Direktoratet for e-helse

Tilgangsstyring i helse- og omsorgssektoren

Anbefaling av tillitsmodell for data- og dokumentdeling

HITR 1223:2019

Publikasjonens tittel:
Tilgangsstyring i helse- og omsorgssektoren
Anbefaling av tillitsmodell for data- og dokumentdeling

Rapportnummer:
HITR 1223:2019

Utgitt:
03/2019

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Besøksadresse:
Verkstedveien 1, 0277 Oslo
Tlf.: 21 49 50 70

Publikasjonen kan lastes ned på:

www.ehelse.no

Sammendrag

Helse- og omsorgssektoren står midt i et digitalt skifte hvor nye samhandlingsformer og teknologiske løsninger blir tatt i bruk av sektorens virksomheter for å fremme bedre liv og helse for innbyggerne. De nye samhandlingsformene utfordrer status quo for bruken av e-helse og helseteknologi da de forutsetter samhandling på tvers av virksomheter og områder i sektoren. I dagens situasjon er det flere hindre som vil påvirke utviklingstakten på dette området om de ikke løses. Ett sentralt område er tilgangsstyring.

Data- og dokumentdeling er samhandlingsformer som det forventes vil få økt utbredelse og volum i sektoren innenfor planperioden til dagens e-helse strategi. Økt samhandling og deling av helseinformasjon vil gi bedre beslutningsgrunnlag for behandlende helsepersonell. Helsedata har også høy verdi for aktører som har til hensikt å misbruke dataene. Det må derfor sørges for at uvedkommende ikke får tilgang, samtidig som de med tjenstlig behov faktisk får tilgang. Dette gjelder også datakilder med relevante opplysninger som befinner seg utenfor helsepersonellets egen virksomhet.

Tilgjengeliggjøring av helsedata til helsepersonell i andre virksomheter forutsetter at det er tillit til at samhandlingspartene det deles data med behandler dataene i henhold til gjeldende lover og forskrifter. Dagens tilgangsstyring i de ulike virksomhetene er ikke innrettet til å adressere de sikkerhetsutfordringene som nye samhandlingsformer på tvers av virksomheter medfører. Det er behov for å etablere overordnede prinsipper og krav som skal gjelde for tilgangsstyring, slik at ikke sikkerhet blir et hinder for utbredelse og bruk av nye samhandlingsformer.

Formålet med denne rapporten er å vurdere ulike alternativer for tilgangsstyring på tvers av virksomheter, med fokus på data- og dokumentdeling, og anbefale en utviklingsretning sektoren bør bevege seg mot.

Rapporten skisserer to alternative utviklingsretninger: harmoniseringsalternativet og samordningsalternativet. Harmoniseringsalternativet omfatter styrking av internkontroll og informasjonssikkerhet i virksomhetene med målrettet standardisering på sentrale områder. Samordningsalternativet beskriver et felles tillitsanker som vil bidra til økt skalerbarhet for å imøtekomme behovene forbundet med sektorens skifte mot nye samhandlingsformer. Rapporten anbefaler at samordningsalternativet legges til grunn for det videre arbeidet med tilgangsstyring for data- og dokumentdeling.

Innhold

1 Bakgrunn for rapporten

1.1 Bakgrunn

Det er en helsepolitisk målsetting for IKT-utviklingen at helsepersonell skal ha rask, enkel og sikker tilgang til alle nødvendige pasient- og brukeropplysninger. Dette gjelder gjennom hele behandlingsforløpet, uavhengig av hvor i landet pasienten blir syk eller får behandling. For å imøtekomme målsettingen pågår det flere større initiativer i sektoren med å ta i bruk nye former for elektronisk samhandling.

For at nye samhandlingsformer som data- og dokumentdeling[1] skal kunne tas i bruk er det nødvendig å avklare hvordan tilgangsstyringen for disse samhandlingsformene best kan ivaretas. I dagens situasjon for tilgangsstyring i sektoren er det en rekke hindre som vil hemme utviklingen av nye samhandlingsformer dersom de ikke blir adressert tidlig nok. Dette gjelder særlig der det er hindre som må adresseres innenfor eksisterende lover og forskrifter, samt innretningen av den underliggende tekniske infrastrukturen som skal muliggjøre effektiv tilgangsstyring ved økt data- og dokumentdeling.

Elektronisk samhandling forutsetter et rettslig grunnlag, og kan omfatte juridiske krav til både innhold, prosesser og løsninger. Tidligere forbud mot deling av helseopplysninger mellom virksomheter ble opphevet ved lovendringer i 2015. Helselovgivningen gir særregler for behandling av helseopplysninger, i tillegg gjelder personopplysningsloven og -forordningen. Deling av helseopplysninger krever hjemmel for utlevering og hjemmel for å motta og behandle opplysningene. Lover og forskrifter bør utformes for å legge til rette for effektiv elektronisk samhandling mellom virksomheter, omsorgsnivåer, helsepersonell og innbyggere.

For at det skal kunne gis tilgang til relevante og oppdaterte pasientopplysninger som er lagret utenfor egen virksomhet, er det en forutsetning at virksomheter som skal tilgjengeliggjøre data har tilstrekkelig tillit til:

- at helsepersonell og annet personell som ber om tilgang faktisk er den de utgir seg for å være,
- at opplysninger om helsepersonellet er korrekt, og
- at tilgangsforespørselen er basert på et tjenstlig behov.

Dette forutsetter at virksomhetene har tilstrekkelig og pålitelig informasjon om hvem vedkommende er (identitet) og hvilke rettigheter vedkommende har (autorisasjon).

Med utgangspunkt i dagens situasjon kan det ikke forutsettes at alle virksomheter vil ha ressurser til å etablere tillitsforhold til alle andre virksomheter i sektoren. Dette vil skape et etterslep og utgjøre et hinder i innføring av data- og dokumentdeling.

---

[1] Med datadeling menes i dette dokumentet deling av strukturerte data mellom helseaktører gjennom felles ressurser eller tjenester i sanntid.

Med dokumentdeling menes i dette dokumentet samhandlingsformen der en konsument kan søke etter publiserte dokumenter fra **andre** produsenter og laste ned dokumenter fra et dokumentlager.

Utfordringer forbundet med sektorens tilgangsstyring er også tidligere blitt utredet. Utredningen av behovet for en nasjonal sikkerhetsinfrastruktur i helse- og omsorgssektoren (NSI[2]) tok utgangspunkt i og anbefalte tiltak for å forbedre samhandling på tvers av virksomheter for de samhandlingsformer som på utredningstidspunktet var utbredt i sektoren. I forlengelsen av arbeidet med NSI ble det også utredet og vurdert nåsituasjon og samordning av PKI-løsninger, da disse har vært introdusert og tatt i bruk ulikt i sektoren. Samhandlingsformene som ble utredet var ikke knyttet til de nye formene som omfatter data- og dokumentdeling. I forlengelsen ble det i gang satt et arbeid med å se på en felles autentiseringsløsning for bruk mellom virksomheter og som har resultert i etablering av HelseID[3]. Vurderingen i denne rapporten er en videreføring av tidligere arbeid, men hvor fokuset er på tilgangsstyring for de nye samhandlingsformene data- og dokumentdeling.

1.2 Omfang og avgrensninger

Denne rapporten vurderer ulike utviklingsretninger for håndtering av tilgangsstyring på tvers av virksomheter i helse- og omsorgssektoren, med særskilt fokus på samhandlingsformene data- og dokumentdeling. Eksisterende samhandlingsformer som meldingsutveksling inngår ikke i rapporten. Vurderingene i rapporten er gjort ut i fra gjeldende lover og forskrifter.

Det anbefalte alternativet for tilgangsstyring på tvers av virksomheter skal legge til rette for enkel og effektiv innføring av data- og dokumentdeling. Rapporten anbefaler ett alternativ for tilgangsstyring for data- og dokumentdeling, som det er ønske om å prøve ut i 2019. Rapporten er videre tenkt å gi økt forutsigbarhet for aktørene i sektoren og tilgrensende prosjekter som er påvirket av, eller har behov for, tilgangsstyring på tvers av virksomheter.

Vurderingene i rapporten omfatter ikke tilgangsstyring internt i virksomhetene. Interne prosesser og modenhet innen informasjonssikkerhet er derimot sentralt for at andre virksomheter skal kunne ha tilstrekkelig tillit til å gjøre helse- og pasientopplysninger tilgjengelig. Dette utfordringsområdet adresseres særskilt i rapporten under alternative utviklingsretninger.

Innbyggers tilgang til egne helseopplysninger er ikke innenfor utredningens omfang. Alternativene som vurderes i rapporten kan også være overførbare til innbyggertjenester, uten at det er diskutert eksplisitt.

1.3 Tilnærming

Rapportens vurderinger baserer seg på analyse av alternative fremtidige utviklingstrekk for data- og dokumentdeling som det vil være behov for å styrke tilgangsstyring for. Det har vært viktig å kartlegge dagens situasjon innen relevante prosesser som omhandler identitets- og tilgangsstyring, samt hva som er ønsket fremtidig situasjon frem mot Én innbygger – én journal[4] og hvordan Direktoratet for e-helse kan gå frem for å legge til rette for dette.

I tett dialog med sektoren har ulike utfordringer ved dagens situasjon og mulighetsrommet for tiltak blitt drøftet. Det har særlig blitt sett nærmere på behovene for økt standardisering og

[2] *Nasjonal sikkerhetsinfrastruktur for helse- og omsorgssektoren - Forstudie*. Helsedirektoratet 2013, IS-2120.

[3] HelseIDs nettsider.

[4] Meld. St. 9 (2012-2013) Én innbygger – én journal.

økt samordning av felles funksjoner i sektoren for å etablere og ivareta krav til tilgangsstyring.

Gjennom dette arbeidet er tre mulige alternativer (utviklingsretninger) for fremtidig tilgangsstyring utarbeidet og vurdert. Alternativene tar sikte på en fremtidig ønsket situasjon, hvor dagens utfordringer adresseres gjennom realisering av et sett med tiltak og en overordnet tillitsmodell. Innspillsrunder har vært benyttet til å konkretisere de ulike alternativene, og for å skape forståelse for de konsekvenser og effekter som hvert alternativ vil medføre.

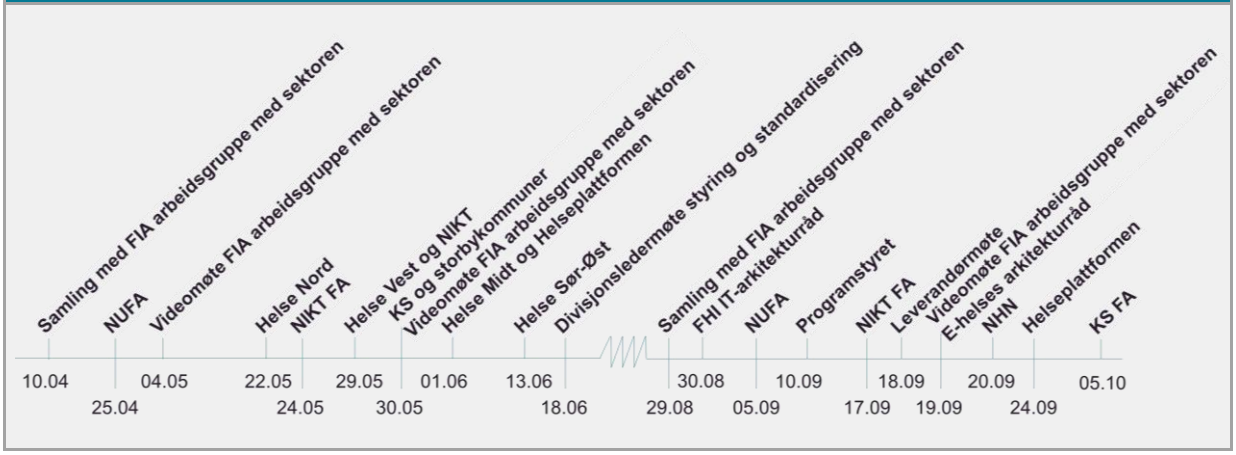
Et alternativ beskriver i denne sammenhengen en tilnærming sektoren kan benytte for å nå og opprettholde ønsket situasjon innen tilgangsstyring. Et alternativ kan for eksempel ha høyere kostnad, men samtidig legge bedre til rette for data- og dokumentdeling fordi det er mer tillitsskapende, skalerer bedre, er sikrere eller mer tilpasningsdyktig enn andre alternativer.

1.4 Forankring

Forankring og innspill fra sektoren har vært svært viktig for kartlegging av dagens situasjon og behov, samt for vurdering av om foreslåtte tiltak er gjennomførbare. Hovedforumet for forankring har vært en arbeidsgruppe i regi av FIA prosjektet Data- og dokumentdeling, som inkluderer representanter fra de regionale helseforetakene, NIKT, KS, KINS og enkelte storbykommuner. Se vedlegg 1 for en liste over deltakende virksomheter.

