilsynet, (2008) *Personvernrapporten 2008*. Hentet fra http://www.datatilsynet.no/Global/04_planer_rapporter/Personvernrapport/Personvernrapporten%202008.pdf

Datatilsynet (2009). *Sviktende tilgangsstyring i elektroniske pasientjournaler?* Hentet fra http://www.datatilsynet.no/Global/05_tilsynsrapporter/2009/Tilsynsrapport_tilgangskontroll_pasientjourn_20090427.pdf

DIPS (2011) *Prosjekt Felles EPJ Førde*. Hentet 10.03.2014, fra http://www.dips.no/nor/kundecase/?&displayitem=459&module=news

DIPS (2013) *Forenklet brukeradministrasjon*. Hentet 27.04.13, fra http://dips.mediabok.no/113/index.html#14/z

Ellingsen, G., og Monteiro, E. (2012). Electronic patient record development: the case for an evolutionary strategy. *Health Policy and Technology* doi: 10.1016/j.hlpt.2012.01.007

Engum, A. (2008). Bruk av aktualisering. Hentet fra http://www.kith.no/upload/4543/anette-engum.pdf

European Court of Human Rights. (2008). *CASE OF I v. FINLAND*. (Application no. 20511/03). Hentet fra http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87510

Faxvaag, A., Johansen, T. S., Heimly, V., Melby, L., og Grimsmo, A. (2011) Healthcare Professionals' Experiences With EHR-System Access Control Mechanisms. *Studies in Health Technology and Informatics, (169)*, 601-605.

Ferraiolo, D. F., og Kuhn, D. R. (1992) *Role-Based Access Controls*. Hentet fra http://csrc.nist.gov/groups/SNS/rbac/documents/Role_Based_Access_Control-1992.html

Ferreira, A., Cruz-Correia, R., Antunes, L., og Chadwick, D. (2007) Access control: how can it improve patients' healthcare? *Studies in health technology and informatics*, 127:65-76. Hentet fra: http://www.ncbi.nlm.nih.gov/pubmed/17901600

Finborud, I. M. (2014) *Prosjekter gjennom tidene – hva har vi lært?* Hentet fra http://www.nasjonalikt.no/filestore/Arrangementer/Prosjektledersamling_2014/IngerM.Finborud_ProsjektarbeidiHelseSrst.pdf

Førde, R. (2013) *Helsinkideklarasjonen.* Hentet 25.04.2014, fra http://www.etikkom.no/FBIB/Praktisk/Lover-og-retningslinjer/Helsinkideklarasjonen/

Gracht, H. A. (2012) Consensus measurement in Delphi studies: Review and implications for future quality assurance. *Technological Forecasting & Social Change*, *79*, 1525–1536 doi: http://dx.doi.org/10.1016/j.techfore.2012.04.013

Grimsmo, A. (2007) *Medisinskfaglig analyse av behovet for enklere kommunikasjon i tilknytning til bruken av elektronisk pasientjournal*. Hentet fra http://www.nsep.no/publikasjoner/Analyse%20av%20behovet%20for%20enklere%20kommunikasjon_5.pdf

Helsedirektoratet (2013) *Norm for informasjonssikkerhet*. Hentet fra http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Documents/Norm%20for%20informasjonssikkerhet%20i%20helse-%20omsorgs-%20og%20sosialsektoren.pdf

Helsedirektoratet (2014) *Nasjonalt fag- og arkitekturutvalg Møteinnkalling, Revisjon av EPJ standarden.* Hentet fra http://helsedirektoratet.no/it-helse/ehelse/fag-og-arkitekturutvalg/moter/Documents/Dagsorden.pdf

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

Helseregisterloven (2001). Lov om helseregistre og behandling av helseopplysninger. Hentet fra http://lovdata.no/dokument/NL/lov/2001-05-18-24?q=helseregisterloven

Helsetilsynet. (2008). *Mangelfull tilgangsstyring til elektronisk pasientjournal truer taushetsplikten i sykehus*. Hentet fra http://www.helsetilsynet.no/no/Publikasjoner/Brev-hoeringsuttalelser/Brev-hoeringsuttalelser-2008/Tilgangsstyring-pasientjournal-truer-taushetsplikten-sykehus/

Helse Sør-Øst, (2014) *Tidsplan klinisk dokumentasjon.* Hentet 10.03.2014, fra http://www.helse-sorost.no/aktuelt/digitalfornying/Documents/Tidsplan/Tidsplan%20klinisk%20dokumentasjon%20mars2014.pdf

Hsieh, H.F. & Shannon, S.E. (2005) Three Approaches to Qualitative Content Analysis. *Qualitative Health Research, 15*(9), s. 1277-1288 doi: 10.1177/1049732305276687

Innomed (2012). Mønstergjenkjenning som metode for å oppdage taushetspliktbrudd ved bruk av pasientjournal: «Mønstergjenkjenningsprosjektet» Hentet fra http://www.innomed.no/media/media/prosjekter/rapporter/56_-_Monstergjenkjenning.pdf

Innomed (u. å.). Mønstergjenkjenning av journallesing for å oppdage misbruk og tilpasse tilganger. Hentet fra http://www.innomed.no/nb/prosjektoversikt/systemet-fra-innsiden/mnstergjenkjenning-av-journallesing-for-a-oppdage-/

Johannesen A., Tufte P.A., og Kristoffersen L. (2010). *Introduksjon til samfunnsvitenskaplig metode*. Oslo: Abstrakt forlag

Kallbekken, S. (2014). *Innføring av én pasientjournal ved helseforetakene i nord*. Hentet 10.03.2014, fra http://www.helse-nord.no/aktuelt-om-fiks/stafettpinnen-overlevert-til-helgelandssykehuset-article112045-32197.html

KITH, (2001) *Elektronisk pasientjournal standard. Arkitektur, arkivering og Tilgangsstyring. Del I: Funksjonsrettet beskrivelse.* Hentet fra http://www.kith.no/upload/1364/EPJ-HS-del1-v1.pdf

KITH (2010). *Grunnleggende EPJ-standard*. Tilgjengelig fra http://www.kith.no/templates/kith_WebPage____3351.aspx

Kvale, S., og Brinkmann, S. (2009). *Det kvalitative forskningsintervju* (2. utg.). Oslo: Gyldendal Akademisk

Nasjonal IKT (2013). Styringsgruppemøte 5. juni 2013. Hentet 21.03.2014 fra http://www.nasjonalikt.no/no/nyheter/

NOU 2006: 5 (2006). *Norsk helsearkiv – siste stopp for pasientjournalene.* Hentet fra http://www.regjeringen.no/nb/dep/hod/dok/nouer/2006/nou-2006-05/7/5/2.html?id=157267

Norges teknisk-naturvitenskapelige universitet. (2014) *Hovedside iAccess.* Hentet 02.03.2014, fra http://iaccess.idi.ntnu.no/index.php/Main_Page

Nystadnes, T. (2007) EPJ Standard del 2: Tilgangsstyring, redigering, retting og sletting Vol. 6/05, 2007. *KITH-rapport.* Hentet fra http://www.kith.no/upload/3985/R06-05_EPJ2-Del2-Tilgangsstyring-v1.pdf

Okoli, C., og Pawlowski, S. D. (2004). The Delphi method as a research tool: an example, design considerations and applications. *Information & Management, 42*(1), 15-29. doi: http://dx.doi.org/10.1016/j.im.2003.11.002

Oslo universitetssykehus (2013) Prinsipper for tilgangsstyring av EPJ. Hentet 12.03.2014, fra http://ehandbok.ous-hf.no/Modules/Module_136/maincontent_fs.aspx?url=view_document.aspx&documentId=37667

Pasient- og brukerrettighetsloven (1999) Lov om pasient og brukerrettigheter. Hentet fra http://lovdata.no/dokument/NL/lov/1999-07-02-63?q=pasientrettighetsloven

Personopplysningsforskriften (2000) Forskrift om behandling av personopplysninger. Hentet fra http://lovdata.no/dokument/SF/forskrift/2000-12-15-1265

Prop. 72 L, 2013-2014 (2014) *Pasientjournalloven og helseregisterloven*. Hentet fra http://www.regjeringen.no/nb/dep/hod/dok/regpubl/prop/2013-2014/Prop-72-L-201320141.html?id=756657

Rogstad, K. (2011). *Kontroll av logger fra behandlingsrettede helseregistre*. (Mastergradsavhandling, Universitetet i Oslo). Hentet fra https://www.duo.uio.no/bitstream/handle/10852/19388/117525.pdf?sequence=4

Rowe, G. Wright, G. (2001) *Expert opinions in forecasting: the role of the Delphi technique*. Hentet fra http://www.gwern.net/docs/predictions/2001-rowe.pdf

Røstad, L. (2009) *Access Control in Healthcare Information Systems*. (Doktorgradsavhandling, Norges teknisk-naturvitenskapelige universitet) Hentet fra http://www.idi.ntnu.no/~lilliaro/docs/lr_phd_final.pdf

Schmidt, R. (1997). Managing Delphi surveys using nonparametric statistical techniques. *Decision Sciences,*
28(3), 763-774. Doi: 10.1111/j.1540-5915.1997.tb01330.x

Schmidt, R., Lyytinen, K., Keil, M., og Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems, 17*(4), 5 - 36. Hentet fra http://www.cs.usyd.edu.au/~isys3207/readingsondesign/identifyingprojectrisk.pdf

Skulmoski, G. J., Hartman, F. T., og Krahn, J. (2007) The Delphi Method for Graduate Research. *Journal of Information Technology Education*, vol. 6, s 1-21. Hentet fra http://www.jite.org/documents/Vol6/JITEv6p001-021Skulmoski212.pdf

St. meld nr. 9 2012-2013 (2013). *Én innbygger – én journal* [Oslo]: Helse- og omsorgdepartmenetet. Hentet fra http://www.regjeringen.no/nb/dep/hod/dok/regpubl/stmeld/2012-2013/meld-st-9-20122013.html?id=708609

Strømmen, E.M. (2013) *Elektronisk tilgang på tvers for klinisk informasjon i spesialisthelsetjenesten - Forslag til arkitektur* (Mastergradsavhandling, *Norges teknisk-naturvitenskapelige universitet)*, Hentet fra: http://www.diva-portal.org/smash/record.jsf?pid=diva2:663111

Wester, A. (2007). *Elektroniska patientjournaler – inre sekretess och gränserna för åtkomst.* Hentet fra https://gupea.ub.gu.se/bitstream/2077/3339/1/200732.pdf

Økland, S., Haumann, K., og Christiansen, R. S., (2011). *Urettmessig tilegnelse av taushetsbelagte opplysninger fra kliniske IT-systemer* **(**Masteroppgave, Universitetet i Agder). Hentet fra http://brage.bibsys.no/xmlui/bitstream/handle/11250/138585/HSI500-G_2011_v%c3%a5r_Masteroppgave_Solveig%20%c3%98kland.pdf?sequence=1

Åhlfeldt, R. M. (2008) *Information Security in Distributed Healthcare: Exploring the Needs for Achieving Patient Safety and Patient Privacy* (Doktorgradsavhandling, Stockholms universitet. Hentet fra http://www.diva-portal.org/smash/get/diva2:198213/FULLTEXT01.pdf

Vedlegg 1 Meldeskjema NSD

MELDESKJEMA

Meldeskjema (versjon 1.4) for forsknings- og studentprosjekt som medfører meldeplikt eller konsesjonsplikt (jf. personopplysningsloven og helseregisterloven med forskrifter).

1. Prosjekttittel		
Tittel	Tilgangsstyring av elektronisk pasientjournal -En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer	
2. Behandlingsansvarlig institusjon		
Institusjon	Universitetet i Agder	Velg den institusjonen du er tilknyttet. Alle nivå må oppgis. Ved studentprosjekt er det studentens tilknytning som er avgjørende. Dersom institusjonen ikke finnes på listen, vennligst ta kontakt med personvernombudet.
Avdeling/Fakultet	Fakultet for helse- og idrettsvitenskap	
Institutt	Institutt for helse- og sykepleievitenskap	
3. Daglig ansvarlig (forsker, veileder, stipendiat)		
Fornavn	Rune	Før opp navnet på den som har det daglige ansvaret for prosjektet.Veileder er vanligvis daglig ansvarlig ved studentprosjekt. Veileder og student må være tilknyttet samme institusjon. Dersom studenten har ekstern veileder, kan biveileder eller fagansvarlig ved studiestedet stå som daglig ansvarlig.Arbeidssted må være tilknyttet behandlingsansvarlig institusjon, f.eks. underavdeling, institutt etc. NB! Det er viktig at du oppgir en e-postadresse som brukes aktivt. Vennligst gi oss beskjed dersom den endres.
Etternavn	Fensli	
Akademisk grad	Doktorgrad	
Stilling	Førsteamanuensis	
Arbeidssted	Institutt for informasjons- og kommunikasjonsteknologi, Universitetet i Agder, Grimstad	
Adresse (arb.sted)	Jon Lilletunsvei 9, Grimstad	
Postnr/sted (arb.sted)	4898 Grimstad	
Telefon/mobil (arb.sted)	37233000 / 91305222	
E-post	rune.fensli@uia.no	
4. Student (master, bachelor)		
Studentprosjekt	Ja ● Nei ○	NB! Det er viktig at du oppgir en e-postadresse som brukes aktivt. Vennligst gi oss beskjed dersom den endres.
Fornavn	Rune	
Etternavn	Hystad	
Akademisk grad	Høyere grad	
Privatadresse	Klomreheia 13B	
Postnr/sted (privatadresse)	4885 Grimstad	
Telefon/mobil	48265643 /	
E-post	runehystad@gmail.com	
5. Formålet med prosjektet		
Formål	Formålet er å innhente kunnskap fra sluttbrukere og IT-personell/forvaltere, og andre med kjennskap til forvaltningsproblematikk om hvordan tilgangsstyringen i elektronisk pasientjournal fungerer i dag, og hvordan den kan forbedres.	Redegjør kort for prosjektets formål, problemstilling, forskningsspørsmål e.l. Maks 750 tegn.
6. Prosjektomfang		

Velg omfang	● Enkel institusjon ○ Nasjonalt samarbeidsprosjekt ○ Internasjonalt samarbeidsprosjekt	Med samarbeidsprosjekt menes prosjekt som gjennomføres av flere institusjoner samtidig, som har samme formål og hvor personopplysninger utveksles.
Oppgi øvrige institusjoner		

Oppgi hvordan samarbeidet foregår		
7. Utvalgsbeskrivelse		
Utvalget	Utvalget skal bestå av personer som kan karakteriseres som eksperter. Det vil si sluttbrukere (leger, sykepleiere, sekretærer osv.), i tillegg til forvaltere av elektronisk pasientjournal, og andre med kjennskap til forvaltningsproblematikk.	Med utvalg menes dem som deltar i undersøkelsen eller dem det innhentes opplysninger om. F.eks. et representativt utvalg av befolkningen, skoleelever med lese- og skrivevansker, pasienter, innsatte.
Rekruttering og trekking	Sluttbrukerne rekrutteres gjennom kontaktperson ved forskningsenheten i Sørlandet sykehu,s via veileder Rune Fensli. I tillegg vil noen deltakere rekrutteres fra eget nettverk, og i tillegg vil andre med spesifikk kompetanse rundt tilgangsstyring bli invitert til å delta i studien.	Beskriv hvordan utvalget trekkes eller rekrutteres og oppgi hvem som foretar den. Et utvalg kan trekkes fra registre som f.eks. Folkeregisteret, SSB-registre, pasientregistre, eller det kan rekrutteres gjennom f.eks. en bedrift, skole, idrettsmiljø, eget nettverk.
Førstegangskontakt	Sluttbrukere ved SSHF kontaktes først av kontaktperson ved forskningsenheten deres. Resterene respondenter vil veileder Rune Fensli sende ut mail med henvendelse til, dette for å unngå at jeg kontakter mulige respondenter direkte.	Beskriv hvordan førstegangskontakten opprettes og oppgi hvem som foretar den. Les mer om dette på våre temasider.
Alder på utvalget	□ Barn (0-15 år) □ Ungdom (16-17 år) ■ Voksne (over 18 år)	
Antall personer som inngår i utvalget	Rundt 30 personer.	
Inkluderes det myndige personer med redusert eller manglende samtykkekompetanse?	Ja ○ Nei ●	Begrunn hvorfor det er nødvendig å inkludere myndige personer med redusert eller manglende samtykkekompetanse. Les mer om Pasienter, brukere og personer med redusert eller manglende samtykkekompetanse
Hvis ja, begrunn		
8. Metode for innsamling av personopplysninger		
Kryss av for hvilke datainnsamlingsmetoder og datakilder som vil benyttes	□ Spørreskjema □ Personlig intervju □ Gruppeintervju □ Observasjon □ Psykologiske/pedagogiske tester □ Medisinske undersøkelser/tester □ Journaldata □ Registerdata ■ Annen innsamlingsmetode	Personopplysninger kan innhentes direkte fra den registrerte f.eks. gjennom spørreskjema, intervju, tester, og/eller ulike journaler (f.eks. elevmapper, NAV, PPT, sykehus) og/eller registre (f.eks. Statistisk sentralbyrå, sentrale helseregistre).
Annen innsamlingsmetode, oppgi hvilken	Delphimetode via e-post, evt. SurveyXact som er et elektronisk verktøy for gjennomføring av spøøreundersøkelser.	
Kommentar		
9. Datamaterialets innhold		

Redegjør for hvilke opplysninger som samles inn	Det skal utføres en Delphiundersøkelse for å identifisere og rangere hindringer, og mulige forbedringer i tilgangsstyringen i elektronisk pasientjournal.	Spørreskjema, intervju-/temaguide, observasjonsbeskrivelse m.m. sendes inn sammen med meldeskjemaet. NB! Vedleggene lastes opp til sist i meldeskjema, se punkt 16 Vedlegg.
Samles det inn direkte personidentifiserende opplysninger?	Ja ● Nei ○	Dersom det krysses av for ja her, se nærmere under punkt 11 Informasjonssikkerhet. Les mer om hva personopplysninger er NB! Selv om opplysningene er anonymiserte i oppgave/rapport, må det krysses av dersom direkte og/eller indirekte personidentifiserende opplysninger innhentes/registreres i forbindelse med prosjektet.
Hvis ja, hvilke?	□ 11-sifret fødselsnummer ■ Navn, fødselsdato, adresse, e-postadresse og/eller telefonnummer	
Spesifiser hvilke	Navn, e-postadresse og telefonnummer.	

Samles det inn indirekte personidentifiserende opplysninger?	Ja ● Nei ○	En person vil være indirekte identifiserbar dersom det er mulig å identifisere vedkommende gjennom bakgrunnsopplysninger som for eksempel bostedskommune eller arbeidsplass/skole kombinert med opplysninger som alder, kjønn, yrke, diagnose, etc. Kryss også av dersom ip-adresse registreres.
Hvis ja, hvilke?	Yrke og arbeidsplass kan utilsiktet bli samlet inn, dersom respondentene bruker signatur i e-posten, som inneholder informasjon om dette.	
Samles det inn sensitive personopplysninger?	Ja ○ Nei ●	
Hvis ja, hvilke?	□ Rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning □ At en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling □ Helseforhold □ Seksuelle forhold □ Medlemskap i fagforeninger	
Samles det inn opplysninger om tredjeperson?	Ja ○ Nei ●	Med opplysninger om tredjeperson menes opplysninger som kan spores tilbake til personer som ikke inngår i utvalget. Eksempler på tredjeperson er kollega, elev, klient, familiemedlem.
Hvis ja, hvem er tredjeperson og hvilke opplysninger registreres?		
Hvordan informeres tredjeperson om behandlingen?	□ Skriftlig □ Muntlig □ Informeres ikke	
Informeres ikke, begrunn		

10. Informasjon og samtykke

Oppgi hvordan utvalget informeres	■ Skriftlig □ Muntlig □ Informeres ikke	Vennligst send inn informasjonsskrivet eller mal for muntlig informasjon sammen med meldeskjema. NB! Vedlegg lastes opp til sist i meldeskjemaet, se punkt 16 Vedlegg. Dersom utvalget ikke skal informeres om behandlingen av personopplysninger må det begrunnes. Last ned vår veiledende mal til informasjonsskriv
Begrunn		
Oppgi hvordan samtykke fra utvalget innhentes	■ Skriftlig □ Muntlig □ Innhentes ikke	Dersom det innhentes skriftlig samtykke anbefales det at samtykkeerklæringen utformes som en

Innhentes ikke, begrunn		svarslipp eller på eget ark. Dersom det ikke skal innhentes samtykke, må det begrunnes
11. Informasjonssikkerhet		
Direkte personidentifiserende opplysninger erstattes med et referansenummer som viser til en atskilt navneliste (koblingsnøkkel)	Ja ● Nei ○	Har du krysset av for ja under punkt 9 Datamaterialets innhold må det merkes av for hvordan direkte personidentifiserende opplysninger registreres. NB! Som hovedregel bør ikke direkte personidentifiserende opplysninger registreres sammen med det øvrige datamaterialet.
Hvordan oppbevares navnelisten/ koblingsnøkkelen og hvem har tilgang til den?	Dette oppbevares på privat passordbeskyttet datamaskin. Det er kun meg som får tilgang til disse opplysningene	
Direkte personidentifiserende opplysninger oppbevares sammen med det øvrige materialet	Ja ○ Nei ●	
Hvorfor oppbevares direkte personidentifiserende opplysninger sammen med det øvrige datamaterialet?		