Det har også blitt avholdt separate møter med hver helseregion og kommunerepresentantene i arbeidsgruppen for å spenne ut mulighetsrommet og diskutere ønsket ambisjonsnivå og utviklingsretning. Orienterings-, innspills-, og drøftingsmøter med andre berørte aktører og initiativer har også blitt avholdt. Figur 1 viser forankringsaktivitetene som har blitt gjennomført i forbindelse med arbeidet. I tillegg ble det gjennomført en skriftlig innspillsrunde på et utkast av denne rapporten.

Figur 1 – Møter med sektoren i forbindelse med vurderingen

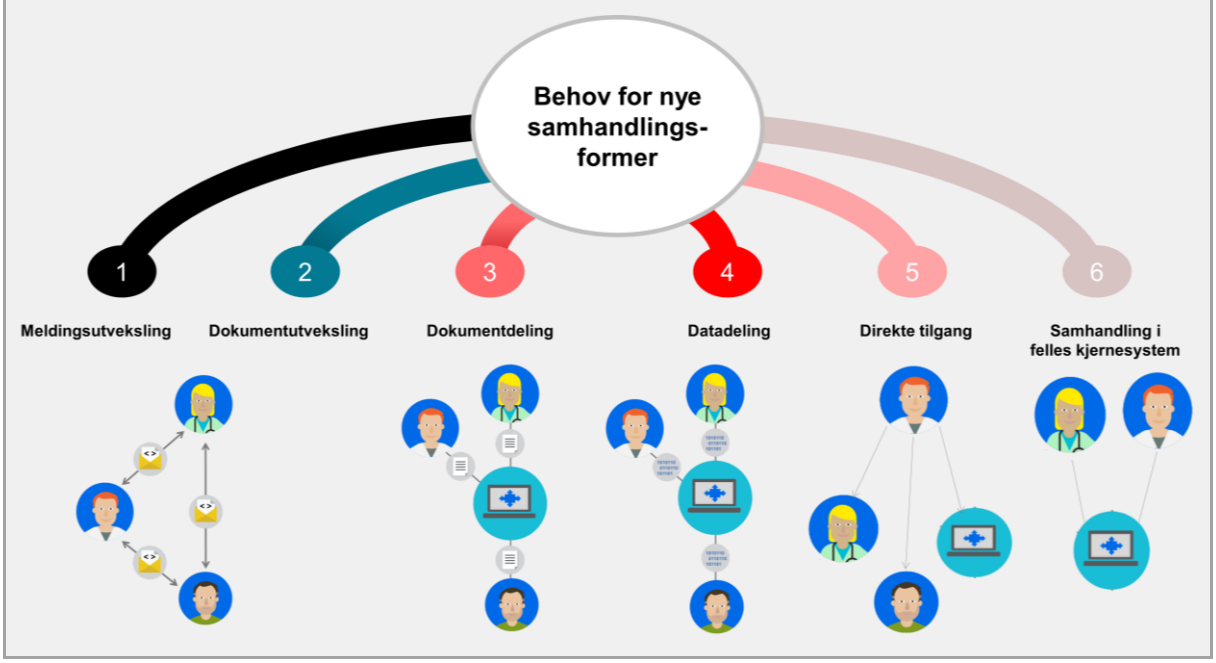


2 Dagens samhandling

Helse- og omsorgssektoren har behov for mer effektiv samhandling for å øke tilgjengeligheten til relevante helseopplysninger som ligger lagret i andre virksomheter og i sentrale kilder. Eksisterende samhandlingsformer som meldingsutveksling dekker noe av behovet, men ny teknologi muliggjør i økende grad at helsepersonell selv kan søke etter og få tilgang til data ved behov. I tillegg til meldingsutveksling benyttes sentrale registre som kjernejournal, medisinske kvalitetsregistre og grunndataplattformen til deling av helseinformasjon. Det finnes også eksempler på at helsepersonell får direkte tilgang til fagsystem i samarbeidende virksomheter hvor de ikke har et ansettelsesforhold. Direkte tilgang er en samhandlingsform som krever mye forvaltning, og det er krevende for helsepersonell å ha brukere i flere andre virksomheter.

Figur 2 nedenfor viser seks ulike former for samhandling, inkludert de nye samhandlingsformene.

Figur 2 – Samhandlingsformer i helse- og omsorgssektoren

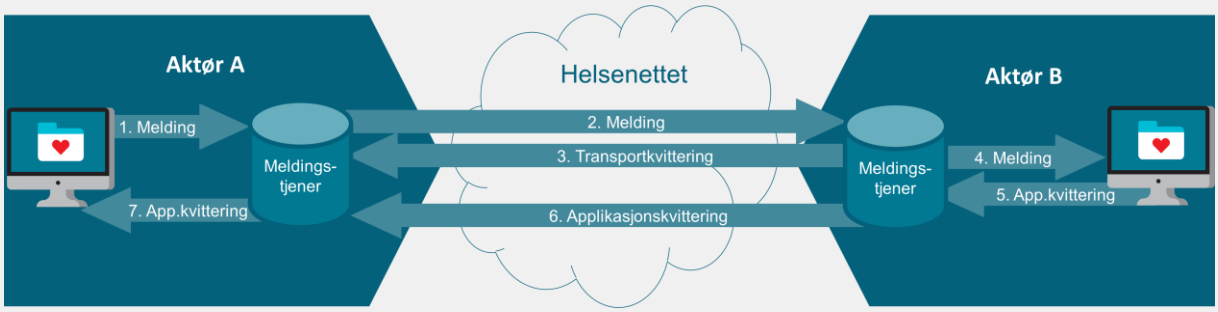


Et behandlingsforløp involverer ofte helsepersonell fra forskjellige virksomheter i forskjellige deler av helsetjenesten. Særlig gjelder dette pasientgrupper med kroniske og sammensatte helseproblemer. Kvaliteten på behandlingen er dermed avhengig av samhandling mellom virksomhetene som er delaktige i et behandlingsforløp. Ordninger som fritt behandlingsvalg bidrar også til behovet for samhandling. Innbyggerne forventer at helsepersonell har tilgang til all informasjon som er nødvendig for behandling av sitt sykdomsbilde. I tillegg forventes det at personvern er ivaretatt, og at sensitive opplysninger er utilgjengelige for helsepersonell som ikke har tjenstlig behov og for andre uvedkommende.

2.1 Fra meldingsutveksling til data- og dokumentdeling

Etter stortingsmelding «Én innbygger – én journal» (2012-2013) ble det et økt fokus på å dele helseinformasjon ved hjelp av andre samhandlingsformer enn meldingsutveksling. Regelverket som skulle legge til rette for dette ble endret 01.01.2015. Frem til dette lå mye av fokuset på å sikre konfidensialitet i datautvekslingen, og tilgangsstyringen var bygd opp med fokus på å beskytte helseinformasjon internt i virksomhetene. Siden den enkelte virksomhet har hatt ansvaret for informasjonssikkerhet og tilgangsstyring for sine egne data har resultatet vært ulike tolkninger av regelverket. Dette har medført ulike implementeringer som har gjort elektronisk samhandling vanskeligere. I tillegg er det er et spenn i modenheten til de interne prosessene for tilgangsstyring i de forskjellige deler av sektoren. Prosessen for meldingsutveksling er illustrert i figuren under.

Figur 3 – Stegene i en meldingsutveksling



2.1.1 Dagens situasjon

Med unntak av virksomheter som har inngått samarbeid om felles behandlingsrettet helseregister er dagens samhandling på tvers av virksomheter i hovedsak basert på meldingsutveksling. Tilliten i meldingsutveksling er i stor grad basert på at:

- Det alltid er en person som beslutter om helseopplysninger kan utleveres (manuell tilgangsbeslutning), der tilgangskontrollen ivaretas av fagsystemet.
- Mottakers virksomhet gjennom sin tilgangsstyring sørger for at riktig person får tilgang til opplysningene.
- Meldingsinnholdets integritet er ivaretatt og at utleverende virksomhet (juridisk person) kan identifiseres ved bruk av elektronisk signatur.
- Meldingsinnholdet krypteres med mottakers sertifikat slik at kun valgt mottakervirksomhet kan dekryptere og få tilgang til innholdet.
- Helsepersonellet er identifisert med personlig signatur for meldingstyper der det er påkrevd (eresept og sykemelding).
- Virksomhetene har inngått avtale om tilknytning med Norsk Helsenett SF, og gjennom denne skal oppfylle krav til meldingsutveksling[5] og Normen[6].

[5] Krav til elektronisk meldingsutveksling.

[6] Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten.

Med meldingsutveksling sendes opplysninger mellom virksomheter, og meldingene signeres på virksomhetsnivå (juridisk person). Hvis det er spesielle krav til identifikasjon av helsepersonellet benyttes også personlig signatur (e-resept og sykemelding). Beslutningen om å sende opplysninger er en manuell prosess, der tilgangskontrollen ivaretas gjennom tilgang til virksomhetens fagsystem. Selve utvekslingen skjer også via fagsystemet, og sendes til mottakers fagsystem, der det er opp til virksomheten som mottar opplysningene å sørge for at det er riktig personell som får tilgang til opplysningene gjennom sin tilgangsstyring og tilgangskontroll. Dermed får kun personell som har tjenstlig behov til informasjonen tilgang.

I tillegg til prosessen beskrevet over støtter tilliten mellom partene seg på signaturen på virksomhetsnivå og at det foreligger tilknytningsavtale med Norsk Helsenett SF. Gjennom denne avtalen forplikter virksomhetene seg til å oppfylle kravene i Norm for informasjonssikkerhet i Helse- og omsorgssektoren.

Kjernejournal er et konkret eksempel på en tillitsmodell på tvers av virksomheter som allerede er i bruk. Som et behandlingsrettet helseregister er Kjernejournal underlagt særskilte krav til ansvarsfordeling i forbindelse med tilgangsstyring gjennom kjernejournalforskriften[7]. Forskriften legger ansvaret for å gjennomføre en tilgangsbeslutning til hver enkelt virksomhet, men stiller krav om at helsepersonellet autentiseres på et høyt sikkerhetsnivå. Forskriften sier også at Direktoratet for e-helse, som dataansvarlig, kan sette vilkår for tilgang samt føre kontroll med at tilgang skjer i samsvar med reglene for tilgangsstyring. Kjernejournal logger brukerens identitet samt tilhørighet til virksomhet.

2.1.2 Forventet utvikling

Selv om meldingsbasert samhandling er utbredt og har et tydelig bruksområde har den teknologiske utviklingen gjort nye samhandlingsformer som data- og dokumentdeling mulig. Moderne systemer benytter ofte API-er (grensesnitt), som gjør det mulig å kjøre spesifikke deler av systemet fra annen programvare. Dette gjør det enklere å gi innsyn i andre systemer, og gir muligheten til økt integrasjon mellom systemer på tvers av virksomheter. Bruk av API-er har i dag lav utbredelse i norsk helse- og omsorgssektor, men det pågår flere initiativer som vil øke dette i årene fremover.

Sammenlignet med meldingsutveksling medfører data- og dokumentdeling en endring i hva tilliten baserer seg på. Siden tilgangsstyringen i disse tjenestene må utføres automatisk er det ikke tilstrekkelig å bare vite hvilken virksomhet som forespør opplysninger. Det må også være tillit til en rekke andre elementer i tillitskjeden mellom virksomhetene. Dette diskuteres videre i kapittel 2.3.

2.1.3 Nødvendige egenskaper for fremtidig data- og dokumentdeling

For at data- og dokumentdeling skal kunne etableres og oppnå utbredelse er det nødvendig med et fungerende tilgangsstyringsregime for de involverte virksomhetene. For å oppnå dette bør tilgangsstyringen legges til rette på en måte som gir:

- **Skalerbarhet –** Det bør være mulig å samhandle med et høyt antall andre virksomheter. For at dette skal være mulig bør etablering av samhandling med nye

[7] Forskrift om nasjonal kjernejournal (kjernejournalforskriften)

virksomheter kunne gjøres med lave kostnader og ressurssbruk, og liten grad av spesialtilpasning. Samtidig bør ikke avtaleverk og risikohåndtering kreve omfattende forvaltning.

- **Utbredelse –** Helsepersonell i virksomheter av alle størrelser bør kunne få tilgang til opplysninger lagret andre steder, og flere virksomheter bør kunne tilgjengeliggjøre data for andre virksomheter.
- **Tillit** – Før en virksomhet kan gis tilgang må tjenesten ha tillit til tilgangsstyringen som skal ligge til grunn. For å oppnå tillit må intern **informasjonssikkerhet** være tilstrekkelig, og krav til **sporbarhet** må etterleves.
- **Endringsevne** – Uviklingsretningen for tilgangsstyring bør **understøtte den strategisk retningen** for digitalisering av helse- og omsorgssektoren. Dette forutsetter at systemer virksomheter, styring- og finansieringsordninger gir tilstrekkelig evne til å tilpasse seg til endringer. Et dynamisk landskap med demografiske endringer, teknologisk utvikling, politiske føringer og strenge lovkrav vil gjøre at tilgangsstyringen trenger en stor grad av endringsevne.

For at sektoren skal kunne oppnå disse egenskapene på en enhetlig måte, og bevege seg i samme retning, kan det være behov for elementer av standardisering og samordning. Overordnet styring og tett samarbeid med sektoren vil være nødvendig for å gjennomføre nasjonalt koordinerte tiltak.