Oppbevares direkte personidentifiserbare opplysninger på andre måter?	Ja ○ Nei ●	
Spesifiser		
Hvordan registreres og oppbevares datamaterialet?	□ Fysisk isolert datamaskin tilhørende virksomheten □ Datamaskin i nettverkssystem tilhørende virksomheten □ Datamaskin i nettverkssystem tilknyttet Internett tilhørende virksomheten □ Fysisk isolert privat datamaskin ■ Privat datamaskin tilknyttet Internett □ Videoopptak/fotografi □ Lydopptak □ Notater/papir ■ Annen registreringsmetode	Merk av for hvilke hjelpemidler som benyttes for registrering og analyse av opplysninger. Sett flere kryss dersom opplysningene registreres på flere måter.
Annen registreringsmetode beskriv	Passordbeskyttet ekstern harddisk.	
Behandles lyd-/videoopptak og/eller fotografi ved hjelp av datamaskinbasert utstyr?	Ja ○ Nei ●	Kryss av for ja dersom opptak eller foto behandles som lyd-/bildefil. Les mer om behandling av lyd og bilde.
Hvordan er datamaterialet beskyttet mot at uvedkommende får innsyn?	Alle lagringsmedier er beskyttet med brukernavn og passord.	Er f.eks. datamaskintilgangen beskyttet med brukernavn og passord, står datamaskinen i et låsbart rom, og hvordan sikres bærbare enheter, utskrifter og opptak?
Dersom det benyttes mobile lagringsenheter (bærbar datamaskin, minnepenn, minnekort, cd, ekstern harddisk, mobiltelefon), oppgi hvilke	Bærbar datamaskin og ekstern harddisk.	NB! Mobile lagringsenheter bør ha mulighet for kryptering.
Vil medarbeidere ha tilgang til datamaterialet på lik linje med daglig ansvarlig/student?	Ja ● Nei ○	
Hvis ja, hvem?	Veileder Rune Fensli	
Overføres personopplysninger ved hjelp av e-post/Internett?	Ja ● Nei ○	F.eks. ved bruk av elektronisk spørreskjema, overføring av data til

Hvis ja, hvilke?	Navn overføres via e-post.	samarbeidspartner/databehandler mm.
Vil personopplysninger bli utlevert til andre enn prosjektgruppen?	Ja ○ Nei ●	
Hvis ja, til hvem?		
Samles opplysningene inn/behandles av en databehandler?	Ja ○ Nei ●	Dersom det benyttes eksterne til helt eller delvis å behandle personopplysninger, f.eks. Questback, Synovate MMI, Norfakta eller transkriberingsassistent eller tolk, er dette å betrakte som en databehandler. Slike oppdrag må kontraktsreguleres Les mer om databehandleravtaler her
Hvis ja, hvilken?		
12. Vurdering/godkjenning fra andre instanser		
Søkes det om dispensasjon fra taushetsplikten for å få tilgang til data?	Ja ○ Nei ●	For å få tilgang til taushetsbelagte opplysninger fra f.eks. NAV, PPT, sykehus, må det søkes om dispensasjon fra taushetsplikten. Dispensasjon søkes vanligvis fra aktuelt departement. Dispensasjon fra taushetsplikten for helseopplysninger skal for alle typer forskning søkes Regional komité for medisinsk og helsefaglig forskningsetikk
Kommentar		

Søkes det godkjenning fra andre instanser?	Ja ● Nei ○	F.eks. søke registereier om tilgang til data, en ledelse om tilgang til forskning i virksomhet, skole, etc.
Hvis ja, hvilke?	Fakultetets etikkomité ved Fakultet for helse- og idrettsvitenskap, Universitetet i Agder.	
13. Prosjektperiode		
Prosjektperiode	Prosjektstart:05.01.2014 Prosjektslutt:12.06.2014	Prosjektstart Vennligst oppgi tidspunktet for når førstegangskontakten med utvalget opprettes og/eller datainnsamlingen starter. Prosjektslutt Vennligst oppgi tidspunktet for når datamaterialet enten skal anonymiseres/slettes, eller arkiveres i påvente av oppfølgingsstudier eller annet. Prosjektet anses vanligvis som avsluttet når de oppgitte analyser er ferdigstilt og resultatene publisert, eller oppgave/avhandling er innlevert og sensurert.
Hva skal skje med datamaterialet ved prosjektslutt?	■ Datamaterialet anonymiseres □ Datamaterialet oppbevares med personidentifikasjon	Med anonymisering menes at datamaterialet bearbeides slik at det ikke lenger er mulig å føre opplysningene tilbake til enkeltpersoner.NB! Merk at dette omfatter både oppgave/publikasjon og rådata. Les mer om anonymisering
Hvordan skal datamaterialet anonymiseres?	E-poster slettes, data i SurveyXact slettes.	Hovedregelen for videre oppbevaring av data med personidentifikasjon er samtykke fra den registrerte. Årsaker til oppbevaring kan være planlagte
Hvorfor skal datamaterialet oppbevares med personidentifikasjon?		

Hvor skal datamaterialet oppbevares, og hvor lenge?		oppfølgningsstudier, undervisningsformål eller annet. Datamaterialet kan oppbevares ved egen institusjon, offentlig arkiv eller annet. Les om arkivering hos NSD
14. Finansiering		
Hvordan finansieres prosjektet?	Prosjektet finansieres ikke.	
15. Tilleggsopplysninger		
Tilleggsopplysninger		
16. Vedlegg		
Antall vedlegg	1	

Vedlegg 2 Søknad om tillatelse til innhenting av data

Til: xxx avdeling ved Sørlandet sykehus HF

SØKNAD OM TILLATELSE TIL INNHENTING AV DATA

I forbindelse med prosjektarbeid i helse- og sosialinformatikk er det noen ganger ønskelig å innhente opplysninger. I den anledning søker undertegnede student om tillatelse til å gjennomføre datainnsamling ved:

Sted: xxx avdeling ved Sørlandet sykehus HF

Tema og foreløpig problemformulering på oppgaven er:

Tema:	Tilgangsstyring i elektronisk pasientjournal i spesialisthelsetjenesten
Problemformulering:	Hvilke utfordringer er det med beslutningsstyrt tilgangskontroll i elektronisk pasientjournal i spesialisthelsetjenesten, og hvordan kan den forbedres?
Veileder ved universitetet: E-post / Telefon:	Førsteamanuensis Rune Fensli, tlf 37 25 33 73, rune.fensli@uia.no
Hensikt med og metode for datainnsamling	Se vedlagte informasjonsskriv.

Presiseringer i forhold til datainnsamlingen:

Populasjon/utvalg:	Utvalget vil bestå av sluttbrukere (leger, sykepleiere, sekretærer osv.), i tillegg til forvaltere av elektronisk pasientjournal, og andre med kjennskap til forvaltningsproblematikk.
Ønsket antall respondenter:	Rundt 45 respondenter totalt. Fra deres klinikk/avdeling ønskes: Sett inn navn her
Tidspunkt/varighet:	Ønskes gjennomført i perioden rundt 3.-24. februar. Undersøkelsen består av tre til fire runder med spørreskjema, hver runde vil ta ca. 10 min.
Ved ønske om utfyllende informasjon, og ved bekreftelse/ avslag på denne søknaden, vennligst ta kontakt med: (Navn, E-post, Tlf)	Student Rune Hystad, tlf. 48 26 56 43, runehystad@gmail.com Veileder Rune Fensli, tlf 91305222/37253373, rune.fensli@uia.no

Med hilsen

Rune Hystad
17.01.2014

Vedlegg 3 Informasjon om undersøkelsen

Informasjon om undersøkelsen

Jeg er masterstudent ved helse- og sosialinformatikkstudiet ved UiA, og for tiden skriver jeg masteroppgave, som skal leveres våren 2014, og det er i den sammenheng jeg henvender meg til deg. Jeg jobber med forvaltning av elektronisk pasientjournal, og har blant annet jobbet mye med tilgangsstyring. Beslutningsstyrt tilgangskontroll i DIPS er innført ved flere av landets helseforetak, og det tas sikte på å implementeres på tvers av flere regionale helseforetak, som ledd i standardiseringsprosesser. Det finnes mye forskning på området tilgangskontroll, men lite forskning som tar for seg evaluering av beslutningsstyrt tilgang i Norge.

Dette ønsker jeg som tema for min masteroppgave, som har fått arbeidstittel:

Tilgangskontroll av elektronisk pasientjournal
-En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

Litteratursøk på tema/området har identifisert et hull vedrørende erfaringer med bruk av beslutningsstyrt tilgangskontroll. EPJ-standarden som er utviklet av Helsedirektoratet har lagt føringer for at tilgangskontrollen i EPJ ved sykehus skal være basert på beslutningsstyrt tilgangskontroll.
I denne oppgaven søkes det å fokusere på både sluttbrukere, og forvalteres erfaringer med bruk av beslutningsstyrt tilgangskontroll, i forhold til ivaretakelse av brukeres behov for informasjon, og pasienters konfidensialitet.

Funnene kan bidra til å belyse eventuelle utfordringer med tilgangsstyring, og gi gevinster i forhold til å komme med anbefalinger for videre utvikling og bruk av tilgangsstyring i DIPS EPJ.

Design og metode for undersøkelsen

I denne oppgaven vil jeg benytte Delphimetoden for datainnsamling og analyse. I min studie vil jeg søke å få svar på forskningsspørsmålene mine ved å ha to ekspertpanel (hvert bestående av 10-15 eksperter), ett bestående av sluttbrukere, og ett bestående av forvaltere av DIPS og andre som kjenner til utfordringer fra et forvaltningsperspektiv.

Vedlegg 4 Forespørsel om deltakelse i undersøkelse

Forespørsel om deltakelse i undersøkelse

Tilgangsstyring av elektronisk pasientjournal

-En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

Jeg er masterstudent ved helse- og sosialinformatikkstudiet ved UiA, og for tiden skriver jeg masteroppgave, og det er i den sammenheng jeg henvender meg til deg.

Fokus for masteroppgaven er å undersøke brukere og forvaltere sine erfaringer med tilgangsstyring i DIPS elektronisk pasientjournal (EPJ), i forhold til at brukere skal ha den informasjonen de trenger om pasienten, samtidig som pasientens personvern ivaretas ved å minimere muligheten for urettmessig tilegnelse av taushetsbelagte opplysninger (snoking).

Jeg ber deg om å delta på følgende:

Undersøkelsen består av fire runder med elektroniske spørreskjemaer. I første runde skal dere foreslå minst fem punkter/faktorer som dere mener beskriver utfordringer, og minst fem punkter/faktorer med forslag til forbedring av tilgangsstyringen. Undersøkelsen består av tre trinn, der første trinn er en idémyldring av viktige faktorer, trinn to er en innsnevring av faktorene i idémyldringen, og trinn tre er en rangering av faktorene.

Jeg ser for meg fire runder med spørreskjemaer for å komme igjennom de tre trinnene, for å forsøke å komme frem til rimelig grad av enighet blant deltakerne, rundt 5-10 faktorer som vil kunne beskrive utfordringer, og forslag til forbedring av tilgangsstyringen. Deltakerne vil være anonyme overfor hverandre.