2.2 Utfordringer i dagens situasjon

2.2.1 Ikke dekkende krav og retningslinjer for data- og dokumentdeling

I praksis er det få eksempler utover bruk av felles journal på etablerte løsninger som muliggjør nye samhandlingsformer, i stor grad fordi det er så stor usikkerhet knyttet til hvordan informasjonssikkerhet og personvern skal ivaretas. Dette tyder på et behov for å etablere nye krav til tilgangsstyring i løsninger for data- og dokumentdeling som er mer tilrettelagt for at virksomheter enkelt kan etablere og administrere slike løsninger samtidig som lover og forskrifter etterleves.

Intern tilgangsstyring håndteres i dag ulikt i de forskjellige virksomhetene. Ofte er det fagsystemene som står for tilgangsstyringen for helsepersonell, andre har knytninger til lokale løsninger for tilgangsstyring. Enkelte leverandører av fagapplikasjoner har implementert beslutningsstyrt tilgangskontroll, mens andre har modeller basert på helsepersonellets rolle og organisasjonstilhørighet. Denne diversiteten, samt at det ofte ikke er full forståelse for hvordan beslutningene utføres i systemene, gjør det utfordrende å vurdere risiko og ha tillit til den interne tilgangskontrollen hos hver enkelt virksomhet.

Gjennom Normen, samt tilhørende faktaark og veiledere, gis det informasjon til virksomhetene om hvordan de kan etterleve krav til informasjonssikkerhet, inkludert krav til tilgangsstyring ved tilgang mellom av virksomheter. Det er foreløpig ikke etablert et sett med krav for data- og dokumentdeling. Etablerte samhandlingsformer som dagens lovverk legger opp til, som direkte tilgang til annen virksomhet, innebærer en omstendelig prosess som skalerer dårlig dersom informasjonen skal deles med et større antall virksomheter, personell og et ukjent antall data- og dokumentdelingstjenester.

2.2.2 Krevende avtalestruktur

Det finnes ikke noe generelt avtaleverk for data- og dokumentdeling slik som det gjør for meldingsutveksling, som medfører at hver "nye" samhandling må gjennom en omfattende

prosess med å sette opp avtaleverk, kravstilling og ansvarsfordeling. I stedet må det inngås én-til-én avtaler mellom virksomheter som skal hente ut data og virksomheter som har tjenester som skal tilby data. Dette utgjør en av de største utfordringene i dagens situasjon. Uten en form for samordning eller økt grad av standardisering av avtaleforholdene vil oppsett og forvaltning av avtaler være ressurskrevende. Dette vil redusere antall aktører hver virksomhet har kapasitet til å samhandle med.

Direktoratet for e-helse gjennomførte i 2016 en kartlegging[8] av sektorens bruk av forskrift om tilgang til helseinformasjon mellom virksomheter, som viser at forskriften benyttes i liten grad. Direktoratet peker på at årsakene til lav anvendelse av forskriften kan skyldes kompleksitet rundt praktisk etterfølgelse av kravene. Undersøkelsen viser at forskriftens krav til én-til-én avtaler per ressurs fører til høy kompleksitet både i forbindelse med etablering av avtalene og forvaltning i etterkant. Dette gir tydelige signaler om at regelverket bør forenkles slik at det legger til rette for økt elektronisk samhandling.

Helse- og omsorgsdepartementet har vedtatt ny forskrift om pasientjournal, og at forskrift om tilgang til helseopplysninger mellom virksomheter oppheves ved ikrafttredelse av den nye pasientjournalforskriften. Den nye pasientjournalforskriften trer i kraft 1. juli 2019.

2.2.3 Ulik praksis for sikkerhetsvurderinger

Dagens praksis rundt gjennomføring av sikkerhetsvurderinger som foretas av hver enkelt aktør, for hver ny samhandling som skal på plass (herunder risikovurdering, vurdering av informasjonssikkerhet, autentiserings- og autorisasjonsløsning m.m.) utgjør et stort hinder for økt utbredelse for data- og dokumentdeling. De viktigste årsakene er behovene for tilstrekkelig og tilgjengelig kompetanse, og en omfattende vurderingsprosess innen området. Dette er tidkrevende å gjennomføre for hver aktør det skal samhandles med, og gir ulik praksis og kapasitetsutfordringer.

Hvordan ulike sikkerhetskrav tolkes og risiko vurderes vil variere. Om risikoen er akseptabel eller ikke vil avhenge av subjektive vurderinger, og gjør det utfordrende å ha tillit til risikovurderinger utført av andre virksomheter. Med dagens situasjon vil dette gi økte kostnader og begrense antall virksomheter man har kapasitet nok til å etablere samhandling med. I tillegg vil resultatet av vurderingene (om risiko vurderes som akseptabel), avhenge av de subjektive vurderingene som er gjort.

2.2.4 Liten grad av standardisering

Sektoren har ikke etablert et felles vokabular for å beskrive helsepersonells rolle, organisasjonstilhørighet, grunnlag for tjenstlig behov samt annen relevant informasjon. Denne typen informasjon benyttes ofte i tilgangsbeslutningen, men danner også grunnlaget for at logger kan tilfredsstille krav i lover og forskrifter[9].

[8] *Kartlegging av sektorens bruk av forskrift om tilgang til helseopplysninger mellom virksomheter, 28.06.2016.*

[9] Veileder ved tilgang mellom virksomheter, støttedokument til Normen.

Samhandlingsevne påvirkes også av hvordan informasjonen som benyttes i en tilgangsbeslutning formateres og utveksles mellom konsument og tjeneste[10]. I dag finnes det ingen nasjonale krav til bruk av standardiserte protokoller og spesifikasjoner for autentisering og autorisasjonsformål i forbindelse med data- og dokumentdeling.

2.2.5 Lav tillit mellom virksomheter

Et viktig tema i forbindelse med elektronisk identitet (eID[11]) er tilliten som dataansvarlige har til identitetstilbyderne i sektoren. Tillitsnivåene som gjelder i dag er blant annet gitt av «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor[12]», som omfatter de ulike nivåene av autentiseringsstyrke. Innspill tilsier at nivåene er for grovkornete, og det ses eksempler på dette i forbindelse med identitetstilbydere som tilbyr autentisering med selvutstedte sertifikater. Autentiseringsstyrken beskrives ofte som f.eks. «3,5» eller «3+». Internasjonalt er det en bevegelse mot å beskrive flere uavhengige tillitsnivå som kan samles i ett uttrykk[13]. For konsument og tjeneste er det ønskelig å representere tillitsnivået på en enkel og omforent måte, for eksempel med tillitsnivåene gitt av eIDAS. For mellomparter vil det være ønskelig med en mer detaljert og omforent representasjon av tillitsnivået.

Med sektorens store diversitet i virksomheter er det svært ulik kapasitet til å innfri krav til informasjonssikkerhet og tilgangsstyring på egen hånd. Mindre virksomheter vil ha behov for å støtte seg på sentrale eller tredjeparts tjenester for å kunne oppnå tilstrekkelig sikkerhet, utføre etterkontroll, sette opp avtaler og utføre sikkerhetsvurderinger.

2.3 Utfordringer i tillitskjeden ved innføring av data- og dokumentdeling

I tillegg til de overordnede utfordringene beskrevet i foregående kapittel er det spesifikke utfordringer knyttet til de ulike leddene i tillitskjeden mellom virksomheter. Effektiv tilgangsstyring i data- og dokumentdeling er ikke mulig med manuelle prosesser For at tilgangsprosessen skal kunne automatiseres må det bygges tillit til en rekke faktorer, vist i Figur 4.

---

[10] Med konsument menes i dette dokumentet en programvarekomponent eller automatisert prosess som handler på vegne av et helsepersonell med tjenstlig behov, og som kan utføre tjenestekall til data- og dokumentdelingstjenester tilgjengeliggjort av en annen virksomhet i sektoren.

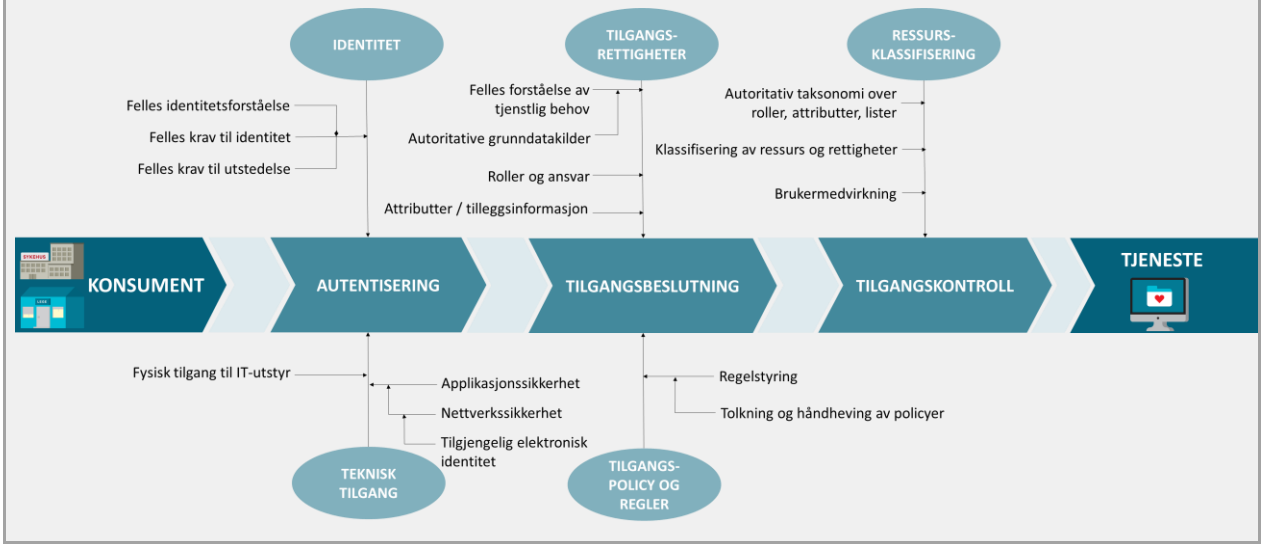
Med tjeneste menes programvare som tilgjengeliggjør data eller dokumenter for andre virksomheter.

[11] En elektronisk identitet (eID) kan for eksempel være et brukernavn, sertifikat eller annen entydig identifikasjon av et helsepersonell.

[12] Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor. Det kongelige fornyings- og administrasjonsdepartementet, 2008.

[13] NIST beskriver dette i siste versjon av 800-63 digital authentication guidelines, og det finnes eksempler på standardiseringsarbeid for hvordan dette kan uttrykkes hos IETF.

Figur 4 – Tillitskjeden på tvers av virksomheter



For å kartlegge dagens utfordringer, ønsket ambisjonsnivå og spenne ut mulighetsrommet for tiltak i de ulike leddene ble tillitskjeden på tvers av virksomheter vurdert i fem områder:

1. **eID-forvaltning** – Utstedelse, bruk, validering og tilbaketrekking av elektroniske identiteter for helsepersonell og annet personell.
2. **Tilgangskontroll og sporbarhet** – Håndheving av retningslinjer for hvem som har tilgang til hva, samt logging og overvåkning av utøvelsen.
3. **Identifisering av helsepersonell og virksomhet** – Verifisering av at helsepersonellet som forespør opplysninger er den de utgir seg for å være, og hvilken virksomhet de tilhører.
4. **Grunnlag for vurdering av tjenstlig behov** – Oppretting av brukere, roller, rettigheter og autorisasjoner. Internkontroll rundt vedlikehold og fjerning av disse.
5. **Overordnet styring av tilgangsstyring i sektoren** – Overordnet styring og forvaltning av krav og standarder, eventuelt tillitsorgan, tredjeparts tillitstjenester, administrative støttefunksjoner og avtalehåndtering m.m.

Dagens situasjon, utfordringer og mulige løsninger for å standardisere eller samordne funksjoner i hver av de fem delene ble diskutert i samråd med sektoren. En oppsummering av overordnede prinsipper som må ligge til grunn i hvert område er gitt videre i kapittelet.

2.3.1 eID-forvaltning

Elektronisk identiteter (eID-er), som for eksempel brukernavn eller sertifikat, utstedes av virksomhetene selv eller av en tredjepart (f.eks. BuyPass, Commfides eller BankID). Kravet ved tilgang til opplysninger er at helseopplysninger bare gjøres tilgjengelig for personell som gjennom autentisering kan bekrefte sin identitet med en tilstrekkelig grad av sikkerhet. Dette kravet gjelder både ved tilgang til opplysninger i egen virksomhet og i andre virksomheter.

Hvilke løsninger som vil gi tilstrekkelig sikkerhet til å benyttes i data- og dokumentdeling er avhengig av det totale risikobildet. Sentrale elementer i denne vurderingen vil blant annet være virksomhetens størrelse, hvor oversiktlig den er, samt hvor god mulighet for etterkontroll av tilganger den dataansvarlige har. Gitt den store diversiteten av virksomheter anses det som utfordrende å skape tillit til andre løsninger enn ved bruk av

autentiseringsmidler med høyt sikkerhetsnivå. Innspillene fra sektoren tyder på at det er behov for et nasjonalt bestemt minstekrav til eID ved data- og dokumentdeling.