Det er ønskelig at dere svarer raskt, og det er tre dagers frist på hvert skjema. Hvert skjema er kort, med få spørsmål og svartid er anslått til ca. 10 minutter per spørreskjema. Link til det første spørreskjemaet finner du lenger nede på siden. Skjemaene sendes med en ukes mellomrom, og studien vil foregå i tidsrommet rundt 10. februar til 3. mars.

Studien er for øvrig godkjent av din avdelingsleder.

Funnene kan bidra til å belyse eventuelle utfordringer med tilgangsstyringen, og komme med anbefalinger for videre utvikling og bruk av tilgangsstyring i DIPS EPJ.

Jeg vil holde kontakt med deg per e-post. Dette innebærer at jeg får kjennskap til ditt navn og e-postadresse. Dette vil ikke bli videreformidlet til andre personer/instanser, og i alt materiale

vil dine utsagn forbli anonyme. Svar fra deg vil oppbevares elektronisk, og slettes innen to uker etter sensur av oppgaven (juni 2014).

Rett til innsyn og sletting av opplysninger om deg:

Hvis du samtykker til å delta i studien, har du rett til å få innsyn i hvilke opplysninger som er registrert om deg. Du har videre rett til å få korrigert eventuelle feil i de opplysningene jeg har registrert. Dersom du trekker deg fra studien, kan du kreve å få slettet innsamlede opplysninger, med mindre opplysningene allerede er inngått i analyser eller brukt i vitenskapelige publikasjoner.

Frivillig deltakelse:

Det er frivillig å delta i studien. Du kan når som helst og uten å oppgi noen grunn trekke ditt samtykke til å delta i studien uten at dette vil få konsekvenser for deg. Dersom du ønsker å delta, og svarer på denne forespørselen, betraktes dette som ditt samtykke. Om du nå sier ja til å delta, kan du senere trekke tilbake ditt samtykke. Dersom du senere ønsker å trekke deg eller har spørsmål til studien, kan du kontakte student eller veileder (se under).

Link til spørreundersøkelsen:

<%MorpheusMailLink%>

Svarfrist på dette spørreskjemaet er førstkommende onsdag.

Tusen takk for hjelpen!

Mvh

Rune Hystad

Navn, telefonnummer og E-postadresser: **Navn**	**Telefonnummer**	**E-postadresse**
Student Rune Hystad	48 26 56 43	runehystad@gmail.com
Veileder Rune Fensli	37 25 33 73/91 30 52 22	rune.fensli@uia.no

Vedlegg 5 Spørreskjemaer

Tilgangsstyring av elektronisk pasientjournal

- En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

Runde 1

Jeg setter stor pris på at du tar deg tid til å svare på denne undersøkelsen.

I denne runden får du to spørsmål som du besvarer i fritekstfeltet nedenfor spørsmålene. Gå til første spørsmål ved å trykke på "Neste" og så skrive inn svarene i friteksfeltene.

Spørsmål 1: Hvilke utfordringer opplever du knyttet til beslutningsstyrt tilgang (tilgangsstyringen i DIPS)? Du bør nevne punktvis (i stikkordsform) minst fem utfordringer du kommer på.

_____

_____

Spørsmål 2: Hvordan kan tilgangsstyringen i DIPS etter din mening forbedres? Du bør nevne punktvis (i stikkordsform) minst fem faktorer du kommer på.

Tusen takk for at du tok deg tid til å delta i første runde av denne undersøkelsen!

En e-post med kvittering på dine svar blir automatisk sendt til din e-postadresse. Ta vare på e-posten til neste uke, da du trenger den til neste runde med spørreskjema.

Denne runden av undersøkelsen kan nå avsluttes ved å trykke på knappen AVSLUTT nede i høyre hjørne.

Tilgangsstyring av elektronisk pasientjournal

- En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

Runde 2:
Jeg har nå gjennomgått svarene som har kommet inn fra alle respondentene, og presentert dem i to lister. Enkelte svar har blitt forkortet, og svar med samme mening har blitt slått sammen. I denne runden skal du se igjennom listene. Dersom du ikke kan finne dine svar i listene, eller jeg har misforstått hva du har ment, ber jeg deg om å fylle dette inn i tekstfeltet under listene.

Dersom du finner dine svar (ikke nødvendigvis ordrett), trenger du ikke å skrive inn noe.

Trykk NESTE for å gå igjennom de to listene.

Ved spørsmål, kontakt meg på:
runehystad@gmail.com

Jeg spurte: Hvilke utfordringer opplever du knyttet til beslutningsstyrt tilgang (tilgangsstyringen i DIPS)? Du bør nevne punktvis (i

stikkordsform) minst fem utfordringer du kommer på.

Svarene som kom inn er oppsummert nedenfor (men ikke nødvendigvis ordrett). Se igjennom listen, og dersom du ikke finner ditt svar, sett det opp i feltet nedenfor i stikkordsform.

- Opplever ingen utfordringer
- Har ikke tilgang til pasientens medikamenter
- Har ikke tilgang til å beslutte tilgang selv, og må få en kollega til å gi tilgang
- Har ikke tilgang fra somatikk til psykiatri
- Det mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal
- Det kreves for mange tastetrykk for å beslutte seg tilgang
- Har for vid tilgang til dokumenter
- Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.
- Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket
- Mangler tilgang til tidligere undersøkelser
- For lite opplæring i tilgangsstyring
- Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang
- Bruker kan velge feil beslutningsmal
- Beslutningsstyrt tilgang fungerer bra, begrensningene ligger i lovverket
- Det tar mye tid å måtte beslutte tilgang

- Mangler info om hvorfor felter i skjermbilder er låst for redigering
- Misvisende tekst i skjermbilder som skal fortelle at man må beslutte tilgang for å få frem ønsket informasjon
- Når man beslutter tilgang har man automatisk bare tilgang i ett døgn
- Når man gir tilgang ang. tilsyn får man også tilgang til pasientjournalen
- Automatisk/implisitt tilgang forsvinner for kort tid etter utskrivelse
- Mangler implisitt/automatisk tilgang til pasientjournal

- Det er en utfordring at brukere kan gi seg selv tilgang
- Kan være lett å aktivere feil pasient, og derfor åpne feil journal
- Man har ikke tilgang til endring/registrering i henvisninger etter at de er sendt
- Man må beslutte tilgang for å få tilgang til PAS-delen, f.eks. bestilling av time
- Skjermbilder oppdateres ikke ved bytte av pasient
- Ikke alle brukere som har behov for det, har tilgang til nødretts-/blålystilgang

- Nødrett/blålystilgang brukes i tilfeller hvor det ikke er tale om en nødrettssituasjon
- Utilstrekkelig funksjonalitet for sperring av journal
- Utilstrekkelig funksjonalitet for registrering av pasientsamtykke
- Prosesstankegangen er ikke tilstrekkelig på plass, f.eks. ved at brukere som ikke er tilknyttet samme avdeling som pasientene de behandler, får bredere eller smalere tilgang enn ønskelig
- Kan ikke styre tilgang til et pasientforløp (en henvisningsperiode) på tvers av virksomheter
- Tilgangsstyringen er ikke integrert med personalsystemet
- Mangler funksjonalitet for beslutningsstyrt tilgang (f.eks. rapporter, lokalisering og listefunksjonalitet)
- Ikke tilstrekkelig antall/dekkende implisitte beslutningsmaler
- Tilpasninger til spesialtilganger er utfordrende for forvaltere
- Psykiatrifilter gir ikke alltid brukeren definerte tilganger i alle skjermbilder
- Definering av korrekte tilgangsprofiler
- Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig

- Det er gjort mange avvik fra beslutningsstyrt tilgang som bygger på dagens lovverk
- Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har
- Stor treghet ved administrering av tilganger
- Det er for dårlig støtte for logganalyse

- Vanskelig å følge opp loggene som skal kontrolleres for å finne eventuelle snokere
- Det er utfordrende å motivere brukere til å dokumentere korrekte data ved eksplisitte tilganger
- Kan ikke tidsbegrense tilgang gitt via profiler
- Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke
- Hvis tilgangene settes for vide, vil brukerne sjelden måtte beslutte tilgang, som kan medføre en risiko for manglende kompetanse ved en kritisk situasjon der tilgang må besluttes
- Vanskelig å gi tilgang til brukere med mange ulike funksjoner
- For lite tid til å gå gjennom tilgangene for å passe på at de er i samsvar med lover og regler

- Interessekonflikt mellom eier (HF) og forvalter av DIPS ift. tilgangsstyring
- Lite standardisering av tilgangsstyring på tvers av helseforetakene
- Krevende å få enkelte grupper av sluttbrukere til å anerkjenne at beslutningsstyrt tilgang er en hensiktsmessig løsning for å oppfylle krav om riktig tilgangsstyring
- Vanskelig å gi brukere tilganger som gjør at de ikke må bruke grønnlys/beslutte tilgang ofte

Jeg spurte: Hvordan kan tilgangsstyringen i DIPS etter din mening forbedres? Du bør nevne punktvis (i stikkordsform) minst fem utfordringer du kommer på.

Svarene som kom inn er oppsummert nedenfor (men ikke nødvendigvis ordrett). Se igjennom listen, og dersom du ikke finner ditt svar, sett det opp i feltet nedenfor i stikkordsform.

- Ser ingen områder for forbedring
- Redusere antall klikk som trengs for å beslutte seg tilgang
- Skjermbildet for å beslutte tilgang bør kommer opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til
- Mulighet for selv å kunne opprette egendefinert beslutningsmal
- Den besluttede tilgangen bør automatisk vare i mer enn én dag
- Lengre implisitt/automatisk tilgang til en journal etter en konsultasjon eller utskrivelse
- Medisinkort bør være tilgjengelig for alle avdelinger
- Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen
- Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang
- Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn
- Forfatter av dokument bør enkelt kunne sperre enkeltdokumenter/avsnitt/setninger i dialog med pasienten
- Bilder i DIPS bør bli tilgjengelige i det man har benyttet grønnlyset, slik at man slipper å lukke og åpne skjermbilder
- Bruke beslutningsmal/grønnlys i stedet for blålys/nødrettstilgang
- Nødrettsstilgang/blålystilgang må kunne utløses/legitimeres ut fra det enkelte helsepersonells skjønn/vurdering
- Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang
- Entydige meldinger om hvorfor man ikke får åpne/se dokumenter/labsvar man