For å sikre endringsevne over tid vurderes det som viktig at valg knyttet til eID ikke bindes opp i teknologi, og at mobile enheter som etter hvert har fått utbredelse også kan benyttes. Videre observeres det at utbredelse av eID på tilstrekkelig nivå i primærhelsetjenesten anses som lav og med variert grad av modenhet, samtidig som smartkort-basert eID er utfordrende å bruke i situasjoner hvor utstyr og infrastruktur mangles (f.eks. hjemmesykepleien).

2.3.2 Tilgangskontroll og sporbarhet

I helse- og omsorgssektoren er vurderingen av hvem som har tjenstlig behov for tilgang til helseopplysninger sentral i tilgangsstyringen, og det er nødvendig at tjenesteeieren har tillit til at helsepersonell som gis tilgang har et reelt tjenstlig behov for opplysningene. Beslutninger om tilgang kan utføres med ulik ansvarsfordeling, som strekker seg fra at både konsument og tjeneste gjør en full tilgangskontroll (distribuert tilgangskontroll), til at alle tilgangsbeslutninger er samlet i en felles komponent (sentralisert tilgangskontroll).

I arbeidet med vurderingen ble det sett på mulige måter å samordne tilgangsbeslutninger i en felles komponent, men dette ble gjennomgående ansett som for krevende og ikke ønskelig. Med dagens organisering av helsesektoren sitter hver enkelt virksomhet på detaljert og oppdatert informasjon om helsepersonellets ansattforhold og pasienter som får behandling av virksomheten. Den lokale informasjonen ble derfor vurdert som best egnet til automatisert tilgangsstyring på tvers av virksomheter. Etablering av en felles komponent for tilgangskontroll i hele helse- og omsorgssektoren ble derfor ikke utredet videre som et alternativ. Alternativene som beskrives i kapittel 3 legger dermed til grunn at:

- Vurdering av tjenstlig behov utføres av konsumentens virksomhet (tilgangsbeslutning).
- Tjenesten må ha mulighet til å vurdere forespørselen opp mot sine sikkerhetskrav (tilgangskontroll).

Felles komponenter for håndtering av personvern (sperringer, reservasjon m.m.), og etterkontroll av logger ble ansett som muligheter, og ble tatt videre med i de utarbeidede alternativene.

2.3.3 Identifisering av helsepersonell og virksomhet

Prosessen hvor en brukers identitet blir verifisert kalles autentisering, og innebærer at brukeren må presentere bevis på at han er den han sier han er. Hvordan dette bevises kategoriseres ved å gruppere ulike mekanismer i autentiseringsfaktorer. De klassiske autentiseringsfaktorene er:

- Noe brukeren vet: f.eks brukernavn og passord, PIN-kode.
- Noe brukeren har: smart-kort, mobiltelefon etc.
- Noe brukeren er: fingeravtrykk, ansiktsgjenkjenning.

Ved å kombinere to eller flere av disse faktorene kan man styrke autentiseringen, og være tryggere på personens identitet. Dette kalles to- eller flerfaktorautentisering.

I tillegg til identifisering av bruker er tjenestene i mer eller mindre grad avhengig av identifikasjon av hvilken virksomhet helsepersonellet som forespør opplysninger tilhører i øyeblikket det forespørres. I dagens samhandling bygger dette på virksomhetssertifikater, men dette gir ikke tilstrekkelig grad av granularitet for enkelte formål. Det kan derfor være

behov for andre mekanismer for å verifisere brukerens organisasjon, inkludert avdelingstilhørighet for helsepersonellet for å bygge tillit og benytte informasjonen til tilgangskontroll.

2.3.4 Grunnlag for vurdering av tjenstlig behov

I tillegg til at tjenestetilbyderne må ha tillit til at brukerens identitet er korrekt er det også nødvendig at informasjonen som benyttes i tilgangsstyringen er korrekt og oppdatert. Siden virksomhetene selv skal være ansvarlig for å vurdere tjenstlig behov er interne prosesser som omhandler registrering og kontroll av autorisasjoner og opplysninger om pasienter og ansatte viktige. Standardiserte prosesser kan øke tilliten til at virksomhetene har tilstrekkelig kontroll på brukere og autorisasjoner, og at etterkontroll av hendelsesregistre gjennomgås. Som en del av dette ble det vurdert en mulighet for selvdeklarering, revisjon og eventuelt eksternt tilsyn for å verifisere at internkontrollen er god nok til at data og dokumenter kan gjøres tilgjengelig for en virksomhet. Muligheten for å verifisere enkelte opplysninger i grunndata, som f.eks. at helsepersonellets autorisasjon er gyldig i HPR, ble også vurdert som tillitsøkende mekanismer.

2.3.5 Helhetlig styring og koordinering

For at ulike deler av sektoren skal kunne utvikle seg i samme retning innen tilgangsstyring, og at tiltak som adresserer de kartlagte utfordringene gjennomføres, er det behov for en bedre overordnet styring. Styring vil også være nødvendig for å få på plass standarder for informasjon som skal utveksles, felles krav og retningslinjer, gi felles forståelse av sikkerhetskrav og økt forutsigbarhet for virksomhetene i sektoren som skal ta i bruk data- og dokumentdelingsløsninger. Uten sentral koordinering vil virksomheter utvikle tjenester og implementerer krav og standarder ulikt. Dette vil igjen begrense mulighetene for effektiv og skalerbar tilgangsstyring i data- og dokumentdeling, og for å kunne ha god oppfølging av om krav og retningslinjer etterleves.

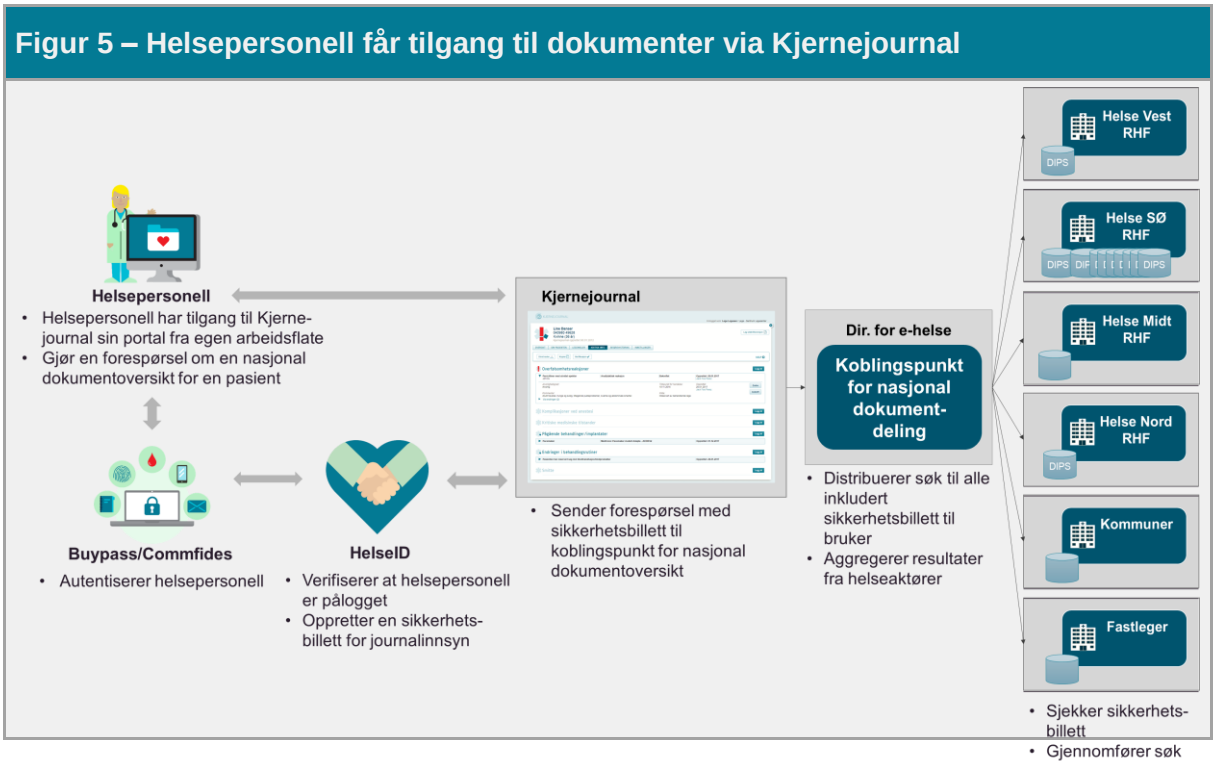
3 Utviklingsretninger for fremtidig tilgangsstyring

Basert på kartlagte utfordringer i tillitskjeden og ønsket ambisjonsnivå innenfor de fem områdene beskrevet i 2.3, er det i samråd med prosjektets arbeidsgruppe utledet to mulige utviklingsretninger som adresserer utfordringene i dagens situasjon. Utviklingsretningene representerer ulike måter helse- og omsorgssektoren kan innrette tilgangsstyring for data- og dokumentdeling:

- **Nullalternativet** – Videreføring av dagens situasjon.
- **Harmoniseringsalternativet –** Videreføring av én-til-én tillits- og avtaleforhold, kombinert med nasjonalt koordinerte tiltak og standardiserte prosesser for å øke virksomhetenes modenhet og effektivitet innen tilgangsstyring.
- **Samordningsalternativet –** Samordning av tillits- og avtaleforhold gjennom etablering av et felles tillitsanker, med oppbygging av tillitstjenester for å øke virksomhetenes mulighet til å etablere tilgang på tvers av virksomheter i større skala.

For å belyse hvordan alternativene vil påvirke data- og dokumentdeling i praksis er det tatt utgangspunkt i et tenkt eksempel: Etablering av en nasjonal tjeneste for helsepersonells tilgang til kliniske dokumenter på tvers av virksomheter gjennom kjernejournal, vist i Figur 5. Tjenesten er basert på profilen IHE XCA[14] (Cross-Community Access).

Figur 5 – Helsepersonell får tilgang til dokumenter via Kjernejournal



[14] Beskrivelse av profilen på IHEs wikisider.

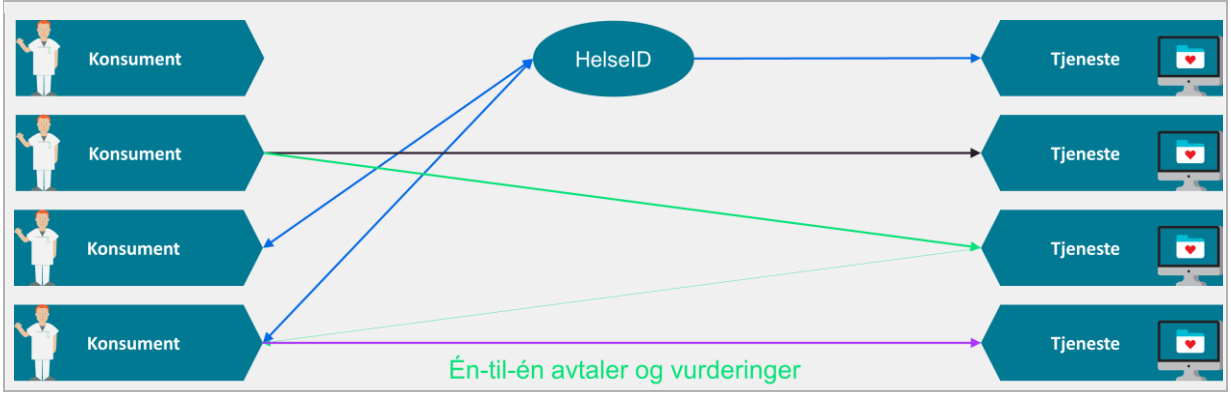
3.1 Nullalternativet – Videreføring av dagens situasjon

Nullalternativet innebærer videreføring av dagens situasjon med én-til-én samhandlingsforhold, avtaler og sikkerhetsvurderinger. Ingen ytterligere tiltak settes i verk på nasjonalt nivå.

Ansvarsfordeling i tilgangsstyringen vil måtte avklares i hvert enkelt tilfelle. Tilgangsstyringen vil kunne utføres i konsumentens virksomhet, av tjenesten eller en kombinasjon av de to. Alternativer til data- og dokumentdeling, som samarbeid om felles behandlingsrettet register eller direkte tilgang til annen virksomhets system, vil også være mulige samhandlingsformer. Hvilke mekanismer som skal skape tilstrekkelig tillit til tilgangsstyringen blir opp til virksomhetene som skal samhandle. Verifikasjon av at sikkerheten er tilstrekkelig må avklares i hvert tilfelle etter hva som er praktisk gjennomførbart. Avtaleverk må settes opp i hvert tilfelle.

Figuren under skisserer hvordan avtaleforhold og sikkerhetsvurderinger vil se ut med nullalternativet. De ulike tjenestene vil ha ulikt avtaleverk og sikkerhetskrav, HelseID vil benyttes inn til noen tjenester, og ikke alle virksomheter vil være i stand til å etablere data- og dokumentdeling i det hele tatt.