ønsker å åpne

- Flere eksplisitte beslutningsmaler for å kunne dekke reell grunn for åpning av journal
- Valg for "gruppe-beslutning" hvis man skal gjøre oppslag på flere pasienter, f.eks. ved sammenligning av pasienter (diagnoser, koder osv.)
- Informasjon tilbake i tid bør være tilgjengelige uten at man må beslutte tilgang
- Forbedre søkemuligheter på pasienter
- Ta i bruk funksjonalitet som innebærer at for å få tilgang, må en annen gi deg tilgang, f.eks. for forvaltere
- Tilgang til retting ved feilsendt henvisning til annen avdeling
- Implementere beslutningsstøtte i forhold til behandlingsforløp
- Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk
- Felles retningslinjer for tilgangsstyring på regionalt eller nasjonalt nivå
- Strengere føringer for hva lokale helseforetak kan bestemme ift. tilgangsstyring
- Forbedre rutiner for bestilling og avslutning av tilganger
- Forbedre kommunikasjon mellom helseforetak og forvalter rundt tilgangsstyring
- Hyppigere kontroll av hvem som har tilgang til hva
- Aktiv bruk av innsynslogg for kvalitetssikring
- Det bør benyttes systemer som kontinuerlig analyserer innsynslogger
- Klarere retningslinjer fra nasjonale myndigheter i forhold til hvordan tilgangsstyringen skal legges opp
- Forbedre rutiner rundt opplæring/informasjon til sluttbrukere om tilgangsstyring, og lover og regler for dette
- Mer fleksible løsninger på tildeling av tilganger, uten at oversikten forsvinner for forvalterne
- Tilgang basert på eksplisitt beslutningsstyrt tilgang, vil for de som har både eksplisitt og implisitt beslutningsmyndighet, kunne unngå å bruke den implisitte tilgangen. Den videste eksplisitte beslutningsstyrte tilgang vil gi tilgang til det meste
- Mer prosessorientert tilgangsstyring/videreutvikling av implisitte beslutningsmaler for å støtte oppunder arbeidsflyt
- Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperioder

· Man bør kunne styre tilgang på tvers av lokaliseringer, avdelinger og seksjoner/fagområder, også innenfor samme virksomhet
· Utvikle beslutningsstyrt tilgang for rapporter og listefunksjonalitet
· Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS
· Bedre oversikt over alt hva en bruker har tilgang til
· Flere muligheter teknisk for å differensiere tilgang til beslutningsmaler
· Gi videre tilganger for å unngå spesialtilpasninger
· Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon
· En definisjon av beslutning må kunne knyttes til alle beslutninger som gjelder behandling av pasienten
· Mer fleksibilitet for inn- og utmelding av ressurser til for eksempel traumeteam

Tusen takk for at du tok deg tid til å delta i andre runde av denne undersøkelsen!

E-post med neste runde av undersøkelsen sendes ut i neste uke.

Denne runden av undersøkelsen kan nå avsluttes ved å trykke på knappen AVSLUTT nede i høyre hjørne.

Runde 3:

I denne runden ber jeg deg om å velge ut minst 10 av de viktigste punktene under hvert spørsmål ved å sette kryss.

Ved spørsmål, ta kontakt på e-post: runehystad@gmail.com

Spørsmål 1:

Velg minst 10 utsagn/faktorer som du mener er viktige utfordringer knyttet til beslutningsstyrt tilgang. Dine svar skal være basert på den kompetansen du har i din stilling. Utfordringene trenger ikke å forholde seg til dine egne erfaringer.

(2) ❑ Har ikke tilgang til pasientens medikamenter
(3) ❑ Har ikke tilgang til å beslutte tilgang selv, og må få en kollega til å gi tilgang
(4) ❑ Har ikke tilgang fra somatikk til psykiatri
(5) ❑ Det mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal
(6) ❑ Det kreves for mange tastetrykk for å beslutte seg tilgang
(7) ❑ Har for vid tilgang til dokumenter
(8) ❑ Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.
(9) ❑ Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket
(10) ❑ Mangler tilgang til tidligere undersøkelser
(11) ❑ For lite opplæring i tilgangsstyring
(12) ❑ Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang

(13) ❑ Bruker kan velge feil beslutningsmal
(14) ❑ Beslutningsstyrt tilgang fungerer bra, begrensningene ligger i lovverket
(15) ❑ Det tar mye tid å måtte beslutte tilgang
(16) ❑ Mangler info om hvorfor felter i skjermbilder er låst for redigering
(17) ❑ Misvisende tekst i skjermbilder som skal fortelle at man må beslutte tilgang for å få frem ønsket informasjon
(18) ❑ Når man beslutter tilgang har man automatisk bare tilgang i ett døgn
(19) ❑ Når man gir tilgang ang. tilsyn får man også tilgang til pasientjournalen
(20) ❑ Automatisk/implisitt tilgang forsvinner for kort tid etter utskrivelse
(21) ❑ Mangler implisitt/automatisk tilgang til pasientjournal
(22) ❑ Det er en utfordring at brukere kan gi seg selv tilgang
(23) ❑ Kan være lett å aktivere feil pasient, og derfor åpne feil journal
(24) ❑ Man har ikke tilgang til endring/registrering i henvisninger etter at de er sendt
(25) ❑ Man må beslutte tilgang for å få tilgang til PAS-delen, f.eks. bestilling av time
(26) ❑ Skjermbilder oppdateres ikke ved bytte av pasient
(27) ❑ Ikke alle brukere som har behov for det, har tilgang til nødretts-/blålystilgang
(28) ❑ Nødrett/blålystilgang brukes i tilfeller hvor det ikke er tale om en nødrettssituasjon
(29) ❑ Utilstrekkelig funksjonalitet for sperring av journal
(30) ❑ Utilstrekkelig funksjonalitet for registrering av pasientsamtykke
(31) ❑ Prosesstankegangen er ikke tilstrekkelig på plass, f.eks. ved at brukere som ikke er tilknyttet samme avdeling som pasientene de behandler, får bredere eller smalere tilgang enn ønskelig
(32) ❑ Kan ikke styre tilgang til et pasientforløp (en henvisningsperiode) på tvers av virksomheter
(33) ❑ Tilgangsstyringen er ikke integrert med personalsystemet
(34) ❑ Mangler funksjonalitet for beslutningsstyrt tilgang (f.eks. rapporter, lokalisering og listefunksjonalitet)
(35) ❑ Ikke tilstrekkelig antall/dekkende implisitte beslutningsmaler
(36) ❑ Tilpasninger til spesialtilganger er utfordrende for forvaltere
(37) ❑ Psykiatrifilter gir ikke alltid brukeren definerte tilganger i alle skjermbilder
(38) ❑ Definering av korrekte tilgangsprofiler
(39) ❑ Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig
(40) ❑ Det er gjort mange avvik fra beslutningsstyrt tilgang som bygger på dagens lovverk
(41) ❑ Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har
(42) ❑ Stor treghet ved administrering av tilganger
(43) ❑ Det er for dårlig støtte for logganalyse
(44) ❑ Vanskelig å følge opp loggene som skal kontrolleres for å finne eventuelle snokere
(45) ❑ Det er utfordrende å motivere brukere til å dokumentere korrekte data ved eksplisitte tilganger
(46) ❑ Kan ikke tidsbegrense tilgang gitt via profiler
(47) ❑ Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke

(48) ❑ Hvis tilgangene settes for vide, vil brukerne sjelden måtte beslutte tilgang, som kan medføre en risiko for manglende kompetanse ved en kritisk situasjon der tilgang må besluttes
(49) ❑ Vanskelig å gi tilgang til brukere med mange ulike funksjoner
(50) ❑ For lite tid til å gå gjennom tilgangene for å passe på at de er i samsvar med lover og regler
(51) ❑ Interessekonflikt mellom eier (HF) og forvalter av DIPS ift. tilgangsstyring
(52) ❑ Lite standardisering av tilgangsstyring på tvers av helseforetakene
(53) ❑ Krevende å få enkelte grupper av sluttbrukere til å anerkjenne at beslutningsstyrt tilgang er en hensiktsmessig løsning for å oppfylle krav om riktig tilgangsstyring
(54) ❑ Vanskelig å gi brukere tilganger som gjør at de ikke må bruke grønnlys/beslutte tilgang ofte
(55) ❑ Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang
(56) ❑ Hver enkelt virksomhet har ikke forutsetninger eller kapasitet til å forvalte slik komplisert brukeradministrasjonen og sørge for korrekte tilganger til sine egne ansatte
(57) ❑ Beslutningsstyrt tilgang er knyttet til virksomhetsnivå, men virksomhetsnivået er egentlig irrelevant for taushetsplikten etter helsepersonelloven § 25 og 45

Spørsmål 2:

Velg minst 10 utsagn/faktorer som du mener er viktige faktorer for at tilgangsstyringen skal forbedres. Dine svar skal være basert på den kompetansen du har i din stilling. Forbedringsforslagene trenger ikke å forholde seg til dine egne erfaringer.

(2) ❑ Redusere antall klikk som trengs for å beslutte seg tilgang
(3) ❑ Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til
(4) ❑ Mulighet for selv å kunne opprette egendefinert beslutningsmal
(5) ❑ Den besluttede tilgangen bør automatisk vare i mer enn én dag
(6) ❑ Lengre implisitt/automatisk tilgang til en journal etter en konsultasjon eller utskrivelse
(7) ❑ Medisinkort bør være tilgjengelig for alle avdelinger
(8) ❑ Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen
(9) ❑ Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang
(10) ❑ Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn
(11) ❑ Forfatter av dokument bør enkelt kunne sperre enkeltdokumenter/avsnitt/setninger i dialog med pasienten
(12) ❑ Bilder i DIPS bør bli tilgjengelige i det man har benyttet grønnlyset, slik at man slipper å lukke og åpne skjermbilder
(13) ❑ Bruke beslutningsmal/grønnlys i stedet for blålys/nødrettstilgang
(14) ❑ Nødrettsstilgang/blålystilgang må kunne utløses/legitimeres ut fra det enkelte helsepersonells skjønn/vurdering
(15) ❑ Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang
(16) ❑ Entydige meldinger om hvorfor man ikke får åpne/se dokumenter/labsvar man ønsker å åpne

(17) ❑ Flere eksplisitte beslutningsmaler for å kunne dekke reell grunn for åpning av journal
(18) ❑ Valg for "gruppe-beslutning" hvis man skal gjøre oppslag på flere pasienter, f.eks. ved sammenligning av pasienter (diagnoser, koder osv.)
(19) ❑ Informasjon tilbake i tid bør være tilgjengelige uten at man må beslutte tilgang
(20) ❑ Forbedre søkemuligheter på pasienter
(21) ❑ Ta i bruk funksjonalitet som innebærer at for å få tilgang, må en annen gi deg tilgang, f.eks. for forvaltere
(22) ❑ Tilgang til retting ved feilsendt henvisning til annen avdeling
(23) ❑ Implementere beslutningsstøtte i forhold til behandlingsforløp
(24) ❑ Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk
(25) ❑ Felles retningslinjer for tilgangsstyring på regionalt eller nasjonalt nivå
(26) ❑ Strengere føringer for hva lokale helseforetak kan bestemme ift. tilgangsstyring
(27) ❑ Forbedre rutiner for bestilling og avslutning av tilganger
(28) ❑ Forbedre kommunikasjon mellom helseforetak og forvalter rundt tilgangsstyring
(29) ❑ Hyppigere kontroll av hvem som har tilgang til hva
(30) ❑ Aktiv bruk av innsynslogg for kvalitetssikring
(31) ❑ Det bør benyttes systemer som kontinuerlig analyserer innsynslogger
(32) ❑ Klarere retningslinjer fra nasjonale myndigheter i forhold til hvordan tilgangsstyringen skal legges opp
(33) ❑ Forbedre rutiner rundt opplæring/informasjon til sluttbrukere om tilgangsstyring, og lover og regler for dette
(34) ❑ Mer fleksible løsninger på tildeling av tilganger, uten at oversikten forsvinner for forvalterne
(35) ❑ Tilgang basert på eksplisitt beslutningsstyrt tilgang, vil for de som har både eksplisitt og implisitt beslutningsmyndighet, kunne unngå å bruke den implisitte tilgangen. Den videste eksplisitte beslutningsstyrte tilgang vil gi tilgang til det meste
(36) ❑ Mer prosessorientert tilgangsstyring/videreutvikling av implisitte beslutningsmaler for å støtte oppunder arbeidsflyt
(37) ❑ Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperioder
(38) ❑ Man bør kunne styre tilgang på tvers av lokaliseringer, avdelinger og seksjoner/fagområder, også innenfor samme virksomhet
(39) ❑ Utvikle beslutningsstyrt tilgang for rapporter og listefunksjonalitet
(40) ❑ Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS
(41) ❑ Bedre oversikt over alt hva en bruker har tilgang til
(42) ❑ Flere muligheter teknisk for å differensiere tilgang til beslutningsmaler (er du f.eks. ansatt på intensivenhet som sykepleier skal du kunne få tilgang til en annen beslutningsmal enn andre spl. på vanlig post)
(43) ❑ Gi videre tilganger for å unngå spesialtilpasninger
(44) ❑ Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon
(45) ❑ En definisjon av beslutning må kunne knyttes til alle beslutninger som gjelder behandling av pasienten

(46) ❑ Mer fleksibilitet for inn- og utmelding av ressurser (brukertilgang) til for eksempel traumeteam

Tusen takk for svarene!

Neste uke kommer runde fire, der du skal rangere faktorene.

Mvh
Rune Hystad

Tilgangsstyring av elektronisk pasientjournal

- En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

I denne runden ber jeg deg om å rangere listene med faktorer, fra 1 til 10 under spørsmål 1, og 1 til 9 under spørsmål 2, der 1 = viktigst, og henholdsvis 10, og 9 = minst viktig.

Hvert tall kan kun benyttes én gang under hvert spørsmål.

Du svarer på skjemaet ved å trykke på NESTE, og så angi svaret ved å rangere viktigheten av hver faktor. Dersom du ønsker det, kan du gi en forklaring til rangeringen i fritekstfeltene på høyre side.

Spørsmål 1: I hvilken grad anser du følgende utsagn/faktorer som utfordringer i tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-10 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-10, der 1 = viktigst.

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

Evt. begrunnelse

Det _ _____

		Evt. begrunnelse
mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal		_____ _____ _____
Det kreves for mange tastetrykk for å beslutte seg tilgang	_	_____ _____ _____ _____
Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.	_	_____ _____ _____ _____
Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket	_	_____ _____ _____ _____
For lite opplæring i tilgangsstyring	_	_____ _____ _____ _____
Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang	_	_____ _____ _____ _____
Bruker kan velge feil beslutningsmal	_	_____ _____ _____ _____
Når man beslutter tilgang har man automatisk bare tilgang i ett døgn	_	_____ _____ _____ _____
Ikke	_	_____

		Evt. begrunnelse
tilstrekkelig antall/dekkende implisitte beslutningsmaler	_	_____
Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang	_	_____

Spørsmål 2: I hvilken grad tror du følgende utsagn/faktorer kan forbedre tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-9 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-9, der 1 = viktigst.

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

		Evt. begrunnelse
Redusere antall klikk som trengs for å beslutte seg tilgang	_	_____
Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til	_	_____
Mulighet for selv å kunne opprette egendefinert beslutningsmal	_	_____

		Evt. begrunnelse
Den besluttede tilgangen bør automatisk vare i mer enn én dag	_	_____
Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen	_	_____
Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang	_	_____
Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn	_	_____
Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang	_	_____
Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon	_	_____

Tusen takk for at du tok deg tid til å delta i denne spørreundersøkelsen! Evt. spørsmål kan rettes til E-postadressen nederst på siden.

Denne runden av undersøkelsen kan nå avsluttes ved å trykke på knappen AVSLUTT nede i høyre hjørne.

Mvh
Rune Hystad
runehystad@gmail.com

Tilgangsstyring av elektronisk pasientjournal

- En Delphistudie av dagens utfordringer og synliggjøring av potensielle forbedringer

I denne runden ber jeg deg om å rangere listene med faktorer, fra 1 til 9 under spørsmål 1, og 1 til 8 under spørsmål 2, der 1 = viktigst, og henholdsvis 9, og 8 = minst viktig.

Hvert tall kan kun benyttes én gang under hvert spørsmål.

Du svarer på skjemaet ved å trykke på NESTE, og så angi svaret ved å rangere viktigheten av hver faktor. Dersom du ønsker det, kan du gi en forklaring til rangeringen i fritekstfeltene på høyre side.

Spørsmål 1: I hvilken grad anser du følgende utsagn/faktorer som utfordringer i tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-9 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-9, der 1 = viktigst.

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

		Evt. begrunnelse
Utilstrekkelig	_	_____

		Evt. begrunnelse
funksjonalitet for sperring av journal		
Tilgangsstyringen er ikke integrert med personalsystemet	_	
Tilpasninger til spesialtilganger er utfordrende for forvaltere	_	
Definering av korrekte tilgangsprofiler	_	
Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig	_	
Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har	_	
Det er for dårlig støtte for logganalyse	_	
Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke	_	
Lite standardisering av tilgangsstyring på tvers av	_	

Evt. begrunnelse

helseforetakene _____

Spørsmål 2: I hvilken grad tror du følgende utsagn/faktorer kan forbedre tilgangsstyringen?

Nedenfor følger en liste av de viktigste faktorene dere valgte ut, og nå vil jeg at du skal rangere dem, ved å skrive et tall fra 1-8 i den lille ruten etter faktoren. Du må bruke alle tallene fra 1-8, der 1 = viktigst.

Ønsker du å komme med en begrunnelse for rangeringene kan du skrive dette inn i fritekstfeltet helt til høyre.

Evt. begrunnelse

Skjermbildet
for å beslutte tilgang bør komme
opp med én gang man forsøker _
å gå inn på en
pasient man ikke har tilgang til

_____
_____
_____
_____

Tilgangsstyringen
bør integreres med
personalsystemet slik at _
tilganger gis automatisk

_____
_____
_____
_____

Felles
retningslinjer for tilgangsstyring _
på regionalt eller nasjonalt nivå

_____
_____
_____
_____

Aktiv
bruk av innsynslogg for _
kvalitetssikring

_____
_____
_____
_____

Klarere
retningslinjer fra nasjonale _

_____
_____

	Evt. begrunnelse
myndigheter i forhold til hvordan tilgangsstyringen skal legges opp	_____
Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperiod er	_____
Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS	_____
Bedre oversikt over alt hva en bruker har tilgang til	_____

Tusen takk for at du tok deg tid til å delta i denne fjerde og siste del av undersøkelsen! Evt. spørsmål kan rettes til E-postadressen nederst på siden.

Denne runden av undersøkelsen kan nå avsluttes ved å trykke på knappen AVSLUTT nede i høyre hjørne.

Mvh
Rune Hystad
runehystad@gmail.com

Vedlegg 6 Svarene fra tredje spørreskjemarunde sortert i kategorier

Sluttbrukere

Spørsmål 1

Kategori	Utfordring	Identifisert av eksperter som viktig N=16		Identifisert av mer enn 30 % av ekspertene som viktig
Intern	Har ikke tilgang til pasientens medikamenter	2	12,5%	
Intern	Har ikke tilgang til å beslutte tilgang selv, og må få en kollega til å gi tilgang	0	0,0%	
Intern	Har ikke tilgang fra somatikk til psykiatri	3	18,8%	
Intern	Det mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal	7	43,8%	x
IT-sikkerhet	Det kreves for mange tastetrykk for å beslutte seg tilgang	8	50,0%	x
Intern	Har for vid tilgang til dokumenter	0	0,0%	
IT-sikkerhet	Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.	5	31,3%	x
Intern	Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket	5	31,3%	x
Intern	Mangler tilgang til tidligere undersøkelser	1	6,3%	
Intern	For lite opplæring i tilgangsstyring	8	50,0%	x
Intern	Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang	12	75,0%	x
IT-sikkerhet og Uformell	Bruker kan velge feil beslutningsmal	8	50,0%	x
Ekstern	Beslutningsstyrt tilgang fungerer bra, begrensningene ligger i lovverket	4	25,0%	
IT-sikkerhet	Det tar mye tid å måtte beslutte tilgang	4	25,0%	
IT-sikkerhet	Mangler info om hvorfor felter i skjermbilder er låst for redigering	4	25,0%	
IT-sikkerhet	Misvisende tekst i skjermbilder som skal fortelle at man må beslutte tilgang for å få frem ønsket informasjon	4	25,0%	
Intern	Når man beslutter tilgang har man automatisk bare tilgang i ett døgn	5	31,3%	x
IT-sikkerhet	Når man gir tilgang ang. tilsyn får man også tilgang til pasientjournalen	2	12,5%	
Intern	Automatisk/implisitt tilgang forsvinner for kort tid etter utskrivelse	4	25,0%	
Intern og IT-sikkerhet	Mangler implisitt/automatisk tilgang til pasientjournal	3	18,8%	
Intern	Det er en utfordring at brukere kan gi seg selv tilgang	1	6,3%	
IT-sikkerhet	Kan være lett å aktivere feil pasient, og derfor åpne feil journal	4	25,0%	
Intern	Man har ikke tilgang til endring/registrering i henvisninger etter at de er sendt	0	0,0%	
IT-sikkerhet og Intern	Man må beslutte tilgang for å få tilgang til PAS-delen, f.eks. bestilling av time	2	12,5%	