Figur 6 – Illustrasjon av nullalternativet



Vurdering av nullalternativet

Skalerbarhet og utbredelse	Tillit og sikkerhet
- Begrenset mulighet for små virksomheter til å ta i bruk data- og dokumentdeling. - Utfordringer med å skalere opp data- og dokumentdelingsløsninger til et større antall virksomheter. - Lav grad av standardisering øker kompleksitet ved etablering av nye samhandlingsforhold. - Hvilket sikkerhetsnivå som er tilstrekkelig må vurderes i hvert enkelt tilfelle.	- Liten grad av standardisering og innsyn i hvordan tilgangsbeslutninger er tatt. - Utfordringer med å ivareta reell kontroll av tjenstlig behov ved deling. - Utfordringer med å ivareta krav til personvern, innsyn og etterprøvbarhet ved deling. - Ulik praksis for bruk av egne eID-er og eID levert av tredjepart.

Understøttelse av strategisk retning og endringsevne	Kostnads- og gevinstbilde
+ HelseID vil i økende grad kunne tas i bruk av de virksomhetene som enes om at dette er formålstjenlig for autentisering. - Ulik praksis for prosesser og mekanismer for autentisering internt i virksomhetene. - Mangel på utvikling innen tilgangsstyring vil kunne utgjøre et vesentlig hinder for målet om «Én innbygger – én journal».	+ Lavere kostnad for forvaltning og videreutvikling av HelseID enn ved de andre alternativene. + Mindre press for å anskaffe eID på høyere nivå. - Begrenser gevinsten av felleskomponenter som er etablert (HelseID, felles registre, Kjernejournal).

Samlet vurdering

Nullalternativet anses totalt sett som lite egnet til å etablere tilstrekkelig tilgangsstyring for data- og dokumentdeling på tvers av virksomheter av følgende årsaker:

- Understøtter ikke forventede, fremtidige krav til informasjonssikkerhet og personvern for det langsiktige målbildet forbundet med «Én innbygger – én journal».
- Utnytter ikke de muligheter som forventes realisert gjennom andre pågående initiativer.
- Manglende helhetlig tilnærming vil føre til økt forvaltningskostnad for virksomhetene som skal samhandle over tid, og begrense antall virksomheter det kan samhandles med.
- Det vil være krevende for mindre virksomheter å etablere noen form for data- og dokumentdeling.

Alternativet har lavest etableringskostnad, men kostnader på lang sikt antas å bli høyere enn de to andre alternativene, samtidig som gevinstene antas å bli vesentlig lavere.

3.2 Harmoniseringsalternativet – Standardisering og styrket internkontroll

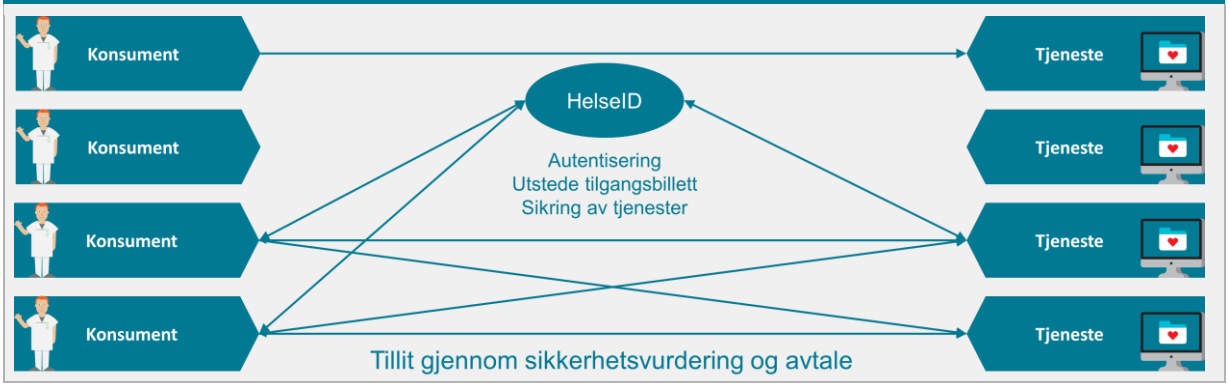
Harmoniseringsalternativet viderefører dagens situasjon med én-til-én avtaleforhold, med fokus på å tilrettelegge for at samhandling med nye virksomheter kan etableres mer effektivt.

Alternativet setter fokus på å styrke virksomhetenes internkontroll og informasjonssikkerhet, og gjennom dette forbedre grunnlaget for at andre kan ha tillit til virksomheten. Virksomheter som skal konsumere data og dokumenter må følge omforente standarder for tilgangsstyring, informasjon som skal sendes med forespørsler og logging. Gjennom standardisering av avtaleverket og et felles rammeverk for sikkerhetsvurderinger vil det bli enklere å etablere samhandling med nye virksomheter.

Ansvaret for å vurdere om tjenstlig behov foreligger vil ligge hos konsumerende virksomhet, og baseres på lokale data. Standardisert informasjon om identitet, virksomhet og grunnlag for tilgang må sende med i forespørselen, og verifiseres av HelseID. Tjenesten mottar standardisert informasjon, og kan kontrollere og logge forespørselen opp mot sine sikkerhetskrav.

Figuren under skisserer hvordan tilgangsstyring i data- og dokumentdeling vil kunne utvikle seg med harmoniseringsalternativet. Samhandling mellom konsumenter og tjenester vil settes opp på en enhetlig måte, og HelseID vil kunne benyttes til å identifisere helsepersonell mot tjenester som ser det som formålstjenlig. Selv med økende grad av standardisering vil det være ressurskrevende å opprette samhandling med mange aktører. Tjenestene når dermed ikke ut til alle konsumentene, og konsumentene får ikke tilgang til alle tjenestene de kan ha behov for. Videre i kapitlet gis også et praktisk eksempel på harmoniseringsalternativet.

Figur 7 – Illustrasjon av harmoniseringsalternativet



Sentrale tiltak	
Styrket internkontroll	• Sette nasjonale krav til elementer fra styringssystem for informasjonssikkerhet som må være på plass for data- og dokumentdeling, som virksomheter som skal samhandle må iverksette og etterleve. • Styrking av internkontroll og informasjonssikkerhet i tråd med Normens krav.
Avtalemodell	• Standardisering av avtaleverk.

Sikkerhetsvurderinger	• Etablering av et felles rammeverk for én-til-én sikkerhetsvurderinger.
Standarder	• Omforenes om og stille krav til sikkerhetsnivå for eID til bruk i data- og dokumentdeling. Kravet bør nedfelles i Normen. • Etablere nødvendige standarder (innhold i sikkerhetsbilletter, logging, grunnlag for tjenstlig behov m.m.). • Etablere krav til sikring av tjenester.

Harmoniseringsalternativet i praksis

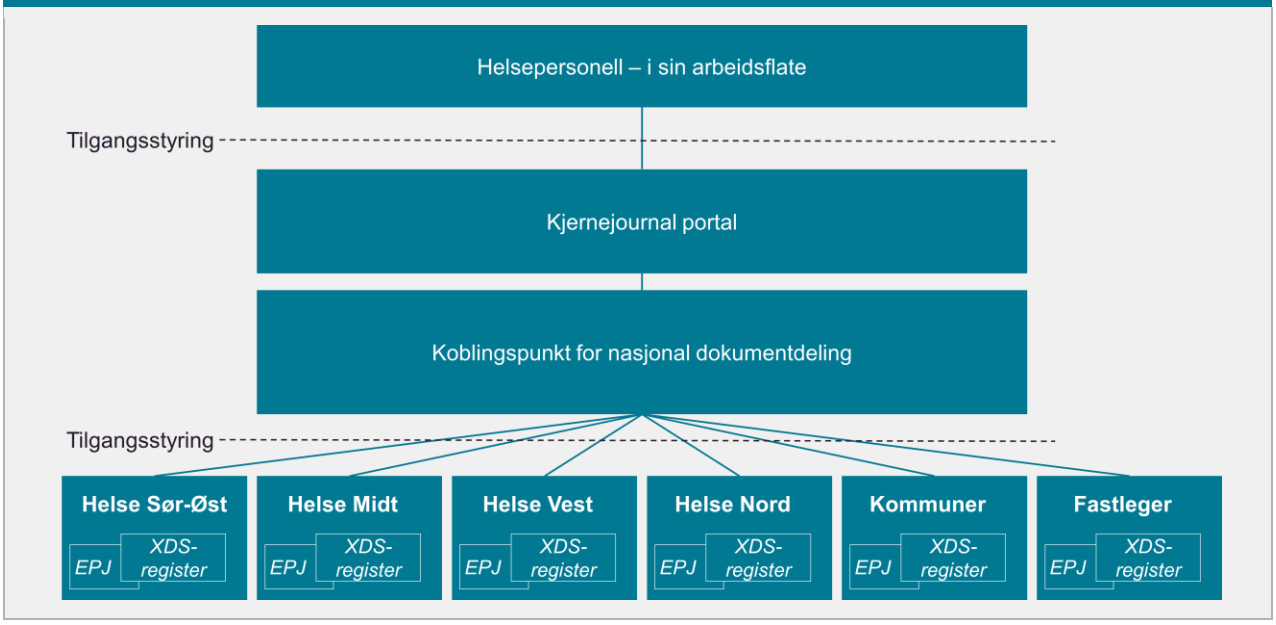
Eksempel: Helsepersonell får tilgang til kliniske dokumenter via Kjernejournal

Med tillitsmodellen i harmoniseringsalternativet må følgende være på plass før helsepersonellet kan be om tilgang til kliniske dokumenter:

- Avtale må være inngått mellom partene, med nødvendige forarbeid som risikovurdering, etterlevelse av krav til informasjonssikkerhet etc. på plass. Partene vil kunne benytte et harmonisert avtaleverk og avtalestruktur.
- Helsepersonellet må være registrert og autorisert i egen virksomhet – enten i fagsystem eller i en lokal tilgangsstyringskomponent.
- Dersom tjenesteeier skal ha tillit til konsument må kodeverk og prinsippene som ligger bak begrunnelse for tjenstlig behov være felles for alle parter.
- Identitetstilbyderen konsumenten benytter må være tilgjengelig via HelseID. I harmoniseringsalternativet har ikke HelseID en kontrollerende funksjon ovenfor identitetstilbyderne. Derfor angir identitetstilbyderne autentiseringsstyrke selv, og dette videreformidles i sikkerhetsbilletter fra HelseID etter vellykket autentisering.
- For å etablere høy grad av tillit må både fagsystemet og Kjernejournal registreres og autentiseres som klient og ressurs i HelseID før de får lov til å autentisere brukere. Klientautentiseringen er basert på en konfigurasjon som må eksistere i HelseID.

Når dette er på plass vil helsepersonellet ha mulighet til å søke etter opplysninger om pasienter de har tjenstlig behov til.

Figur 8 – Illustrasjon av bruksscenario



Dokumentdeling i bruksscenariet over vil følge følgende steg:

1. Helsepersonellet åpner sitt fagsystem og pasientens journal.
2. Fagsystemet utfører en tilgangskontroll. Her sjekkes også om det er registrert sperringer eller lignende i interne system.
3. Dersom det gis tilgang til pasientens journal åpner helsepersonellet Kjernejournal for pasienten i sitt fagsystem. Kjernejournal er sikret med HelseID, og krever autentisering med tilstrekkelig autentiseringsstyrke[15]. Helsepersonell som er innlogget i fagsystem med kun brukernavn og passord må autentiseres med dagens sikkerhetsnivå 4 før tilgang til Kjernejournal gis.
4. Kjernejournal må deretter få overført kontekstuell informasjon om helsepersonellet fra fagsystemet før den kan gjøre et kall til nasjonalt koblingspunkt for dokumentdeling. Informasjon som må overføres er hvilken virksomhet helsepersonellet er tilknyttet og grunnlag for tjenstlig behov.
5. Kjernejournal benytter koblingspunktet for nasjonal dokumentdeling, som gjør distribuerte søk i dokumentregistrene i foretakene. Når koblingspunktet kontakter dokumentregistrene sjekkes det for gyldig sikkerhetsbillett.
    - Sikkerhetsbilletten må være signert av en autoritativ kilde som virksomheten har tillit til. Dette kan være en billettutsteder i virksomheten hvor dokumentkilden befinner seg, eller en sentral billettutsteder, som f.eks Kjernejournal eller HelseID.
    - Sikkerhetsbilletten må inneholde tilstrekkelig informasjon om helsepersonellet. Tjenestetilbyder må derfor stole på at informasjonen signert av billettusteder er korrekt.
6. Tjenesten godkjenner autentiseringsstyrke og validerer kontekstuell informasjon.
7. Før dokumentkilden kan gi tilgang til dokumentet må den sjekke i eget register om pasienten har reservert seg mot innsyn fra det aktuelle helsepersonellet.
8. Dersom det ikke foreligger sperringer, reservasjoner eller lignende logges tilgangen med tilstrekkelig informasjon, og tilgang til dokumentet returneres.

Vurdering av harmoniseringsalternativet

Skalerbarhet og utbredelse	Tillit og sikkerhet
+ Standardisering av avtaleverk og sikkerhetsvurderinger gir redusert kostnad og tidsbruk for å etablere samhandling med nye aktører sammenlignet med dagens situasjon. - Én-til-én tillitsforhold gir utfordringer med å skalere opp data- og dokumentdeling til større antall virksomheter og brukere. - Begrenset mulighet for mindre aktører til å oppnå tillit, og dermed til å få	+ Styrket informasjonsikkerhet/ personvern gjennom forbedret internkontroll. + Styrket internkontroll vil kunne gi økt tillit til identitetsforvaltningen hos konsumentens virksomhet. + Økt tillit til at tilgangsbeslutninger blir gjennomført tilfredsstillende. - Økt behov for løsninger som skal kunne brukes for sporing og etterprøvbarhet. - Forutsetter etterlevelse av krav til sikkerhet

[15] Sikkerhetsbillett for Kjernejournal:
- Fagsystemet har allerede autentisert bruker i HelseID, får SSO når kjernejournal åpnes.
- Brukeren er ikke autentisert før han åpner Kjernejournal. Kjernejournal ber om at brukeren autentiseres i HelseID før han gis tilgang.

tilgang til data- og dokumentdelingstjenester.	og tilfredsstillende tilgangsbeslutninger i konsumerende virksomheter. - Fortsatt diversitet i tilgangsbesluning og tilgangskontroll.

Understøttelse av strategisk retning og endringsevne	Kostnads- og gevinstbilde
- Fortsatt diversitet i identifisering av helsepersonell. - Ingen felles betydning av eID-sikkerhetsnivåer på tvers av virksomheter, reduserer muligheten for at alternative autentiseringsløsninger kan tas i bruk.	+ Standardisering av avtaleverk og sikkerhetsvurderinger gjør etablering av nye samhandlingsforhold mindre ressurskrevende. + Lavere utviklings- og driftskostnader for sikkerhet i felles grunnmur (HelseID) enn ved samordningsalternativet. - Økte kostnader til styrking av virksomheters tilgangsstyring og internkontroll. - Økte kostnader til oppsett og forvaltning av avtaler. - Økte kostnader til gjennomføring av sikkerhetsvurderinger i virksomhetene.

Samlet vurdering

Harmoniseringsalternativet styrker grunnlaget for tillit til tilgangsstyringen i andre virksomheter gjennom tydeliggjøring og harmonisering av krav til virksomhetene. Dette gjelder særskilt innenfor:

- Internkontroll og forbedringer i styringssystemer for informasjonssikkerhet med hovedfokus på policykrav for identitets- og tilgangsstyring.
- Gjennom Norm og forskrift ansvarliggjøres virksomheter i større grad med hensyn til informasjonssikkerhet og personvern ved data- og dokumentdeling.
- Felles standarder for avtaler, sikkerhetsvurderinger og informasjon som skal benyttes i tilgangsstyringen (attributter med mer) forenkler og effektiviserer tilgjengeliggjøring av nye tjenester for data- og dokumentdeling.

Alternativet legger til rette for raskere og enklere utvikling av nye tjenester for data- og dokumentdeling, og øker potensialet for å oppnå utbredelse sammenlignet med dagens situasjon. Dette forutsetter at virksomhetene prioriterer å styrke internkontrollrutiner som skal bidra til økt tillit mellom partene som deler. På mellomlang sikt vil utfordringer knyttet til skalerbarhet og utbredelse redusere gevinstpotensialet, og lokale kostnader vil øke for hver antall virksomhet det etableres samhandling med.

3.3 Samordningsalternativet – Etablering av felles tillitsanker

Samordningsalternativet legger til rette for data- og dokumentdeling ved å etablere et felles tillitsanker. Tillitsankeret vil fungere som felles avtalepunkt, som vil redusere antall avtaler som må inngås betraktelig, i motsetning til én-til-én avtaleforholdene i de andre alternativene.

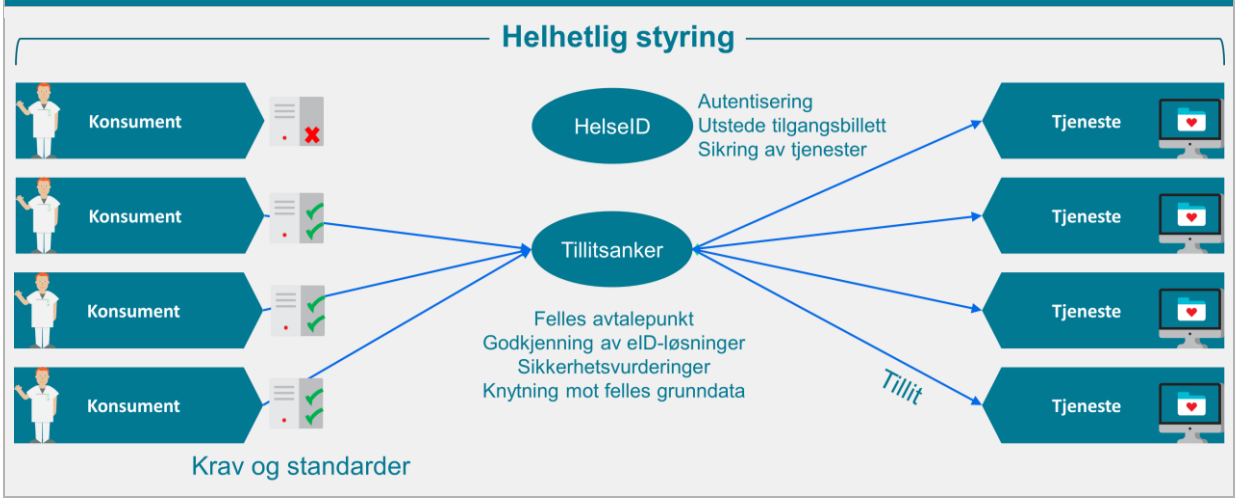
Tillitsankeret vil legge til grunn et sett med overordnede krav og retningslinjer for intern tilgangsstyring hos konsument, samt standarder for data som skal sendes med i forespørsler. Virksomheter som oppfyller disse kravene vil kunne inngå avtale med tillitsankeret, og få tilgang til opplysninger fra tjenester som har avtale med tillitsankeret. Kravene bør være bredt forankret og besluttet, og nedfelles gjennom Normen og/eller avtaleverk for tillitsankeret.

Tillitsankeret som forvaltningsfunksjon vil bygges opp over tid for å kunne ivareta og levere tillitsskapende tjenester. Eksempler på slike tjenester er å verifisere påstander om tjenstlig behov, identitet, virksomhetstilhørighet og annen informasjon, samt verifikasjon av sikkerhetsnivå i eID-løsninger.

Ansvaret for å vurdere om tjenstlig behov foreligger vil ligge hos konsumerende virksomhet. Tilgangsbeslutning baseres på lokale data hos konsumenten, som må sende med standardisert informasjon om identitet, virksomhet og grunnlag for tilgang i forespørselen. Tillitsankeret vil verifisere at konsumenten tilfredsstiller krav og har avtale med tillitsankeret, og kan berike sikkerhetsbilletten med informasjon fra sentrale registre. Tjenesten får samme inndata tillitsankeret, og kan kontrollere og logge forespørselen opp mot sine sikkerhetskrav.

Figuren under viser hvordan tilgangsstyring i data- og dokumentdeling vil kunne utvikle seg med samordningsalternativet. Tillitsankeret vil være bindeleddet mellom konsumenter og tjenester. Virksomheter som etterlever krav og standarder og kan verifisere dette vil kunne få tilgang til tjenestene som har avtale med tillitsankeret. HelseID vil være nært knyttet opp til tillitsankeret, og vil være obligatorisk. Et praktisk eksempel på tilgangsstyring med samordningsalternativet er gitt senere i kapitlet.

Figur 9 – Illustrasjon av samordningsalternativet



Sentrale tiltak	
Felles krav og retningslinjer	• Etablere felles krav og standarder for data- og

	dokumentdeling gjennom Normen. ○ Omforenes om og stille krav til sikkerhetsnivå for eID til bruk i data- og dokumentdeling. Kravet bør nedfelles i Normen. ○ Organisatoriske krav (internkontroll, interne prosesser knyttet til registrering og oppfølging av data m.m.) ○ Elementer fra styringssystem for informasjonssikkerhet som må være på plass.
Standarder	• Etablere felles standarder i samhandlingsdomenet. ○ Standardisere representasjon av rolle, tjenstlig behov m.m. • Omforenes om hvilke protokoller som skal benyttes.
Avtalemodell	• Etablering og stegvis utvikling av et tillitsanker for data- og dokumentdeling, som fungerer som felles avtalepart. • Tilrettelegge for høy grad av selvbetjening og automatisering av avtalehåndteringen.
Sikkerhetsvurderinger	• Felles godkjenningsordning, der tillitsankeret verifiserer at virksomhetene oppfyller krav og standarder til tilgangsstyring. Kan etableres med selvdeklarering, og utvides til at tillitsankeret utfører sikkerhetsvurderinger etter hvert som kapasiteten økes.
Tillitsanker	• Bygge tillit til påstander om tjenstlig behov, identitet, virksomhetstilhørighet og annen informasjon. • Knytning mot felles grunndata om innbygger, personell og virksomheter. • Heve kvalitet og tilgjengelighet i felles grunndata til et nivå som er tilstrekkelig for bruk i tilgangsstyring. • Vurdere behov for ny felles grunndata til bruk i tilgangsstyringen.
HelseID	• HelseID videreføres med dagens ambisjon for modenhet og utbredelse, og tas i bruk til identifisering mot alle tjenester som skal tilby data- og/eller dokumentdeling. På sikt vil det være behov for høyere forvaltningskapasitet for å imøtekomme økt antall aktører som skal benytte løsningen. • Sikring av tjenester samordnes gjennom HelseID.

Samordningsalternativet i praksis

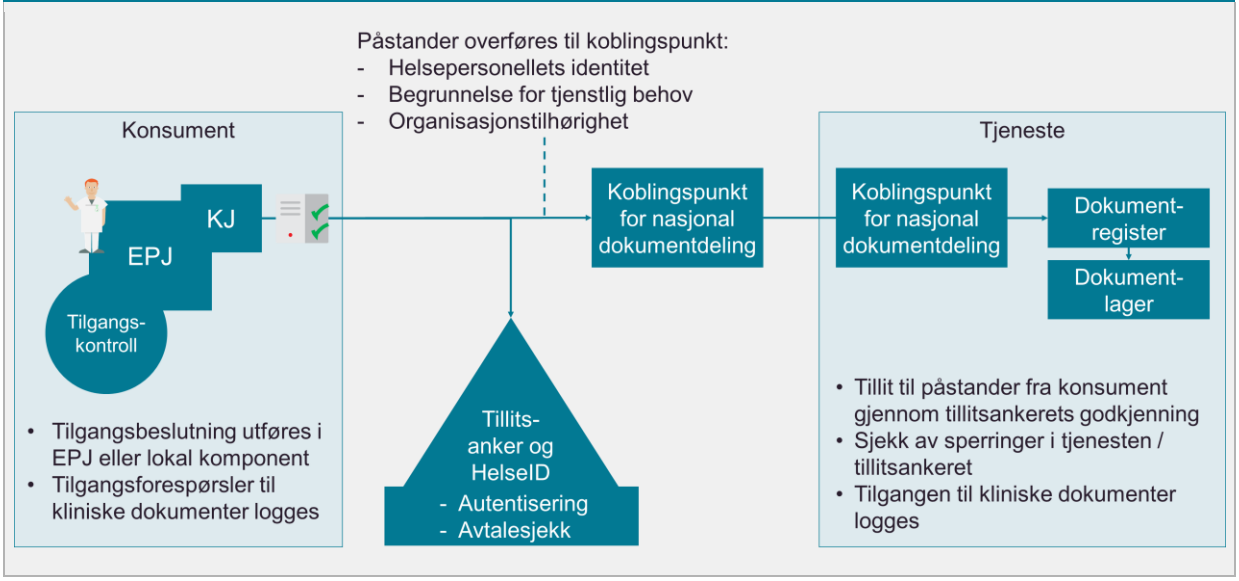
Eksempel: Helsepersonell får tilgang til kliniske dokumenter via Kjernejournal
Med tillitsmodellen i samordningsalternativet må følgende være på plass før helsepersonellet kan be om tilgang til kliniske dokumenter:

- Konsumentens virksomhet må være godkjent av tillitsankeret, herunder etterleve krav til sikkerhet, internkontroll og følge standardene som benyttes.
- Avtale må være inngått mellom konsument og tillitsanker.
- Avtale må være inngått mellom tjenesten og tillitsanker.

- Helsepersonellet må være registrert og autorisert i konsumerende virksomhet – enten i fagsystem eller i lokal tilgangsstyringskomponent.
- Virksomhetens identitetstilbyder må være tilgjengelig via HelseID. I samordningsalternativet har HelseID en kontrollerende funksjon ovenfor identitetstilbyderne, og verifiserer autentiseringsstyrke (videreformidles i sikkerhetsbilletter fra HelseID etter vellykket autentisering).
- For å etablere høy grad av tillit må både fagsystemet og Kjernejournal autentiseres som system i HelseID før de får lov til å autentisere bruker. Klientautentiseringen er basert på en konfigurasjon som må eksistere i HelseID.