IT-sikkerhet	Skjermbilder oppdateres ikke ved bytte av pasient	3	18,8%	
Intern	Ikke alle brukere som har behov for det, har tilgang til nødretts-/blålystilgang	1	6,3%	
Intern	Nødrett/blålystilgang brukes i tilfeller hvor det ikke er tale om en nødrettssituasjon	1	6,3%	
Datasikkerhet	Utilstrekkelig funksjonalitet for sperring av journal	2	12,5%	
IT-sikkerhet	Utilstrekkelig funksjonalitet for registrering av pasientsamtykke	1	6,3%	
IT-sikkerhet	Prosesstankegangen er ikke tilstrekkelig på plass, f.eks. ved at brukere som ikke er tilknyttet samme avdeling som pasientene de behandler, får bredere eller smalere tilgang enn ønskelig	3	18,8%	
Ekstern	Kan ikke styre tilgang til et pasientforløp (en henvisningsperiode) på tvers av virksomheter	2	12,5%	
Datasikkerhet	Tilgangsstyringen er ikke integrert med personalsystemet	1	6,3%	
IT-sikkerhet	Mangler funksjonalitet for beslutningsstyrt tilgang (f.eks. rapporter, lokalisering og listefunksjonalitet)	2	12,5%	
IT-sikkerhet	Ikke tilstrekkelig antall/dekkende implisitte beslutningsmaler	5	31,3%	x
Intern	Tilpasninger til spesialtilganger er utfordrende for forvaltere	1	6,3%	
IT-sikkerhet	Psykiatrifilter gir ikke alltid brukeren definerte tilganger i alle skjermbilder	2	12,5%	
Intern	Definering av korrekte tilgangsprofiler	4	25,0%	
IT-sikkerhet	Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig	4	25,0%	
Intern	Det er gjort mange avvik fra beslutningsstyrt tilgang som bygger på dagens lovverk	0	0,0%	
IT-sikkerhet	Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har	4	25,0%	
Intern	Stor treghet ved administrering av tilganger	1	6,3%	
IT-sikkerhet	Det er for dårlig støtte for logganalyse	2	12,5%	
IT-sikkerhet	Vanskelig å følge opp loggene som skal kontrolleres for å finne eventuelle snokere	2	12,5%	
Intern	Det er utfordrende å motivere brukere til å dokumentere korrekte data ved eksplisitte tilganger	3	18,8%	
IT-sikkerhet	Kan ikke tidsbegrense tilgang gitt via profiler	0	0,0%	
Intern	Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke	1	6,3%	
Intern	Hvis tilgangene settes for vide, vil brukerne sjelden måtte beslutte tilgang, som kan medføre en risiko for manglende kompetanse ved en kritisk situasjon der tilgang må besluttes	3	18,8%	
IT-sikkerhet	Vanskelig å gi tilgang til brukere med mange ulike funksjoner	1	6,3%	
Intern	For lite tid til å gå gjennom tilgangene for å passe på at de er i samsvar med lover og regler	1	6,3%	

Intern	Interessekonflikt mellom eier (HF) og forvalter av DIPS ift. tilgangsstyring	0	0,0%	
Ekstern	Lite standardisering av tilgangsstyring på tvers av helseforetakene	2	12,5%	
Intern	Krevende å få enkelte grupper av sluttbrukere til å anerkjenne at beslutningsstyrt tilgang er en hensiktsmessig løsning for å oppfylle krav om riktig tilgangsstyring	1	6,3%	
IT-sikkerhet	Vanskelig å gi brukere tilganger som gjør at de ikke må bruke grønnlys/beslutte tilgang ofte	1	6,3%	
Uformell	Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang	5	31,3%	x
Intern	Hver enkelt virksomhet har ikke forutsetninger eller kapasitet til å forvalte slik komplisert brukeradministrasjonen og sørge for korrekte tilganger til sine egne ansatte	3	18,8%	
Ekstern	Beslutningsstyrt tilgang er knyttet til virksomhetsnivå, men virksomhetsnivået er egentlig irrelevant for taushetsplikten etter helsepersonelloven § 25 og 45	2	12,5%	

Systemforvaltere

Spørsmål 1

Kategori	Utfordring	Identifisert av eksperter som viktig N=16		Identifisert av mer enn 35% av ekspertene som viktig
Intern	Har ikke tilgang til pasientens medikamenter	0	0,0%	
Intern	Har ikke tilgang til å beslutte tilgang selv, og må få en kollega til å gi tilgang	1	6,3%	
Intern	Har ikke tilgang fra somatikk til psykiatri	1	6,3%	
Intern	Det mangler/er for få passende eksplisitte beslutningsmaler ift. reell grunn for åpning av journal	4	25,0%	
IT-sikkerhet	Det kreves for mange tastetrykk for å beslutte seg tilgang	3	18,8%	
Intern	Har for vid tilgang til dokumenter	2	12,5%	
IT-sikkerhet	Man må for ofte beslutte tilgang, f.eks. ved sjekk av prøvesvar, utskrift til fastlege, avsluttet kontakt osv.	1	6,3%	
Intern	Å måtte beslutte tilgang gir en følelse av å gjøre noe ulovlig, og å være mistrodd og overvåket	2	12,5%	
Intern	Mangler tilgang til tidligere undersøkelser	1	6,3%	
Intern	For lite opplæring i tilgangsstyring	5	31,3%	
Intern	Uklarhet i bruk av fritekstfeltet når man beslutter seg tilgang	0	0,0%	
IT-sikkerhet og Uformell	Bruker kan velge feil beslutningsmal	2	12,5%	

Ekstern	Beslutningsstyrt tilgang fungerer bra, begrensningene ligger i lovverket	2	12,5%	
IT-sikkerhet	Det tar mye tid å måtte beslutte tilgang	2	12,5%	
IT-sikkerhet	Mangler info om hvorfor felter i skjermbilder er låst for redigering	3	18,8%	
IT-sikkerhet	Misvisende tekst i skjermbilder som skal fortelle at man må beslutte tilgang for å få frem ønsket informasjon	4	25,0%	
Intern	Når man beslutter tilgang har man automatisk bare tilgang i ett døgn	0	0,0%	
IT-sikkerhet	Når man gir tilgang ang. tilsyn får man også tilgang til pasientjournalen	1	6,3%	
Intern	Automatisk/implisitt tilgang forsvinner for kort tid etter utskrivelse	0	0,0%	
Intern og IT-sikkerhet	Mangler implisitt/automatisk tilgang til pasientjournal	1	6,3%	
Intern	Det er en utfordring at brukere kan gi seg selv tilgang	2	12,5%	
IT-sikkerhet	Kan være lett å aktivere feil pasient, og derfor åpne feil journal	0	0,0%	
Intern	Man har ikke tilgang til endring/registrering i henvisninger etter at de er sendt	1	6,3%	
IT-sikkerhet og Intern	Man må beslutte tilgang for å få tilgang til PAS-delen, f.eks. bestilling av time	1	6,3%	
IT-sikkerhet	Skjermbilder oppdateres ikke ved bytte av pasient	5	31,3%	
Intern	Ikke alle brukere som har behov for det, har tilgang til nødretts-/blålystilgang	0	0,0%	
Intern	Nødrett/blålystilgang brukes i tilfeller hvor det ikke er tale om en nødrettssituasjon	2	12,5%	
Datasikkerhet	Utilstrekkelig funksjonalitet for sperring av journal	7	43,8%	x
IT-sikkerhet	Utilstrekkelig funksjonalitet for registrering av pasientsamtykke	1	6,3%	
IT-sikkerhet	Prosesstankegangen er ikke tilstrekkelig på plass, f.eks. ved at brukere som ikke er tilknyttet samme avdeling som pasientene de behandler, får bredere eller smalere tilgang enn ønskelig	4	25,0%	
Ekstern	Kan ikke styre tilgang til et pasientforløp (en henvisningsperiode) på tvers av virksomheter	2	12,5%	
Datasikkerhet	Tilgangsstyringen er ikke integrert med personalsystemet	8	50,0%	x
IT-sikkerhet	Mangler funksjonalitet for beslutningsstyrt tilgang (f.eks. rapporter, lokalisering og listefunksjonalitet)	4	25,0%	
IT-sikkerhet	Ikke tilstrekkelig antall/dekkende implisitte beslutningsmaler	5	31,3%	
Intern	Tilpasninger til spesialtilganger er utfordrende for forvaltere	7	43,8%	x
IT-sikkerhet	Psykiatrifilter gir ikke alltid brukeren definerte tilganger i alle skjermbilder	1	6,3%	
Intern	Definering av korrekte tilgangsprofiler	6	37,5%	x
IT-sikkerhet	Brukergrensesnittet i administrasjonsdelen av DIPS er for lite intuitivt og oversiktlig	9	56,3%	x
Intern	Det er gjort mange avvik fra beslutningsstyrt tilgang som bygger på dagens lovverk	3	18,8%	

IT-sikkerhet	Det er umulig/vanskelig å raskt få en oversikt over hvilke tilganger en spesifikk bruker har	6	37,5%	x
Intern	Stor treghet ved administrering av tilganger	3	18,8%	
IT-sikkerhet	Det er for dårlig støtte for logganalyse	10	62,5%	x
IT-sikkerhet	Vanskelig å følge opp loggene som skal kontrolleres for å finne eventuelle snokere	5	31,3%	
Intern	Det er utfordrende å motivere brukere til å dokumentere korrekte data ved eksplisitte tilganger	5	31,3%	
IT-sikkerhet	Kan ikke tidsbegrense tilgang gitt via profiler	3	18,8%	
Intern	Rutiner for bestilling og/eller avslutning av tilgang etterleves ikke	6	37,5%	x
Intern	Hvis tilgangene settes for vide, vil brukerne sjelden måtte beslutte tilgang, som kan medføre en risiko for manglende kompetanse ved en kritisk situasjon der tilgang må besluttes	2	12,5%	
IT-sikkerhet	Vanskelig å gi tilgang til brukere med mange ulike funksjoner	5	31,3%	
Intern	For lite tid til å gå gjennom tilgangene for å passe på at de er i samsvar med lover og regler	2	12,5%	
Intern	Interessekonflikt mellom eier (HF) og forvalter av DIPS ift. tilgangsstyring	3	18,8%	
Ekstern	Lite standardisering av tilgangsstyring på tvers av helseforetakene	8	50,0%	x
Intern	Krevende å få enkelte grupper av sluttbrukere til å anerkjenne at beslutningsstyrt tilgang er en hensiktsmessig løsning for å oppfylle krav om riktig tilgangsstyring	5	31,3%	
IT-sikkerhet	Vanskelig å gi brukere tilganger som gjør at de ikke må bruke grønnlys/beslutte tilgang ofte	3	18,8%	
Uformell	Brukere har manglende forståelse for bruken av beslutningsstyrt tilgang	4	25,0%	
Intern	Hver enkelt virksomhet har ikke forutsetninger eller kapasitet til å forvalte slik komplisert brukeradministrasjonen og sørge for korrekte tilganger til sine egne ansatte	1	6,3%	
Ekstern	Beslutningsstyrt tilgang er knyttet til virksomhetsnivå, men virksomhetsnivået er egentlig irrelevant for taushetsplikten etter helsepersonelloven § 25 og 45	2	12,5%	

Sluttbrukere

Spørsmål 2

Kategori	Forbedring	Identifisert av eksperter som viktig N=16		Identifisert av mer enn 35 % av ekspertene som viktig
IT-sikkerhet	Redusere antall klikk som trengs for å beslutte seg tilgang	9	56,3%	x

IT-sikkerhet	Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til	11	68,8%	x
IT-sikkerhet	Mulighet for selv å kunne opprette egendefinert beslutningsmal	6	37,5%	x
Intern	Den besluttede tilgangen bør automatisk vare i mer enn én dag	6	37,5%	x
Intern	Lengre implisitt/automatisk tilgang til en journal etter en konsultasjon eller utskrivelse	3	18,8%	
Intern	Medisinkort bør være tilgjengelig for alle avdelinger	3	18,8%	
Intern og IT-sikkerhet	Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen	8	50,0%	x
IT-sikkerhet	Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang	9	56,3%	x
IT-sikkerhet	Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn	9	56,3%	x
Datasikkerhet	Forfatter av dokument bør enkelt kunne sperre enkeltdokumenter/avsnitt/setninger i dialog med pasienten	2	12,5%	
IT-sikkerhet	Bilder i DIPS bør bli tilgjengelige i det man har benyttet grønnlyset, slik at man slipper å lukke og åpne skjermbilder	4	25,0%	
Intern	Bruke beslutningsmal/grønnlys i stedet for blålys/nødrettstilgang	5	31,3%	
Intern	Nødrettsstilgang/blålystilgang må kunne utløses/legitimeres ut fra det enkelte helsepersonells skjønn/vurdering	2	12,5%	
IT-sikkerhet	Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang	7	43,8%	x
IT-sikkerhet	Entydige meldinger om hvorfor man ikke får åpne/se dokumenter/labsvar man ønsker å åpne	5	31,3%	
Intern	Flere eksplisitte beslutningsmaler for å kunne dekke reell grunn for åpning av journal	3	18,8%	
IT-sikkerhet	Valg for "gruppe-beslutning" hvis man skal gjøre oppslag på flere pasienter, f.eks. ved sammenligning av pasienter (diagnoser, koder osv.)	3	18,8%	
Intern	Informasjon tilbake i tid bør være tilgjengelige uten at man må beslutte tilgang	5	31,3%	
IT-sikkerhet	Forbedre søkemuligheter på pasienter	3	18,8%	
Intern	Ta i bruk funksjonalitet som innebærer at for å få tilgang, må en annen gi deg tilgang, f.eks. for forvaltere	0	0,0%	
Intern	Tilgang til retting ved feilsendt henvisning til annen avdeling	5	31,3%	
IT-sikkerhet	Implementere beslutningsstøtte i forhold til behandlingsforløp	2	12,5%	
Datasikkerhet	Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk	1	6,3%	
Ekstern	Felles retningslinjer for tilgangsstyring på regionalt eller nasjonalt nivå	5	31,3%	
Ekstern	Strengere føringer for hva lokale helseforetak kan bestemme ift. tilgangsstyring	1	6,3%	
Intern	Forbedre rutiner for bestilling og avslutning av tilganger	5	31,3%	

Intern	Forbedre kommunikasjon mellom helseforetak og forvalter rundt tilgangsstyring	2	12,5%	
Intern	Hyppigere kontroll av hvem som har tilgang til hva	3	18,8%	
Intern	Aktiv bruk av innsynslogg for kvalitetssikring	1	6,3%	
Datasikkerhet	Det bør benyttes systemer som kontinuerlig analyserer innsynslogger	0	0,0%	
Ekstern	Klarere retningslinjer fra nasjonale myndigheter i forhold til hvordan tilgangsstyringen skal legges opp	1	6,3%	
Intern	Forbedre rutiner rundt opplæring/informasjon til sluttbrukere om tilgangsstyring, og lover og regler for dette	2	12,5%	
IT-sikkerhet	Mer fleksible løsninger på tildeling av tilganger, uten at oversikten forsvinner for forvalterne	2	12,5%	
Intern	Tilgang basert på eksplisitt beslutningsstyrt tilgang, vil for de som har både eksplisitt og implisitt beslutningsmyndighet, kunne unngå å bruke den implisitte tilgangen. Den videste eksplisitte beslutningsstyrte tilgang vil gi tilgang til det meste	1	6,3%	
IT-sikkerhet	Mer prosessorientert tilgangsstyring/videreutvikling av implisitte beslutningsmaler for å støtte oppunder arbeidsflyt	2	12,5%	
Ekstern	Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperioder	1	6,3%	
IT-sikkerhet	Man bør kunne styre tilgang på tvers av lokaliseringer, avdelinger og seksjoner/fagområder, også innenfor samme virksomhet	3	18,8%	
IT-sikkerhet	Utvikle beslutningsstyrt tilgang for rapporter og listefunksjonalitet	0	0,0%	
IT-sikkerhet	Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS	0	0,0%	
IT-sikkerhet	Bedre oversikt over alt hva en bruker har tilgang til	5	31,3%	
Intern	Flere muligheter teknisk for å differensiere tilgang til beslutningsmaler (er du f.eks. ansatt på intensivenhet som sykepleier skal du kunne få tilgang til en annen beslutningsmal enn andre spl. på vanlig post)	3	18,8%	
Intern	Gi videre tilganger for å unngå spesialtilpasninger	1	6,3%	
Intern	Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon	6	37,5%	x
IT-sikkerhet	En definisjon av beslutning må kunne knyttes til alle beslutninger som gjelder behandling av pasienten	2	12,5%	
IT-sikkerhet	Mer fleksibilitet for inn- og utmelding av ressurser (brukertilgang) til for eksempel traumeteam	1	6,3%	

Systemforvaltere

Spørsmål 2

Kategori	Forbedring	Identifisert av eksperter som viktig N=16 (%)		Identifisert av mer enn 40 % av ekspertene som viktig
IT-sikkerhet	Redusere antall klikk som trengs for å beslutte seg tilgang	5	31,3%	
IT-sikkerhet	Skjermbildet for å beslutte tilgang bør komme opp med én gang man forsøker å gå inn på en pasient man ikke har tilgang til	7	43,8%	x
IT-sikkerhet	Mulighet for selv å kunne opprette egendefinert beslutningsmal	3	18,8%	
Intern	Den besluttede tilgangen bør automatisk vare i mer enn én dag	0	0,0%	
Intern	Lengre implisitt/automatisk tilgang til en journal etter en konsultasjon eller utskrivelse	0	0,0%	
Intern	Medisinkort bør være tilgjengelig for alle avdelinger	3	18,8%	
Intern og IT-sikkerhet	Ved henvisning fra psykiatrisk til somatisk avdeling, bør man få tilgang til henvisningen	3	18,8%	
IT-sikkerhet	Ha med eksempler for begrunnelse i fritekstfeltet når man beslutter seg tilgang	0	0,0%	
IT-sikkerhet	Mulighet for å kunne velge en standard beslutningsmal som gjelder for alle journalinnsyn	2	12,5%	
Datasikkerhet	Forfatter av dokument bør enkelt kunne sperre enkeltdokumenter/avsnitt/setninger i dialog med pasienten	4	25,0%	
IT-sikkerhet	Bilder i DIPS bør bli tilgjengelige i det man har benyttet grønnlyset, slik at man slipper å lukke og åpne skjermbilder	4	25,0%	
Intern	Bruke beslutningsmal/grønnlys i stedet for blålys/nødrettstilgang	3	18,8%	
Intern	Nødrettsstilgang/blålystilgang må kunne utløses/legitimeres ut fra det enkelte helsepersonells skjønn/vurdering	1	6,3%	
IT-sikkerhet	Mulighet for å velge hva man får tilgang til når man beslutter seg tilgang	3	18,8%	
IT-sikkerhet	Entydige meldinger om hvorfor man ikke får åpne/se dokumenter/labsvar man ønsker å åpne	6	37,5%	
Intern	Flere eksplisitte beslutningsmaler for å kunne dekke reell grunn for åpning av journal	5	31,3%	
IT-sikkerhet	Valg for "gruppe-beslutning" hvis man skal gjøre oppslag på flere pasienter, f.eks. ved sammenligning av pasienter (diagnoser, koder osv.)	3	18,8%	
Intern	Informasjon tilbake i tid bør være tilgjengelige uten at man må beslutte tilgang	1	6,3%	
IT-sikkerhet	Forbedre søkemuligheter på pasienter	0	0,0%	
Intern	Ta i bruk funksjonalitet som innebærer at for å få tilgang, må en annen gi deg tilgang, f.eks. for forvaltere	1	6,3%	
Intern	Tilgang til retting ved feilsendt henvisning til annen avdeling	2	12,5%	
IT-sikkerhet	Implementere beslutningsstøtte i forhold til behandlingsforløp	4	25,0%	

Datasikkerhet	Tilgangsstyringen bør integreres med personalsystemet slik at tilganger gis automatisk	10	62,5%	x
Ekstern	Felles retningslinjer for tilgangsstyring på regionalt eller nasjonalt nivå	9	56,3%	x
Ekstern	Strengere føringer for hva lokale helseforetak kan bestemme ift. tilgangsstyring	3	18,8%	
Intern	Forbedre rutiner for bestilling og avslutning av tilganger	5	31,3%	
Intern	Forbedre kommunikasjon mellom helseforetak og forvalter rundt tilgangsstyring	5	31,3%	
Intern	Hyppigere kontroll av hvem som har tilgang til hva	2	12,5%	
Intern	Aktiv bruk av innsynslogg for kvalitetssikring	10	62,5%	x
Datasikkerhet	Det bør benyttes systemer som kontinuerlig analyserer innsynslogger	6	37,5%	
Ekstern	Klarere retningslinjer fra nasjonale myndigheter i forhold til hvordan tilgangsstyringen skal legges opp	10	62,5%	x
Intern	Forbedre rutiner rundt opplæring/informasjon til sluttbrukere om tilgangsstyring, og lover og regler for dette	5	31,3%	
IT-sikkerhet	Mer fleksible løsninger på tildeling av tilganger, uten at oversikten forsvinner for forvalterne	5	31,3%	
Intern	Tilgang basert på eksplisitt beslutningsstyrt tilgang, vil for de som har både eksplisitt og implisitt beslutningsmyndighet, kunne unngå å bruke den implisitte tilgangen. Den videste eksplisitte beslutningsstyrte tilgang vil gi tilgang til det meste	2	12,5%	
IT-sikkerhet	Mer prosessorientert tilgangsstyring/videreutvikling av implisitte beslutningsmaler for å støtte oppunder arbeidsflyt	6	37,5%	
Ekstern	Logikk for tilgangsstyring bør gjøres nasjonalt og knyttes til pasientforløp/henvisningsperioder	7	43,8%	x
IT-sikkerhet	Man bør kunne styre tilgang på tvers av lokaliseringer, avdelinger og seksjoner/fagområder, også innenfor samme virksomhet	4	25,0%	
IT-sikkerhet	Utvikle beslutningsstyrt tilgang for rapporter og listefunksjonalitet	5	31,3%	
IT-sikkerhet	Forenkle prosessen med tilgangsopprettelse og stenging i administrasjonsdelen i DIPS	9	56,3%	x
IT-sikkerhet	Bedre oversikt over alt hva en bruker har tilgang til	8	50,0%	x
Intern	Flere muligheter teknisk for å differensiere tilgang til beslutningsmaler (er du f.eks. ansatt på intensivenhet som sykepleier skal du kunne få tilgang til en annen beslutningsmal enn andre spl. på vanlig post)	1	6,3%	
Intern	Gi videre tilganger for å unngå spesialtilpasninger	1	6,3%	
Intern	Sikre god kunnskap og opplæring om forvaltning av tilgangsstyring og brukeradministrasjon	6	37,5%	

IT-sikkerhet	En definisjon av beslutning må kunne knyttes til alle beslutninger som gjelder behandling av pasienten	3	18,8%
IT-sikkerhet	Mer fleksibilitet for inn- og utmelding av ressurser (brukertilgang) til for eksempel traumeteam	3	18,8%