Når dette er på plass vil helsepersonellet ha mulighet til å søke etter opplysninger om pasienter basert på sitt tjenstlige behov. En tilgangsprosess beskrives videre i kapitlet.

Figur 10 – Illustrasjon av bruksscenario



Dokumentdeling i bruksscenariet over vil følge følgende steg:

1. Helsepersonellet åpner sitt fagsystem og pasientens journal.
2. Tilgangsbeslutningen utføres (enten i fagsystemet, eller i tilgangsstyringskomponent som er felles for virksomheten). Her sjekkes også om det er registrert sperringer lokalt.
3. Dersom det gis tilgang til pasientens journal åpner helsepersonellet Kjernejournal for pasienten i sitt fagsystem. Kjernejournal er sikret med HelseID, og krever autentisering med tilstrekkelig autentiseringsstyrke. Helsepersonellet som er innlogget i fagsystem med kun brukernavn og passord må autentiseres med dagens sikkerhetsnivå 4 før tilgang til Kjernejournal gis.
4. Kontekstuell informasjon om helsepersonellet blir overført fra fagsystemet til sikkerhetsbillett utstedt av HelseID uten brudd i tillitskjeden slik at den kan brukes i et dokumentsøk. Informasjon som må overføres er blant annet hvilken virksomhet helsepersonellet er tilknyttet og grunnlag for tjenstlig behov.
5. Kjernejournal benytter koblingspunktet for nasjonal dokumentdeling, som gjør distribuerte dokumentsøk i foretakene. Når koblingspunktet kontakter dokumentregistrene sjekkes det for gyldig sikkerhetsbillett.
    - Sikkerhetsbilletten er signert av HelseID.
    - Sikkerhetsbilletten må inneholde tilstrekkelig informasjon om helsepersonellet. Dokumentkilden stoler på at informasjonen fra billettutsteder er korrekt.

6. Før dokumentkilden kan gi tilgang til dokumentet må den sjekke om pasienten har reservert seg mot innsyn fra det aktuelle helsepersonellet.
7. Dersom det ikke foreligger en reservasjon logges tilgangen med tilstrekkelig informasjon, og tilgang til dokumentet returneres.

Vurdering av samordningsalternativet

Skalerbarhet og utbredelse

+ Felles avtalepunkt reduserer tiden det tar å etablere samhandling med nye aktører og reduserer forvaltningsmengden av avtaler.
+ Tillitstjenester øker mindre virksomheters mulighet til å etterleve krav.
- "One size may not fit all", selv for data- og dokumentdeling.

Tillit og sikkerhet

+ Økt tillit til at tilgangsbeslutninger blir gjennomført tilfredsstillende av konsument.
+ Økt tillit til autentisering gjennom felles krav til eID-sikkerhetsnivå i hele sektoren for data- og dokumentdeling.
+ Enhetlig autentiseringsprosess for scenarier som omfatter data- og dokumentdeling.
+ Forenklet tilgangskontroll for tjenestene, basert på standardisert inndata.
- Økt behov for løsninger som skal kunne brukes for sporbarhet og etterprøvbarhet.
- Forutsetter etterlevelse av krav til sikkerhet og tilfredsstillende tilgangsbeslutninger hos konsumenter.

Understøttelse av strategisk retning og endringsevne

+ Adresserer noen av de viktigste hindrene for nye samhandlingsformer.
- Løser ikke dagens utfordringer med f.eks. utbredelse av eID på tilstrekkelig nivå.

Kostnads- og gevinstbilde

+ Økte muligheter for selvbetjening gjennom HelseID.
+ Lavere totale kostnader knyttet til forvaltning av avtaleverk og sikkerhetsvurderinger
- Økte felles kostnader til realisering av godkjenningsordning for etterlevelse av felles krav og retningslinjer.
- Etableringskostnader forbundet med tillitsankeret.
- Kostnadsdrivende for høyere sikkerhetsnivåer (som forventes).

Samlet vurdering

Samordningsalternativet styrker tilgangsstyringen i data- og dokumentdeling gjennom økt grad av samordning og standardisering, og bidrar til økt tillit mellom virksomhetene gjennom:

- Etablering av felles tillitsanker som tilbyr tillitstjenester.
- Mer enhetlig tilnærming til tilgangsstyring gjennom felles krav og retningslinjer, for eksempel ved å nedfelle disse i Normen.

- Felles avtalestruktur bidrar til økt skalerbarhet og utbredelse.
- Økt standardisering av begreper, policykrav og prosesser gir en omforent og felles forståelse av reglene som skal ligge til grunn for data- og dokumentdeling mellom virksomheter i sektoren.

Alternativet understøtter både det kortsiktige/mellomlange behovet for mer harmonisert deling, og gir i tillegg økt trygghet for at en enhetlig tilgangsstyring kan innføres i sektoren. Alternativet har høyest etableringskostnader, men vil ha lavere forvaltningskostnader og høyere andel av disse kostnadene på nasjonalt nivå. Tillitsankeret vil også kunne bidra til å fjerne hindre for realisering av helse- og omsorgssektorens langsiktige målbilder (Én innbygger – én journal, nasjonal journalløsning for kommunal helse- og omsorgstjeneste, velferdsteknologiprogrammet, helseanalyseplattformen etc).

3.4 Anbefalt utviklingsretning

De to utviklingsretningene beskrevet i kapittel 3.2 og 3.3 representerer ulike måter sektoren kan adressere utfordringene ved dagens situasjon. Vurderingen av disse opp mot videreføring av dagens situasjon er basert på de nødvendige egenskapene for fremtidig data- og dokumentdeling beskrevet i 2.1, og på kvalitative innspill fra sektoren opp gjennom arbeidet.

Tabellen nedenfor oppsummerer vurderingen av de ulike alternativene opp mot hverandre, og en overordnet oppsummering av dette er beskrevet i avsnittet under tabellen. Minus/pluss indikerer negativ/positiv utvikling relativt til ambisjonen sektoren har. Flere av samme tegn indikerer større grad av negativitet eller positivitet.

Tabell 1 – Sammenligning av alternativene

	Null-alternativet	Harmoniserings-alternativet	Samordnings-alternativet
Skalerbarhet	- - -	-	+++
Utbredelse	- - -	-	+
Tillit (inkl. sikkerhet og sporbarhet)	-	+	+
Endringsevne	- - -	-	+
Understøttelse av strategisk retning	- - -	+	++

På kort sikt vil **harmoniseringsalternativet** kunne legge grunnlaget for at data- og dokumentdeling kan foregå med økt grad av tillit, og at virksomheter i større grad utarbeider løsninger på en enhetlig måte. Dette kan være et nødvendig steg på veien, og vil bidra til å gjøre tilgangsstyring til et hinder i mindre grad. På mellomlang sikt antas det at skalerbarhetsutfordringer knyttet til avtaleforvaltning og sikkerhetsvurderinger vil være svært begrensende for hvor mange virksomheter det kan samhandles med. Harmoniseringsalternativet anses dermed som et mulig alternativ bare i en tidlig fase av data- og dokumentdeling, og tiltakene som må utføres først i harmoniseringsalternativet er også nødvendige i samordningsalternativet.

På mellomlang til lang sikt er **samordningsalternativet** det eneste alternativet som adresserer skalerbarhetsutfordringene på en tilstrekkelig måte. Med et felles avtalepunkt vil alle-til-alle samhandling mellom virksomheter som tilfredsstiller felles krav og benytter standarder være mulig. Sentrale tillitstjenester legger til rette for at virksomheter som ikke er i stand til å etterleve de overordnede kravene på egen hånd kan komme opp på et tilstrekkelig nivå. Dette gir mulighet for økt utbredelse for data- og dokumentdelingstjenester, som vil gi økte gevinster.

Nullalternativet ble på et tidlig stadium identifisert som ikke tilstrekkelig til å oppnå ønsket situasjon innenfor tilgangsstyring på tvers av virksomheter. Uten felles overordnede krav vil det være høy risiko for at løsninger for data- og dokumentdeling utvikles på ulike måter. Tilgangsstyring ville dermed fortsette å være et hinder for nye samhandlingsformer, og

utbredelsen av data- og dokumentdeling vil ikke være tilstrekkelig til å følge den politiske ambisjonen om å gi helsepersonell enkel og sikker tilgang til helse- og pasientopplysninger.

Basert på innspill fra sektoren og vurdering opp mot et sett med vurderingskriterier skiller samordningsalternativet seg ut som alternativet med høyest grad av måloppnåelse. Det anbefales derfor at Direktoratet for e-helse går videre med dette alternativet som utviklingsretning, og utarbeider en mer detaljert plan for både utprøving av sentrale deler av alternativet og for realisering av alternativet. På kort sikt anses tiltakene som er felles med harmoniseringsalternativet å være mest gevinstskapende, og disse bør utføres som et første ledd i veien mot samordningsalternativet. Kapittel 4 skisserer identifiserte tiltak for det videre arbeidet, og foreslår et veikart for realisering.

Tillitsankeret kan på sikt videreutvikles til å omfatte ulike typer tillitstjenester. Innføring av nye tillitstjenester må ses i sammenheng med sektorens behov over tid, kostnadene ved videreutvikling og øvrig e-helsestrategi. Innspill gjennom arbeidet med denne vurderingen antyder at det ikke nødvendigvis vil være behov for mange tillitstjenester, men at ambisjonsnivået bør være å få gjennomført de sentrale tiltakene i samordningsalternativet.

4 Realisering av anbefalt alternativ

4.1 Prioriterte tiltaksområder

Realisering av samordningsalternativet bør gjøres som et sett av sentralt koordinerte tiltak som samlet legger til rette for tilgangsstyring for data- og dokumentdeling mellom virksomheter. Utbredelsen av etablerte data- og dokumentdelingstjenester i sektoren er fortsatt lav, men det må forventes at både antall tjenester og volumet på bruken av disse vil øke kraftig fremover etter hvert som nye e-helsetjenester blir utviklet og tatt i bruk av sektoren.

Anbefalte tiltak i samordningsalternativet er satt sammen i tiltaksgrupper som adresserer utfordringene beskrevet i kapittel 2.2, og beskrives videre i dette kapittelet. Følgende tiltaksgrupper er blitt identifiserte som sentrale for realisering av alternativet:

- Felles krav og retningslinjer
- Avtalemodell
- Sikkerhetsvurderinger
- Standardisering
- Tillitstjenester

4.1.1 Felles krav og retningslinjer

Det bør utarbeides overordnede krav (policykrav) som skal ligge til grunn for tilgangsstyring ved bruk av data- og dokumentdelingstjenester i sektoren, samt retningslinjer for hvordan kravene kan etterleves. De overordnede kravene skal tydeliggjøre roller og ansvar for alle aktører som er involverte i data- og dokumentdeling, og hvilke forretningsregler som skal ligge til grunn for deling. Kravene bør forankres og besluttes bredt, og nedfelles i Normen.

For at kravene skal kunne være tydelige nok og dekke relevant regelverk bør det gjennomføres en vurdering av lover og forskrifter der tilgangsstyring er nedfelt, hvor det vil kunne være behov for mer lik og enhetlig tolkning av krav og prinsipper.

Eksempler på områder som bør bli nedfelt som policykrav:

- Overordnede prinsipper og avgrensninger for innretting av tillitskjeden mellom virksomheter, for eksempel:
    - Minstekrav til sikkerhetsnivå for identifisering av helsepersonell.
    - Hvordan sperringer etc. skal ivaretas.
    - Dataansvarlige i et økosystem av data- og dokumentdelingstjenester.
- Hva som ligger i ansvaret for å beslutte om tjenstlig behov foreligger.
- Hva som ligger i ansvaret for tilgangskontroll hos tjenestene.
- Hva som ligger i ansvaret for verifikasjon av kontekstuell informasjon om helsepersonell, virksomhetstilhørighet osv.

Det bør gjennomføres et innledende arbeid med å definere prinsipper for data- og dokumentdeling og identifisere tilstrekkelig med krav til at en "driftsmodell" (operating model) for tilgangsstyring i data- og dokumentdeling kan utledes. Anbefalingen av samordningsalternativet peker allerede på relevante kravsett som bør nedfelles som policykrav og bli besluttet i sektorens styringslinje tidlig i realiseringsfasen. Det er også

høstet erfaring rundt krav gjennom andre leveranser i FIA Data- og dokumentdeling og gjennom andre prosjekter som det kan bygges videre på.

4.1.2 Avtalemodell

Et sentralt forhold som må adresseres tidlig i realiseringsfasen er avtalemodellen som skal ligge til grunn for tillit mellom partene som skal inngå i samme tillitskjede. For området data- og dokumentdeling vil det være hensiktsmessig å etablere et felles avtaleverk, der alle inngår avtaler med et felles tillitsanker og avtalene forvaltes av tillitsankeret. Dette er en forenkling av dagens avtalemodell som forventes å gi bedre skaleringsegenskaper enn det dagens én-til-én modell for avtaler har.

I et voksende økosystem av data- og dokumentdelingstjenester med mange parter vil et felles avtaleverk bidra til å redusere antall avtaler som må inngås, forenkle inngåelsen av nye avtaler og forenkle forvaltningen av avtalene over tid.

Tekniske mekanismer i HelseIDs infrastruktur vil kunne benyttes til å verifisere at tillits- og avtaleforhold ivaretas i forbindelse med samhandling. HelseID som grunnmurskomponent vil også kunne utvides med funksjonalitet som kan automatisere viktige deler av tillitsankerets oppgaver, eksempelvis selvbetjeningsløsninger for inngåelse av nye avtaleforhold.

Dataansvarlig for data- og dokumentdeling i samordningsalternativet

Virksomheten som tilbyr en data- eller dokumentdelingstjeneste vil som "eier" av opplysningene som skal behandles være dataansvarlig. Dataansvarlig er den som bestemmer til hvilke formål og på hvilken måte opplysningene skal behandles. Det er dataansvarlig som selv bestemmer akseptabelt nivå for risikoen knyttet til behandlingen. Ny forskrift om pasientjournal legger opp til en mer risikobasert tilnærming til valg av akseptabelt nivå, noe som understøtter at virksomhetene kan ha ulik risikoappetitt og at det er opp til virksomhetene å sette inn nødvendige sikringstiltak for å nå akseptabelt nivå. Det vil være nødvendig med konsensus i sektoren for å sette et nivå for akseptabel risiko, men sikringstiltakene for å oppnå nivået kan variere mellom helsevirksomhetene.

Helsevirksomhetene er ansvarlige for å sikre dataenes konfidensialitet, tilgjengelighet og integritet, men kan i avtale gi databehandler oppgaven med å ivareta enkelte krav til dokumentasjon, oppfølging og kontroll av tilgangsstyring, autentisering og autorisasjon på vegne av seg. Dataansvarlig kan aldri avtale bort sitt formelle ansvar, og databehandler kan aldri behandle dataene på annen måte enn det som følger av avtalen med dataansvarlig. Databehandler har plikt til å bistå den dataansvarlige med overholdelse av rettighetene som den enkelte registrerte har, som for eksempel ivaretakelse av den registrertes innsynsrett i hvilket helsepersonell som har fått tilgang til opplysningene, samt sørge for at det finnes teknisk funksjonalitet for å overholde muligheten for å sperre enkeltpersonell, grupper av helsepersonell eller virksomheters tilgang til opplysningene i hele eller deler av journalen.

Dataansvarlig har selv ansvar for å sikre at det foreligger tilstrekkelige rutiner for internkontrollaktiviteter, og for å vurdere om tidligere satt nivå for akseptabel risiko fremdeles er gjeldende eller om det må justeres ved endringer. En del av dette inkluderer rettighet til å revidere tillitsankeret for å kunne vurdere om kravene ivaretas på en tilstrekkelig måte.

4.1.3 Sikkerhetsvurderinger

Før data og dokumenter skal kunne deles med en annen virksomhet må det vurderes om delingen innebærer en akseptabel risiko. Ved å standardisere gjennomføringen av risikovurderinger i større grad reduseres kostnader tilknyttet dette, og det legges til rette for

bedre konsistens i vurderingene som gjøres. I første omgang bør det enes om en felles fremgangsmåte for risikovurderinger som kan brukes på tvers av helse- og omsorgssektoren. Slik kan hver virksomhet vurdere risiko i data- og dokumentdeling på en mer enhetlig måte, og vurderingene vil baseres på de samme faktorene.

Eksempler på områder i tillitskjeden som vil kunne bli vurdert i en felles risikovurdering:

- Risikostyring og forvaltning av styringssystemet.
- Autentiseringsstyrke, brukerutstedelse og brukerforvaltning.
- Sporbarhet og etterkontroll av autorisasjoner og tilganger som er gitt.

Det er en stor variasjon i virksomheter i helsesektoren når det gjelder størrelse, kompetanse og modenhet til å gjennomføre risikovurderinger. Det kan derfor også være nødvendig med opplæring og kompetansebygging for hvordan sikkerhetsvurderinger av nye tjenester skal gjennomføres. Felles krav og retningslinjer for alle leddene som er involvert i en tilgangsforespørsel mellom virksomheter vil også gjøre det lettere å utføre sikkerhetsvurderinger og koordinere tiltak for å sikre etterlevelse.

4.1.4 Standardisering

For å sikre samhandlingsevnen i forbindelse med tilgangsstyring må det oppnås enighet om hvordan informasjonen som benyttes i en tilgangsbeslutning skal formuleres. Det er nødvendig å etablere et felles vokabular for å beskrive helsepersonellets rolle, organisasjonstilhørighet, grunnlag for tjenstlig behov samt annen relevant informasjon. Denne informasjonen danner også grunnlaget for at logger kan tilfredsstille krav i lover og forskrifter.

Samhandlingsevne og skalerbarhet påvirkes også i stor grad av hvordan informasjonen som benyttes i en tilgangsbeslutning formateres og utveksles mellom konsument og tjeneste. Det bør stilles nasjonale krav til bruk av standardiserte protokoller og spesifikasjoner for autentisering og autorisasjonsformål i forbindelse med tilgang til helseinformasjon på tvers av virksomheter.

I samordningsalternativet benyttes HelseID som utsteder av tilgangsbillett for tilgangspunkt for deling av data. Innholdet i tilgangsbilletten bør standardiseres, og formidle identiteten til både personen og virksomheten som forespør deling av informasjon, samt angi begrunnelse for tjenstlig behov for tilgang som vurdert av den forespørrende virksomheten. Angivelse av type tjenstlig behov bør være basert på felles standardiserte regler og prinsipper for vurdering av tjenstlig behov. Standardisering av regler og prinsipper for tjenstlig behov, samt format og innhold i tilgangsbilletten bør utredes nærmere sammen med utredning av løsning for utstedelse av billett av HelseID i samarbeid med forespørrende virksomhet.

Arbeidet med å standardisere informasjonen som skal benyttes og legges til grunn for tilgangsbeslutninger bør påbegynnes tidlig og forbedres over tid. Erfaring tilsier at denne typen aktiviteter er tidkrevende på veien mot forankring i styringslinjene, selv om det allerede i utgangspunktet foreligger et godt grunnlag på flere sentrale områder.

4.1.5 Nasjonale tillitstjenester

Samordningsalternativet omfatter en stegvis videreutvikling av et tillitsanker for digital samhandling i helse- og omsorgssektoren. Konkretisering av alternativet bør utformes i miljøet rundt dagens HelseID, som består av en infrastrukturløsning og driftstjeneste som understøtter autentisering mellom virksomheter. For å muliggjøre sentrale tillitstjenester og

tillitsmodellen som ligger i samordningsalternativet må forvaltningen styrkes over tid, og det vil være behov for å etablere ny funksjonalitet i felles infrastruktur.

I første omgang er det behov for å identifisere hvilke tillitstjenester som bør prioriteres, og det kan være nødvendig å prøve ut noen av disse tidlig. I tillegg må det finnes og prøves ut konkrete tekniske løsninger for overføring av informasjon om helsepersonell, begrunnelse for tjenstlig behov og tilhørighet til virksomhet. Det bør også vurderes hvilke felles grunndata som bør benyttes ved utstedelse av tilgangsbillett. For eksempel vil fastlegeregisteret kunne benyttes til å verifisere at fastleger som forespør tilgang faktisk er pasientens fastlege, eller HPR-registeret til å verifisere at helsepersonellets autorisasjon fortsatt er gyldig. Det bør også vurderes nærmere om det er behov for en tjeneste som håndterer sperringer for hele sektoren.

Helse- og omsorgssektoren har vært en sentral bruker av «Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor». Med innføringen av den nye EU forordningen for tillitstjenester (eIDAS) har Difi utarbeidet et oppdatert rammeverk som er harmonisert med de nye kravene og som foreslår at dagens tillitsnivåer erstattes med tillitsnivåene i eIDAS[16]. Helseregionene samarbeider allerede om å vurdere tillitsnivå og tillitstjenester som best vil ivareta sektorens behov.

Det bør legges til rette for en høy grad av selvbetjening i HelseID for å begrense omfanget av forvaltning som HelseID må ha. Prosesser rundt etablering av tjenester i HelseID kan i stor grad digitaliseres med selvbetjening slik at kontrollmekanismer kan understøtte automatisert autentisering og tilgangskontroll. Virksomheter som tilbyr deling av data bør via selvbetjening i HelseID kunne registrere og administrere sine grensesnitt for datadeling, inkludert angivelse av sikkerhetsnivå i systemer og til autentisering av personer som benytter grensesnitt. Virksomheter som henter data bør via selvbetjening i HelseID kunne finne tilgangspunkter til datadeling samt registrere og administrere sine systemer som benytter tilgangspunktene.

Det bør etableres et felles regime for registrering og bruk av ulike eID-løsninger i HelseID. Dette vil bidra til at virksomheter vil kunne forstå og ha tillit til sikkerhetsnivået som oppgis for hvert enkelt eID. Virksomheter som identifiserer og autentiserer ansatte og andre brukere av sine IKT-systemer ved hjelp av egenutstedte eID-er bør kunne inngå avtale med tillitsankeret om bruk av eID-ene med HelseID. Denne avtalen kan inneholde krav til tillitsnivå i eID-ene, samt krav til etablering og oppfølging av integrasjonen. Integrasjonen kan etableres for eID-er på ulike sikkerhetsnivå, og gir mulighet for single sign-on funksjonalitet ved data- og dokumentdeling.

HelseID bør utvides til å logge tilstrekkelig med informasjon om aktiviteter og handlinger som gjennomføres, eksempelvis identifisering av helsepersonell og utstedelse av sikkerhetsbilletter. Ved behov for etterkontroll eller sikkerhetshendelser vil logginformasjon kunne utleveres til de aktørene som vil ha behov for å vurdere hvilke handlinger som lå til grunn for tilgangsbeslutninger og tilgangskontroll.

4.2 Forslag til veikart for samordningsalternativet

I Figur 11 illustreres et forslag til veikart for realisering av samordningsalternativet. Veikartet viser et forslag til prioritering av tiltakene som ble introdusert i kapittel 4.1.

[16] Høringsutkast til Rammeverk for identifikasjon og sporbarhet i elektronisk kommunikasjon med og i offentlig sektor (Utkast per 22.06.2018).

Figur 11 – Forslag til veikart for realisering av samordningsalternativet

Utprøving

I første omgang er det behov for å legge grunnlaget for samordningsalternativet. Dette bør skje gjennom erfaringsbasert utprøving, i samarbeid med et pågående initiativ i sektoren. Erfaringsbasert utprøving innebærer at det gjennom et pågående prosjekt trekkes ut læring og identifiseres utfordringer som bør avklares på et nasjonalt nivå. Eksempler på avklaringer som bør gjøres er hvilke nasjonale tillitstjenester som vil være nødvendige for å oppnå tillit til ulike aktørgrupper, og om sperringer bør håndteres distribuert eller sentralisert på sikt. Det er høstet mye erfaring med krav og avtaleverk gjennom arbeidet med denne rapporten og andre prosjekter, som kan brukes som grunnlag inn i utprøvingen.

Det foreslås at utprøvingen gjennomføres i løpet av 2019. I forlengelsen av arbeidet med denne rapporten vil det gjennomføres et planleggingsarbeid, der veikartet vil bli detaljert videre, og omfang og mål for utprøvingen vil bli definert.

Etablering av tillitsankeret

Etter at det i utprøvingsfasen har blitt identifisert hvilke prinsipper, krav og standarder som skal ligge til grunn kan tillitsankeret etableres, med avtalestruktur og godkjenningsordning opp mot felles krav og retningslinjer. I etableringsfasen vil følgende være sentralt:

- Tillitstjenestene som det er identifisert et stort behov for bør utprøves og etableres.
- Det bør legges opp til høy grad av selvbetjening i avtalehåndteringen og rundt HelseID for å redusere behovet for forvaltning av tillitsankeret.
- Godkjenningsordningen bør etableres med selvdeklarering. Sikkerhetsvurderinger kan utføres i regi av tillitsankeret dersom det er nødvendig for å ha tillit til godkjenningsordningen etter hvert som forvaltningskapasiteten økes[17].

[17] Ved hjelp av aktører i markedet, andre statlige organer eller aktiviteter i regi av tillitsankeret selv.

- Det må sørges for at felles grunndata som skal benyttes i tilgangsstyringen har tilstrekkelig kvalitet og tilgjengelighet til formålet.
- Det må sørges for tilstrekkelig endringsevne til å ta i bruk nye tjenester som kan tilføre ytterligere informasjon i tilgangsstyringen, f.eks. innføring av et sentralt register for sperringer.

Etablering av ytterligere tillitstjenester bør vurderes opp mot sektorens behov og øvrig e-helsestrategi. Tillitstjenester som støtter virksomheter som ikke er i stand til å oppfylle krav på egen hånd bør prioriteres.

5 Vedlegg 1 – Arbeidsgruppen

Tabell 2 – Liste over virksomheter som har stilt med representanter i prosjektets arbeidsgruppe
Helse Vest
Helse Midt
Helse Nord
Helse Sør-Øst
Nasjonal IKT (NIKT)
Kommunal informasjonssikkerhet (KINS)
KS
Bergen kommune
Stavanger kommune
Oslo kommune
Trondheim kommune

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO