Møte i Nasjonalt e-helsestyre		
Møte	3/2021	
Dato	10. juni 2021	
Tid	Kl. 10.00 – 13.00	
Sted	Videomøte	
Medlemmer	Inger Cathrine Bryne (Helse Vest RHF) Stig Slørdahl (Helse Midt-Norge RHF) Cecilie Daae (Helse Nord RHF) Jan Frich (Helse Sør-Øst RHF) Karl Vestli (Direktoratet for e-helse) Jan Arild Lyngstad (Helsedirektoratet) Gun Peggy Knudsen (Folkehelseinstituttet) Kristin W. Wieland (KS) Svein Lyngroth (Oslo kommune) Camilla Dunsæd (Kristiansand kommune)	Bjørn-Atle Hansen (Alta kommune) Kjell Wolff (Bergen kommune) Lilly Ann Elvestad (FFO) Mina Gerhardsen (Nasjonalforeningen for folkehelsen) Ivar Halvorsen (Legeforeningen) Steffen Sutorius (Digitaliseringsdirektoratet) Lill Sverresdatter Larsen (Norsk Sykepleierforbund)
Observatører	Johan Ronæs (Norsk Helsenett SF)	

Sak	Agenda Nasjonalt e-helsestyre	Tidspunkt	Sakstype
15/21	Godkjenning av innkalling og dagsorden	10:00	Godkjenning
16/21	Godkjenning av referatet fra Nasjonalt e-helsestyre 6. mai 2021	10:03	Godkjenning
17/21	Orientering fra Direktoratet for e-helse	10:05	Orientering
18/21	Strategi digital sikkerhet i helse- og omsorgssektoren – tilslutning til første leveranse tiltaksoversikten	10:15	Tilslutning
19/21	Nasjonal e-helseportefølje – status og planer	10:55	Drøfting
	Pause	11:15	
20/21	Ny nasjonal e-helsestrategi fra 2023	11:25	Drøfting
21/21	Strategiplan for digitalisering av legemiddelområdet	11:55	Drøfting
22/21	Eventuelt	12:25	

Sak	Tema	Sakstype
15/21	**Godkjenning av innkalling og dagsorden**	**Godkjenning**
	Forslag til vedtak: Nasjonalt e-helsestyre godkjenner innkalling og dagsorden.	
16/21	**Godkjenning av referatet fra Nasjonalt e-helsestyre 6. mai 2021**	**Godkjenning**
	Forslag til vedtak: Nasjonalt e-helsestyre godkjenner referatet fra ekstra møtet 6. mai 2021.	**Vedlegg 1:** Referat fra Nasjonalt e-helsestyre 6. mai 2021
17/21	**Orientering fra Direktoratet for e-helse**	**Orientering**
	Direktoratet for e-helse vil orientere Nasjonalt e-helsestyre som status på følgende saker: • Status videreutvikling nasjonal styringsmodell • Riksrevisjonens rapporter • Forskningsprosjekt knyttet til styringsmodellen på e-helseområdet	**Vedlegg 2:** Toppnotat Orientering fra Direktoratet for e-helse
	Forslag til vedtak: Nasjonalt e-helsestyre tar sakene til orientering.	
18/21	**Strategi digital sikkerhet i helse- og omsorgssektoren – tilslutning til første leveranse tiltaksoversikten**	**Tilslutning**
	Direktoratet for e-helse vil orientere Nasjonalt e-helsestyre om arbeidet med utarbeidelse av Strategi for digital sikkerhet i helse- og	**Vedlegg 3:** Toppnotat Strategi digital sikkerhet i

	omsorgssektoren og få tilslutning til tiltaksoversikten som skal sendes til Helse- og omsorgsdepartementet 18. juni.	helse- og omsorgssektoren **Vedlegg 3A:** Tiltaksoversikt til Strategi for digital sikkerhet for helse- og omsorgssektoren v0.7
	Forslag til vedtak: Nasjonalt e-helsestyre tilslutter seg tiltaksoversikten utarbeidet i forbindelse med Strategi for digital sikkerhet i helse- og omsorgssektoren som skal leveres til Helse- og omsorgsdepartementet 18. juni 2021.	
19/21	**Nasjonal e-helseportefølje – status og planer**	**Drøfting**
	Direktoratet for e-helse ønsker å: 1. Orientere Nasjonalt e-helsestyre om status nasjonal e-helseportefølje nå og om nasjonal e-helseportefølje for 2022. 2. Drøfte utvalgte utfordringer i porteføljen. Vedlegg 4A er lenket opp til ehelse.no i toppnotatet, samt i høyre kolonne her i agendaen.	**Vedlegg 4:** Toppnotat Nasjonal e-helseportefølje – status og planer **Vedlegg 4A:** Nasjonal e-helseportefølje mai 2021
	Forslag til vedtak: Nasjonalt e-helsestyre tar status for nasjonal e-helseportefølje til orientering. Nasjonalt e-helsestyre ber Direktoratet for e-helse ta med seg innspill gitt i møtet i det videre arbeidet.	
20/21	**Ny nasjonal e-helsestrategi fra 2023**	**Drøfting**
	Direktoratet for e-helse legger frem plan for arbeidet med utvikling av ny e-helsestrategi. Denne drøftingen skal ikke dreie seg om innholdet eller mål i strategien, men prosessen knyttet til å utarbeide den og hvordan den kan/bør benyttes. Det ønskes innspill fra Nasjonalt e-helsestyre ut fra følgende spørsmål: • Hvilke innspill har Nasjonalt e-helsestyre til plan for arbeidet med utvikling av ny e-helsestrategi? • Hva er det viktigste en felles nasjonal e-helsestrategi skal bidra til i årene fremover?	**Vedlegg 5:** Toppnotat Ny nasjonal e-helsestrategi fra 2023
	Forslag til vedtak: Nasjonalt e-helsestyre ber Direktoratet for e-helse ta med seg innspill mottatt i møtet i det videre arbeidet.	
21/21	**Strategiplan for digitalisering av legemiddelområdet**	**Drøfting**
	Direktoratet for e-helse ønsker å drøfte innretning på videre prosess for forankring av strategiplan for digitalisering av legemiddelområdet. Bakgrunn og status for arbeidet vil bli presentert som grunnlag for drøfting.	**Vedlegg 6:** Toppnotat Strategiplan for digitalisering av legemiddelområdet
	Forslag til vedtak: Nasjonalt e-helsestyre drøfter saken og ber Direktoratet for e-helse ta med seg innspillene gitt i møtet i det videre arbeidet.	
22/21	**Eventuelt**	

Referat fra møte i Nasjonalt e-helsestyre

Møte	2/2021	
Dato	6. mai 2021	
Tid	Kl. 13.00 – 15.30	
Sted	Videomøte	
Medlemmer		
Til stede	Stig Slørdahl (Helse Midt-Norge RHF) Cecilie Daae (Helse Nord RHF) Cathrine Loftshus (Helse Sør-Øst RHF) Karl Stener Vestli (Direktoratet for e-helse) Jan Arild Lyngstad (Helsedirektoratet) Gun Peggy Knudsen (Folkehelseinstituttet) Kristin W. Wieland (KS) Svein Lyngroth (Oslo kommune) Camilla Dunsæd (Kristiansand kommune)	Kjell Wolff (Bergen kommune) Lilly Ann Elvestad (FFO) Mina Gerhardsen (Nasjonalforeningen for folkehelsen) Steffen Sutorius (Digitaliseringsdirektoratet) Lill Sverresdatter Larsen (Norsk Sykepleierforbund)
Ikke til stede	Ivar Halvorsen (Legeforeningen) Inger Cathrine Bryne (Helse Vest RHF)	Bjørn-Atle Hansen (Alta kommune)
Stedfortreder	Eirik Arnesen (Legeforeningen) – for Ivar Halvorsen	Erik Hansen (Helse Vest RHF) – for Inger Cathrine Bryne
Observatører	Johan Ronæs (Norsk Helsenett SF)	
Direktoratet for e-helse	Jon Helge Andersen Hans Löwe Larsen Siv Ingebrigtsen	Sonja Turøy Brugman Vibeke Jonassen Wang Karen Lima

Sak	Agenda Nasjonalt e-helsestyre	Sakstype
9/21	Godkjenning av innkalling og dagsorden	Godkjenning
10/21	Godkjenning av referatet fra Nasjonalt e-helsestyre 18. mars 2021	Godkjenning
11/21	Orientering fra Direktoratet for e-helse	Orientering
12/21	Program digital samhandling – målbilde og gjennomføringsstrategi for helhetlig samhandling	Drøfting
13/21	Nasjonalt e-helsestyre – mulighet for stedfortreder, forslag til midlertidig ordning	Tilslutning
14/21	Eventuelt	

Sak	Tema
9/21	**Godkjenning av innkalling og dagsorden**
	Det kom ingen innspill til innkalling og dagsorden.
	Vedtak: Nasjonalt e-helsestyre godkjenner innkalling og dagsorden.
10/21	**Godkjenning av referatet fra Nasjonalt e-helsestyre 18. mars 2021**
	Det kom ingen innspill til referat fra Nasjonalt e-helsestyre 18. mars 2021.
	Vedtak: Nasjonalt e-helsestyre godkjenner referatet fra møtet 18. mars 2021.
11/21	**Orientering fra Direktoratet for e-helse**
	Karl Vestli, Direktoratet for e-helse orienterte Nasjonalt e-helsestyre om status på følgende saker: • Ny direktør i Direktoratet for e-helse • Prosess knyttet til etterlevelse- og forvaltningsrevisjon av Riksrevisjonen

	• Status møter om styringsmodellen Nasjonalt e-helsestyre kommenterte at de har vært involvert i mange av tiltakene som Riksrevisjonen gransker. Nasjonalt e-helsestyre har bl.a. vært styringsgruppe for Én innbygger - én journal. Sentrale personer som har deltatt i dette arbeidet har ikke blitt kontaktet av Riksrevisjonen, medlemmene ønsker derfor at Direktoratet for e-helse redegjør for funnene når rapporten offentliggjøres.
	Vedtak: Nasjonalt e-helsestyre tar sakene til orientering.
12/21	**Program digital samhandling – målbilde og gjennomføringsstrategi for helhetlig samhandling**
	Hans Löwe Larsen og Erik Hovde, Direktoratet for e-helse orienterte Nasjonalt e-helsestyre om bakgrunnen for og innhold i programmets målbilde for samhandling, og hvordan dette henger sammen med målene i veikart for nasjonale e-helseløsninger 2021-2025. <u>Følgende spørsmål ble lagt frem for drøfting:</u> Hvordan skal vi legge til rette for at nødvendig støtte for samhandling utvikles for helse- og omsorgssektoren, uten å overstige helsesektorens kapasitet for å delta i denne type arbeid? • Hvordan bør sektor prioritere ressurser i ulike faser, slik at gevinstene kan hentes ut? • Hvordan bør balansen være mellom tiltak rettet mot lokale/regionale behov versus tiltak rettet mot nasjonale behov? **Følgende innspill ble tatt med fra møtet:** • Det er vanskelig å få til samstyring av helheten da kommunal sektor har en annen styring og finansiering enn statlige aktører. • Ute i kommunene arbeides det med felles plan og rammeverk for kommunal prioritering. KS bidrar til større grad av eierskap i flere kommuner. • "Design-to-cost" er en krevende modell å jobbe etter, da den brukes når tiltakseier og den som får gevinst er samme aktør. Dette er ikke alltid tilfellet i arbeidet med samhandlingsløsninger. Innføring lokalt, har andre kostnader enn innføring nasjonalt. "Design-to-value" modell kan være et alternativ. • Smidig tilnærming er viktig fra et innbyggerperspektiv. Da vil innbygger oppleve den forbedrede samhandlingen underveis. Innbyggere læres gradvis opp til å ta i bruk disse samhandlingsløsningene. Det ble påpekt at man også må ha oppmerksomhet på innbyggers kapasitet. • Det er en utfordring for innbygger å orientere seg i løsninger som innføres. Det er store forskjeller i utviklings- og implementeringstakt i kommunene, noe som kan gi store geografiske ulikheter i tilbudet til innbyggerne. • Helsenorge er ikke tilgjengelig for alle; digitalt utenforskap er viktig å adressere. • Vi må i så stor grad som mulig gjenbruke etablerte arenaer. Nasjonalt e-helsestyre må være et topplederforum, mens program- og prosjektstyrer må være på et mer operativt nivå. • Ved drøftingssaker er det viktig at saksunderlaget tydeliggjør problemstillingene og hva direktoratet ønsker fra medlemmene i Nasjonalt e-helsestyre i den aktuelle saken. Det er viktig for å ivareta et topplederperspektiv. • Saksunderlaget og presentasjonen tegnet forskjellige bilder. I saksunderlaget manglet innbyggerperspektivet, mens presentasjonen viste målbilde med utgangspunkt i innbyggers behov.

	• Når det kommer store spørsmål det ønskes drøfting på er det problematisk at vi ikke har fått mulighet til å drøfte i forkant av møtet. Vi som medlemmer får ikke mulighet til å gi en ryddig tilbakemelding. Direktoratet for e-helse kommenterte at Program digital samhandling både er et leveranseprogram og et strategisk program for sektoren. Direktoratet ønsker å skille på disse diskusjonene. Det har i tiden fra sakspapirene ble sendt ut og frem til møtet blitt jobbet med å løfte frem strategiske problemstillinger fra programmet. Direktoratet vil jobbe videre med å sikre saksdokumenter som legger til rette for gode diskusjoner i Nasjonalt e-helsestyre. Direktoratet for e-helse nevnte at ved generelle spørsmål er det fint å få noen betraktninger fra Nasjonalt e-helsestyre uten de store forberedelsene.
	Vedtak: Nasjonalt e-helsestyre hadde en innledende drøfting av problemstillingene i saken og ber prosjektet ta innspill med inn i videre arbeid.
13/21	**Nasjonalt e-helsestyre – mulighet for stedfortreder, forslag til midlertidig løsning**
	Karl Vestli, Direktoratet for e-helse, la frem forslag om at medlemmene i Nasjonalt e-helsestyre ved behov kan stille med fast stedfortreder med talerett i møtene. Det ble foreslått at dette er en midlertidig ordning frem til reviderte mandat for utvalgene i nasjonal styringsmodell legges frem for tilslutning og drøfting høsten 2021. Nasjonalt e-helsestyre stilte seg bak forslaget. Medlemmene mener det er viktig at Nasjonalt e-helsestyre forsetter som en toppleder-arena. Det er derfor en forpliktelse at medlemmene bruker muligheten for stedfortreder med forsiktighet.
	Vedtak: Nasjonalt e-helsestyre gir sin tilslutning til at medlemmene i Nasjonalt e-helsestyre ved behov kan stille med faste stedfortreder med talerett i møtene. Ordningen gjelder frem til reviderte mandat for utvalgene i nasjonal styringsmodell legges frem for tilslutning og drøfting høsten 2021.
14/21	**Eventuelt**
	Ingen saker til eventuelt

Til	Møte 3/21
Dato	10.06.2021
Saksnummer	17/21
Type	Orientering

Fra	Karl Stener Vestli
Saksbehandler	Vibeke Jonassen Wang

Overskrift

Forslag til vedtak

Nasjonalt e-helsestyre tar sakene til orientering.

Hensikt med saken

Direktoratet for e-helse ønsker å orientere Nasjonalt e-helsestyre om følgende saker:

- Status videreutvikling nasjonal styringsmodell
- Riksrevisjonens rapporter
- Forskningsprosjekt knyttet til styringsmodellen på e-helseområdet

Bakgrunn

Direktoratet redegjør gjennom dette notatet for innholdet i sakene. I møtet vil direktoratet ha en kort presentasjon av sakene.

Status videreutvikling nasjonal styringsmodell

Direktoratet for e-helse gjennomførte dialogmøter med medlemmene av Nasjonalt e-helsestyre i april og mai. Dette har gitt nyttige tilbakemeldinger til hvordan nasjonal styringsmodell for e-helse kan videreutvikles. Det pågår nå et analysearbeid med å sammenstille funnene fra dialogmøtene. Dette grupperes i temaer som skal drøftes med sektor og temaer som vil bli håndtert internt. Det vil bli satt opp arbeidsmøter med sektor for videre drøfting av videreutviklingen før og etter sommeren. Innkallinger til disse møtene vil bli sendt til NUIT representantene. Reviderte mandater for de nasjonale utvalgene drøftes i møtene i styringsmodellen i tredje kvartal 2021.

Riksrevisjonens rapporter

Dato for offentliggjøring er endret til 22. juni, fra 29. juni opprinnelig. Nasjonalt e-helsestyre vil holdes orientert ved publisering av rapportene.

Forskningsprosjekt knyttet til styringsmodellen på e-helseområdet

Direktoratet for e-helse har blitt kontaktet av ph.d. student Line Linstad fra Nasjonalt senter for e-helseforskning i forbindelse med rekruttering av informanter til forskningsprosjekt *"Samstyring i e-helse: modeller og strategier for å realisere helsepolitiske mål"*. Formålet er å studere hvordan styringsmodellen på e-helseområdet i Norge fungerer og hvordan styringsmodeller beskrevet i forskningslitteraturen kan sammenlignes med den norske modellen og modellens gjennomføringskraft.

Direktoratet håper at medlemmer i Nasjonalt e-helsestyre stiller seg positive til å være informanter i dette prosjektet og at Line Lindstad tar kontakt.

Til	Møte 3/21
Dato	10.06.2021
Saksnummer	18/21
Type	Tilslutning
Fra	Hans Løwe Larsen
Saksbehandler	Jan Gunnar Broch

Strategi for digital sikkerhet i helse- og omsorgssektoren – tilslutning til første leveranse tiltaksoversikten

Forslag til vedtak

Nasjonalt e-helsestyre tilslutter seg tiltaksoversikten utarbeidet i forbindelse med Strategi for digital sikkerhet i helse- og omsorgssektoren som skal leveres til Helse- og omsorgsdepartementet 18.juni 2021

Hensikt med saken

Hensikten med saken er å orientere Nasjonalt e-helsestyre om arbeidet med utarbeidelse av Strategi for digital sikkerhet i helse- og omsorgssektoren og å få tilslutning til tiltaksoversikten som skal sendes til Helse- og omsorgsdepartementet 18.juni.

Arbeidet med ferdigstilling av tiltaksoversikten pågår, og nasjonalt e-helsestyre har fått oversendt versjon 0.7. Denne versjonen er også sendt på innspillsrunde til prosjektets hovedsamarbeidspartnere med frist for tilbakemelding i uke 23. Det vil kunne forekomme endringer i formuleringer og andre mindre justeringer, samt at det kan bli lagt til ytterligere eksisterende tiltak som følge av tilbakemeldinger i innspillsrunden. I all hovedsak vil ikke dokumentets struktur endres i den endelige leveransen. Eventuelle forslag til nye tiltak som kommer inn før behandling i Nasjonalt e-helsestyre vil tas med videre i strategiprosessen og adresseres i strategien eller i oppdatert versjon av tiltaksoversikten ved utgangen av 2021.

Tilslutningen innebærer at Nasjonalt e-helsestyre stiller seg bak at tiltakene i tiltaksoversikten er hensiktsmessige og vil bidra til å gjøre Strategi for digital sikkerhet i helse- og omsorgssektoren konkret og handlingsrettet. Tilslutningen vil ikke binde berørte aktører økonomisk.

Bakgrunn

På oppdrag for Helse- og omsorgsdepartementet gjennom tildelingsbrev for 2021 utarbeider Direktoratet for e-helse en Strategi for digital sikkerhet i helse- og omsorgssektoren. Strategien skal tydeliggjøre roller og ansvar, og identifisere relevante strategiske virkemidler og tiltak for å løfte arbeidet med digital sikkerhet i sektoren. Det ble utarbeidet en forstudie for prosjektet i 2020 på oppdrag fra HOD: Strategi for digital sikkerhet i helse- og omsorgssektoren - vurdering av behov og innretning (IE-1064).

Arbeidet utføres i samarbeid med Helsedirektoratet, Helsetilsynet, Norsk Helsenett SF, de regionale helseforetakene og kommunesektoren/KS. Disse aktørene inngår i både prosjektets styringsgruppe og i utvidet kjerneteam.

Som delleveranse skal det 18. juni leveres en tiltaksoversikt for helse- og omsorgssektoren som skal understøtte strategien og sikre at den blir handlingsrettet. Tiltaksoversikten bygger videre på Nasjonal strategi for digital sikkerhet og målene i denne. Tiltakene som foreslås i oversikten skal bidra til å gjøre strategien konkret og handlingsrettet, som anbefalt av Direktoratet for e-helse gjennom forstudiet.

I tiltaksoversikten foreslås nye tiltak innen digital sikkerhet, og det beskrives eksisterende og pågående tiltak innen de fem prioriterte områdene i Nasjonal strategi for digital sikkerhet. De foreslåtte tiltakene i denne utgaven er av noe mindre skala, og skal bidra til at sektoren kan oppnå de overordnede målene definert i den nasjonale strategien og svarer ut kjente utfordringer i sektoren som beskrevet blant annet i Digital sårbarhet – sikkert samfunn (Lysneutvalget), Overordnet risiko- og sårbarhetsvurdering for IKT i helse og omsorgssektoren (2019) og Riksrevisjonens vurdering av helseforetakenes forebygging av angrep mot sine IKT-systemer.

Etter at arbeidet med tiltaksoversikten er ferdigstilt vil prosjektet gå videre med å utarbeide strategien. Strategien vil i tillegg til temaene i Nasjonal strategi for digital sikkerhet behandle sektorspesifikke temaer som ble identifisert i forstudien:

- Sikker samhandling
- Sikker digital hjemmeoppfølging
- Sikkerhet i leverandørkjeden

I den videre strategiprosessen vil det vurderes større tiltak og strategiske virkemidler. Tiltak og strategiske virkemidler som identifiseres senere i strategiprosessen og som adresserer de tre sektorspesifikke temaene vil komme i oppdatert utgave av tiltaksoversikten i slutten av 2021.

Vedlegg 3A: Tiltaksoversikt til Strategi for digital sikkerhet for helse- og omsorgssektoren v0.7

Direktoratet for e-helse

Tiltaksoversikt

Til Strategi for digital sikkerhet for helse- og omsorgssektoren v0.7

ARBEIDSDOKUMENT

MERKNAD v0.7: Denne versjonen er sendt på innspillsrunde til prosjektets hovedsamarbeidspartnere. Eventuelle forslag til nye tiltak som kommer inn før behandling i Nasjonalt e-helsestyre vil tas med videre i strategiprosessen og adresseres i strategien eller oppdatert versjon av dokumentet ved utgangen av 2021. Det vil kunne forekomme endringer i formuleringer og struktur på dokumentet

Forord

På oppdrag for Helse- og omsorgsdepartementet utarbeider Direktoratet for e-helse i 2021 en Strategi for digital sikkerhet i helse- og omsorgssektoren. Denne tiltaksoversikten er en delleveranse i arbeidet med strategien, og er utarbeidet i første fase av strategiprosessen.

Strategien og tiltaksoversikten bygger videre på *Nasjonal strategi for digital sikkerhet*[1] og målene i denne. Tiltakene som foreslås i oversikten skal bidra til å gjøre strategien konkret og handlingsrettet, som anbefalt av Direktoratet for e-helse gjennom et forstudie[2] i 2020.

I tiltaksoversikten foreslås nye tiltak innen digital sikkerhet, og det beskrives eksisterende og pågående tiltak innen de fem prioriterte områdene i Nasjonal strategi for digital sikkerhet. Strategi for digital sikkerhet i helse- og omsorgssektoren vil i tillegg ta for seg tre sektorspesifikke områder: Sikker samhandling, sikker digital hjemmeoppfølging og sikkerhet i leverandørkjeden.

De foreslåtte tiltakene i denne utgaven er av noe mindre skala, og skal bidra til at sektoren kan oppnå de overordnede målene definert i den nasjonale strategien og svarer ut kjente utfordringer i sektoren som beskrevet blant annet i *Digital sårbarhet – sikkert samfunn* (Lysneutvalget), *Overordnet risiko- og sårbarhetsvurdering for IKT i helse og omsorgssektoren* (2019) og *Riksrevisjonens vurdering av helseforetakenes forebygging av angrep mot sine IKT-systemer*. I den videre strategiprosessen vil det vurderes større tiltak og strategiske virkemidler Tiltak og strategiske virkemidler som identifiseres senere i strategiprosessen og som adresserer de tre sektorspesifikke områdene vil komme i oppdatert utgave av tiltaksoversikten i slutten av 2021.

Oversikten er utarbeidet med utgangspunkt i Nasjonal strategi for digital sikkerhet og tilhørende tiltaksoversikt, samt NHNs Innspill til oppfølging av Nasjonal Strategi for Digital Sikkerhet i Helse- og omsorgstjenesten. Direktoratet for e-helses hovedsamarbeidspartnere i strategiarbeidet; Norsk Helsenett SF, **Helsedirektoratet**, Kommunesektorens organisasjon (KS), Helsetilsynet og Helse Sør-Øst på vegne av de regionale helseforetakene, har vært involvert i arbeidet gjennom jevnlige møter og en skriftlig innspillsrunde.

[1] Nasjonal strategi for digital sikkerhet

[2] Strategi for digital sikkerhet i helse- og omsorgssektoren – Vurdering av behov og innretning

Innhold

1 Innledning

Denne tiltaksoversikten understøtter *Strategi for digital sikkerhet i helse- og omsorgssektoren*, som er under utarbeidelse og ferdigstilles mot utgangen av 2021. Oversikten inkluderer eksisterende, pågående og ønskede tiltak innen digital sikkerhet i helse- og omsorgssektoren. For hvert tiltak er det pekt på hvem som er tiltaksansvarlig og hvilke virksomheter tiltaket er relevant for.

Sikkerhet er en viktig del av alle små og store digitaliseringsinitiativ. Denne oversikten inkluderer ikke tiltak der digital sikkerhet kun er en del av et større initiativ, eller tiltak som kun er relevant for enkeltvirksomheter.

1.1 Tiltaksoversiktens oppbygning

Tiltaksoversikten er inndelt etter de fem prioriterte områdene fra Nasjonal strategi for digital sikkerhet:

- Forebyggende digital sikkerhet
- Digital sikkerhet i kritiske samfunnsfunksjoner
- Kompetanse
- Avdekke og håndtere digitale angrep
- Bekjempe data- og IKT-relatert kriminalitet

Kapitlene 2.1 til 2.5 inneholder tiltak innen digital sikkerhet i helse- og omsorgssektoren for de fem områdene. For hvert tiltak er det angitt ansvarlig(e) virksomhet(er), hvem tiltaket er relevant for og en beskrivelse av tiltaket. Under hvert område beskrives innledningsvis det overordnede målet tiltakene skal understøtte, der målene er basert på Nasjonal strategi for digital sikkerhet.

Kapittel 3 inneholder en oversikt over 10 grunnleggende tiltak hver enkelt virksomhet anbefales å gjennomføre med henvisninger til relevant veiledningsmateriell. Kapittel 4.2 beskriver en analyse av i hvilken grad tiltakene i oversikten dekker opp under NSMs Grunnprinsipper for IKT-sikkerhet og delmål tilknyttet hvert av de fem områdene. Denne analysen vil benyttes videre i strategiarbeidet til å identifisere ytterligere tiltak og/eller strategiske virkemidler som vil kunne bidra til økt måloppnåelse.

1.2 Rapportering og oppfølging

Helse- og omsorgsdepartementet (HOD) har det overordnede ansvaret for oppfølging av Strategi for digital sikkerhet i helse- og omsorgssektoren etter ferdigstilling ved utgangen av 2021, og er ansvarlig for at strategiens prioriteringer og tiltaksoversikten følges opp i sektoren. HOD vil samarbeide med underlagte virksomheter og berørte aktører i sektoren slik at planlagte sikkerhetstiltak i nødvendig grad blir koordinert med andre departementer.

Det anbefales at aktører i sektoren som er ansvarlig for tiltak må årlig rapportere til HOD på status på oppfølging av iverksatte tiltak. Krav til rapportering iverksettes tidligst ett år etter godkjenning av strategi for digital sikkerhet i sektoren. Dette innebærer at ansvarlige aktører i sektoren må kartlegge hvorvidt de iverksatte tiltakene bidrar til at målformuleringene under de strategiske prioriteringene nås.

For tiltak der Helse- og omsorgsdepartementet er ansvarlig, forutsettes det at den praktiske utførelsen kan delegeres til eksempelvis Direktoratet for e-helse eller Norsk Helsenett. Det samme gjelder informasjonsinnhenting og sammenstilling av rapportering.

2 Tiltak

2.1 Forebyggende digital sikkerhet

Tiltakene skal understøtte et overordnede mål om at norske helsevirksomheter skal digitalisere på en sikker og tillitsvekkende måte, og har bedre evne egenbeskyttelse mot uønskede digitale hendelser.

Eksisterende tiltak 1.1: Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
Ansvarlig: Normens styringsgruppe
Relevant for: Hele sektoren
Beskrivelse: Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) er et omforent sett av krav til informasjonssikkerhet og personvern basert på lovverket, med tilhørende veiledningsmateriell. Normen forvaltes av en styringsgruppe sammensatt av representanter for sektoren, og skal bidra til tilfredsstillende informasjonssikkerhet og personvern i den enkelte virksomhet og i sektoren generelt. I tillegg skal Normen bidra til å etablere mekanismer og regler som sikrer at kommuner og samarbeidende virksomheter i helse- og omsorgssektoren kan ha gjensidig tillit til at behandling av helse- og personopplysninger gjennomføres på et forsvarlig sikkerhetsnivå.

Tiltak 1.2: Stille krav om etterlevelse av Normen
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Alle etater og virksomheter underlagt HOD
Beskrivelse: Alle virksomheter tilknyttet Helsenettet er gjennom medlemskapsavtalen forpliktet til å følge Normen. For å oppnå tydeligere krav til og økt etterlevelse av Normen bør Helse- og omsorgsdepartementet stille krav om at alle underliggende etater og virksomheter skal etterleve kravene i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen). Dette gjøres gjennom tildelingsbrev og foretaksprotokoller. Helse- og omsorgsdepartementet bør vurdere å peke på Normen som tilsynsgrunnlag for Helsetilsynet.

Tiltak 1.3: Videreutvikling av og opplæring gjennom Normen
Ansvarlig: Direktoratet for e-helse
Relevant for: Hele sektoren

Beskrivelse: Normens rolle som bransjenorm for sikkerhet og personvern styrkes og tydeliggjøres. Dette omfatter å være sektorens felles kravsett til informasjonssikkerhet og personvern, utgi veiledningsmateriell og andre produkter som hjelper sektoren med å etterleve Normen, samt være en arena for kompetansebygging og erfaringsutveksling innen Normens temaer. Sekretariatet for Normen i Direktoratet for e-helse har ansvar for forvaltning av Normen i henhold til styringsgruppen for Normens føringer basert på sektorens behov.

Tiltak 1.4: Stille krav til risikobasert tilnærming
Ansvarlig: Helse- og omsorgsdepartementet (HOD)
Relevant for: Alle etater og virksomheter underlagt HOD
Beskrivelse: Helse- og omsorgsdepartementet stiller krav om og ber om rapportering på at alle underliggende etater og virksomheter skal etablere en risikobasert tilnærming til utvikling, drift og forvaltning av digitale løsninger for å unngå tilsiktede og utilsiktede uønskede hendelser i nettverk og informasjonssystemer. Kravstillingen gjøres gjennom tildelingsbrev og foretaksprotokoller, og rapportering gjennom årsrapport og lignende.

Eksisterende tiltak 1.5: Bistand til sektoren gjennom Digital Beskyttelse i Dybden
Ansvarlig: Norsk Helsenett ved HelseCERT
Relevant for: Store virksomheter
Beskrivelse: HelseCERT videreutvikler tjenestene innenfor programmet Digital Beskyttelse i Dybden for å hjelpe virksomheter i sektoren med å forebygge, oppdage og håndtere sikkerhetstruende hendelser internt i virksomhetenes infrastruktur.

Tiltak 1.6: Styrke sentral og regional sikkerhetsmonitorering
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: RHF-ene og Norsk Helsenett
Beskrivelse: Helse- og omsorgsdepartementet stiller krav til sikkerhetsmonitorering i de regionale helseforetakene og Norsk Helsenett som nasjonal tjenesteleverandør, og stiller krav til RHF-ene om å etablere samarbeid med HelseCERT gjennom programmet Digital Beskyttelse i Dybden.

Tiltak 1.7: Styrket sikkerhetstesting gjennom HelseCERT
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Hele sektoren
Beskrivelse: Helse- og omsorgsdepartementet stiller tydelige krav til at HelseCERT styrker kapasiteten til å gjennomføre sikkerhetstesting i sektoren.

Tiltak 1.8: VDI-samarbeid med nasjonale sikkerhetsmyndigheter
Ansvarlig: NSM og virksomheter med installerte VDI-sensorer
Relevant for: Virksomheter med installerte VDI-sensorer
Beskrivelse: Nasjonalt cybersikkerhetssenter (NCSC) drifter og organiserer et nasjonalt sensornettverk på internett; Varslingssystem for digital infrastruktur (VDI). Dette består av sensorer utplassert hos virksomheter som ansees som en del av kritisk infrastruktur i Norge, og benyttes til å analysere metadata fra nettverkstrafikken for å avdekke mistenkelig aktivitet. HOD bør iverksette en kartlegging av VDI-sensorenes dekningsgrad i sektoren opp mot kartleggingen av kritisk infrastruktur (se tiltak 2.2).

Eksisterende tiltak 1.9: DNS-tjenester for medlemmer av Helsenett servertjeneste
Ansvarlig: Norsk Helsenett SF
Relevant for: Hele sektoren
Beskrivelse: Helsenett DNS er en tjeneste som tilbys til og bør benyttes av alle medlemmer av Helsenettet. DNS-tjenesten benytter sperrelister som kontinuerlig oppdateres for å blokkere domener som benyttes av angripere.

Tiltak 1.10: Etablere felles satsning for sikring av IOT-løsninger
Ansvarlig: Avklares
Relevant for: Virksomheter som yter helsetjenester
Beskrivelse: Det bør etableres et felles satsningsområde for å kunne utnytte og sikre fremskridende teknologi som blant annet IoT-løsninger (medisinsk utstyr, avstandsoppfølging i hjemmet m.m.) for å sikre morgendagens helsetjeneste. Det antas at slik ny teknologi vil medføre nye trusler og angrepsvektorer, som krever tilpasningsdyktighet gjennom adaptive sikkerhetstiltak. Arbeidet bør inkludere virksomheter fra primærhelsetjenesten, Normen og relevante private aktører som leverandører av velferdsteknologiløsninger.

Tiltak 1.11: Utarbeide felles IKT-sikkerhetskrav til anskaffelser av medisinsk utstyr
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Virksomheter som yter helsehjelp
Beskrivelse: Helse- og omsorgsdepartementet stiller tydelige krav til at det etableres felles minimumskrav til IKT-sikkerhet i leveranser/anskaffelser av medisinsk utstyr og tilhørende programvare. Arbeidet med å utlede kravene må involvere sikkerhets- og anskaffelsesmiljøer fra helseregionene, primærhelsetjenesten og interesseorganisasjoner.

Tiltak 1.12: Stille felles krav til IKT-teknologileverandører i helse- og omsorgssektoren
Ansvarlig: Helse- og omsorgsdepartementet

Relevant for: Hele sektoren
Beskrivelse: Helse- og omsorgsdepartementet gir i oppdrag til anskaffelsesmiljøer i helse- og omsorgssektoren om å utarbeide felles krav på sikkerhets- og personvernområdet til leverandører av IKT/teknologi til helse- og omsorgstjenesten. Kravene bør bygge på relevante omforente kravgrunnlag som Normen og NSMs Grunnprinsipper for informasjonssikkerhet.

Eksisterende tiltak 1.13: Direktoratet for e-helse som fagmyndighet for sektoren
Ansvarlig: Direktoratet for e-helse
Relevant for: Hele sektoren
Beskrivelse: Som fagmyndighet har direktoratet et hovedansvar for å tydeliggjøre rammebetingelsene for informasjonssikkerhet i digitaliseringsarbeidet i sektoren. Direktoratet er sekretariat for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, gjennomfører utrednings- og strategioppdrag innen fagområdet for Helse- og omsorgsdepartementet, og har ansvar for nasjonal e-helsemonitor med noen aktiviteter innen informasjonssikkerhet. Direktoratet vil utvikle og styrke sin fagmyndighetsrolle på området ytterligere.

Eksisterende tiltak 1.14: Årlig rapportering om trusselbildet
Ansvarlig: Norsk Helsenett SF ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: Norsk Helsenett utgir en årlig rapport som bygger videre på nasjonale sikkerhetsmyndigheters trusselrapporter, og summerer opp konkret innsikt fra det operative sikkerhetsarbeidet i helse- og omsorgssektoren. Rapporten gir anbefalinger til tiltak.

Eksisterende tiltak 1.15: Nasjonal e-helsemonitor
Ansvarlig: Direktoratet for e-helse
Relevant for: Hele sektoren
Beskrivelse: Direktoratet for e-helse skal gjennom Nasjonal e-helsemonitor følge med på IKT-utviklingen i helse- og omsorgssektoren i Norge og etablere et kunnskapsgrunnlag om bruk og effekter av IKT i sektoren. I 2018 startet Direktoratet et arbeid med å etablere indikatorer for informasjonssikkerhet i samarbeid med aktører fra helse- og omsorgssektoren med høy informasjonssikkerhetskompetanse og -erfaring. I 2019 publiserte direktoratet en undersøkelse av modenhet på informasjonssikkerhet blant RHF-ene og NHN. Det gjennomføres også innbygger- og helsepersonellundersøkelser som omfatter sikkerhetsrelaterte spørsmål som tillit til at informasjon er sikker og tilgjengelig.

Tiltak 1.16: Kartlegge sikkerhetstilstand i små virksomheter

Ansvarlig: Direktoratet for e-helse
Relevant for: Små til middels store virksomheter i helse- og omsorgstjenesten
Beskrivelse: Gjennomføre en undersøkelse blant små helsevirksomheter (fastleger, tannlegekontorer o.l.) for å avdekke modenhet og sikkerhetstilstand hos disse. Formålet med undersøkelsen er å skaffe kunnskapsgrunnlag for å si noe om hvilke behov små helsevirksomheter har for veiledning, tjenester for å oppnå et akseptabelt risikonivå og løsninger som kan understøtte de mindre virksomhetenes driftssikkerhet. Undersøkelsen kan omfatte momenter som styringssystem for informasjonssikkerhet, hvem utfører sikkerhets- og driftsoppgaver for små helsevirksomheter og vurdering av risiko.

2.2 Digital sikkerhet i kritiske samfunnsfunksjoner

Tiltakene skal understøtte det overordnede målet om at den norske helse- og omsorgssektoren, som er en kritisk samfunnsfunksjon, er understøttet av en robust og pålitelig digital infrastruktur.

Eksisterende tiltak 2.1: Videreutvikling av Helsenettet
Ansvarlig: Norsk Helsenett SF
Relevant for: Alle virksomheter tilknyttet helsenettet
Beskrivelse: Helsenettet er en lukket og sikker kommunikasjons- og samhandlingsarena for aktørene i helse- og omsorgssektoren, og en av sektorens viktigste sikkerhetsmekanismer. Helsenettet bidrar til å ivareta en sikkerhetsarkitektur, en juridisk konstruksjon som gjør deling og samhandling om helsedata på tvers av aktører mulig innenfor trygge rammer. Over Helsenettet tilbys også sikkerhetsrelaterte tjenester som HelseID (sikker autentisering), Filoverføringstjenesten (sikker delingstjeneste) og Meldingsvalidator (overvåkning av meldingsutveksling). Norsk Helsenett SF videreutvikler Helsenettet i takt med digitaliseringen i sektoren.

Eksiterende tiltak 2.2: Ferdigstille arbeid knyttet til ny sikkerhetslov
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Virksomheter underlagt HOD
Beskrivelse: Helse- og omsorgsdepartementet ferdigstiller arbeidet med Grunnleggende Nasjonale Funksjoner, og stiller krav om at alle underliggende etater og virksomheter etablerer oversikt over kritisk digital infrastruktur som er essensiell for å ivareta helsetjenesten og nasjonalt beredskapsansvar. Nasjonal Sikkerhetsmyndighets rammeverk for verdi- og skadevurdering skal ligge til grunn for arbeidet. Dokumentasjonen skal oppdateres minst en gang per år, og være tilgjengelig for departementet på forespørsel.

Tiltak 2.3: Etablere en oversikt over kritisk infrastruktur i helse- og omsorgssektoren
Ansvarlig: Helse- og omsorgsdepartementet

Relevant for: Hele sektoren
Beskrivelse: I oppfølgingen av arbeidet med Lov om nasjonal sikkerhet (Sikkerhetsloven) og kartlegging av Grunnleggende Nasjonale Funksjoner må det utarbeides en oversikt over kritisk infrastruktur i helse- og omsorgssektoren. Oversikten må holdes kontinuerlig oppdatert, og må inneholde oversikt over verdikjedene for kritisk infrastruktur. HOD må peke ut hvem som skal ha ansvar for å opprette og vedlikeholde oversikten.

Tiltak 2.4: Stille krav til leverandører av kritisk IKT-infrastruktur
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Helseforvaltningen, RHF og infrastrukturleverandører
Beskrivelse: Helse- og omsorgsdepartementet stiller krav om at IKT-leverandører som leverer kritisk infrastruktur skal arbeide systematisk med NSMs grunnprinsipper for IKT-sikkerhet, og i henhold til Normen. Kravene må dekke infrastruktur som klassifiseres som Grunnleggende Nasjonale Funksjoner, og kan utvides til også å dekke annen infrastruktur som er kritisk for å yte helsetjenester.

Tiltak 2.5: Videreutvikle høytilgjengelige løsninger for nasjonale e-helsetjenester
Ansvarlig: Norsk Helsenett SF
Relevant for: Alle virksomheter tilknyttet helsenettet
Beskrivelse: Den nasjonale infrastrukturen levert av Norsk Helsenett er vesentlig for å ivareta digital informasjonsflyt i alle helseregioner, og på tvers av primær- og spesialisthelsetjenesten. Høytilgjengelige løsninger er en forutsetning for god nasjonal helseberedskap og evnen til å levere helsetjenester i krise- og krigssituasjoner. Norsk Helsenett SF videreutvikler kritisk nasjonal e-helseinfrastruktur som redundante og høytilgjengelige løsninger.

Tiltak 2.6: Videreutvikle høytilgjengelige løsninger regionalt
Ansvarlig: RHF
Relevant for: Spesialisthelsetjenesten
Beskrivelse: IKT-driften innenfor regionene er sentralisert og levert av profesjonelle driftsleverandører. Høytilgjengelige løsninger for kritisk IKT-infrastruktur er en forutsetning for god helseberedskap og evnen til å levere helsetjenester innenfor regionene i krise og krigssituasjoner. De regionale helseforetakene videreutvikler kritisk IKT-infrastruktur som redundante og høytilgjengelige løsninger.

Tiltak 2.7: Etablere samhandlingsarena for kritisk infrastruktur
Ansvarlig: Norsk Helsenett SF og RHF-ene
Relevant for: Norsk Helsenett SF, RHF og deres IKT-leverandører

Beskrivelse: Høytilgjengelighet i kritiske tjenester er avhengig av at sikkerhet er ivaretatt gjennom hele verdikjeden fra konsument til produsent av data. Norsk Helsenett SF og helseregionene etablerer en felles samhandlingsarena for å sikre samarbeid og gjensidig forståelse av integrasjoner og avhengigheter i de digitale verdikjedene av kritisk IKT-infrastruktur som bidrar til å ivareta motstandsdyktighet og høytilgjengelighet i kritiske helseløsninger.

Tiltak 2.8: Styrke IKT-tilsyn av kritisk infrastruktur
Ansvarlig: Helsetilsynet
Relevant for: Norsk Helsenett, RHF og deres IKT-leverandører
Beskrivelse: Helsetilsynet viderefører og styrker sitt arbeid med IKT-tilsyn i helsetjenesten, og får et særlig mandat til å føre tilsyn med kritisk IKT-infrastruktur og sammenhengende digitale verdikjeder.

2.3 Kompetanse

Digital sikkerhetskompetanse er viktig for at Norge skal lykkes med digitalisering . Dette er allerede påpekt i Nasjonal strategi for digital sikkerhetskompetanse, og er av betydning for velferd og kunnskapsutvikling også i helse- og omsorgssektoren. Kompetanse innen digital sikkerhet bidrar til økt forståelse for det digitale trusselbildet, tryggere digitale løsninger og at personvernet til den enkelte ivaretas. En forutsetning for trygg bruk av IKT er tilstrekkelig digital modenhet på alle nivåer i sektoren, fra vanlige yrkesutøvere, spesialister og hos ledere innenfor særlig kritiske områder.

Tiltakene skal understøtte det overordnede målet om styrket digital sikkerhetskompetanse i tråd med behovet i helse- og omsorgssektoren.

Tiltak 3.1: Etablere et felles kompetanseprogram for helse- og omsorgssektoren
Ansvarlig: Avklares
Relevant for: Hele sektoren
Beskrivelse: Det etableres et kompetanseprogram innen digital sikkerhet i helse- og omsorgssektoren. Programmet skal utvikle og forvalte virkemidler og læringsressurser tilpasset sektorens behov. Ansvaret for opplæring ligger i hver enkelt virksomhet, men et felles kompetanseprogram gir sektoren tilgang til gode verktøy med lavere samlet ressursinnsats enn om hver enkelt virksomhet skal utvikle alt innhold selv. Tiltaket kan ses på som en videreføring av det tidligere KompIS-programmet som er gjennomført i helseforetak og kommuner. Programmet bør også utarbeide opplæringsmateriell om sikkerhetsarbeid i helse- og omsorgssektoren, rettet mot nyansatte og innleide sikkerhetsressurser uten erfaring fra sektoren Som en del av programmet bør det utføres en kartlegging av generell sikkerhetskompetanse/kultur i sektoren, sett i sammenheng med tiltak 1.16. Kartleggingen skal brukes til å tilpasse kompetanseprogrammet til ulike deler av sektorens kunnskapsbehov.

Tiltak 3.2: Stille krav om sikkerhetsopplæring
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Alle virksomheter underlagt HOD
Beskrivelse: Helse- og omsorgsdepartementet stiller krav til underliggende etater og virksomheter om minimum årlig digital sikkerhetsopplæring av alle ansatte. Dette gjøres gjennom tildelingsbrev og foretaksprotokoller. Virksomhetene er avhengig av felles ressurser for å gjennomføre tilstrekkelig opplæring, og bør benytte det tilpassede opplæringsmaterialet utarbeidet av felles kompetanseprogram (tiltak 3.1) for å tilfredsstille kravet.

Tiltak 3.3: Sikre sikkerhetsopplæring innen helsefaglige utdanninger
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Alle virksomheter som yter helsetjenester
Beskrivelse: Helse- og omsorgsdepartementet sikrer at IKT-sikkerhet kommer på agendaen i yrkesopplæringen av helsepersonell. Basiskunnskap om digital sikkerhet er viktig for å ivareta pasientsikkerheten. Tiltaket er også en del av Nasjonal strategi for digital sikkerhetskompetanse[3].

Tiltak 3.4: Etter- og videreutdanning
Ansvarlig: Helse- og omsorgsdepartementet
Relevant for: Store virksomheter
Beskrivelse: Departementet har utført et arbeid med plan og kompetansemuligheter innen sektoren i samarbeid med NTNUs Center for Cyber and Information Security (CCIS). Dette bør videreføres med en vurdering av hvordan sektoren kan øke spesialistkompetanse gjennom etter- og videreutdanning (CISO, PVO e.l.), og om det er behov for egne opplæringstilbud innen helsespesifikke sikkerhetsområder utover kurs- og utdanningstilbud som tilbys av andre aktører. MERKNAD V0.7: Prosjektet har møte med CCIS neste uke og vil oppdatere tiltaket etter dette møtet.

Eksisterende tiltak 3.5: Normkonferansen
Ansvarlig: Direktoratet for e-helse ved Normsekretariatet
Relevant for: Hele sektoren
Beskrivelse: Normsekretariatet viderefører Normkonferansen som en årlig møteplass og kompetansearena for aktører i helse- og omsorgstjenesten.

[3] Nasjonal strategi for digital sikkerhetskompetanse

Eksisterende tiltak 3.6: Nasjonalt kompetanseforum for IKT-sikkerhet i helse- og omsorgssektoren
Ansvarlig: Norsk Helsenett SF ved HelseCERT
Relevant for: Store virksomheter, helseforvaltningen
Beskrivelse: HelseCERT viderefører nasjonal kompetanseforum for digital sikkerhet. Forumet er rettet mot cybersikkerhetsdomenet, med fokus på erfaringsutveksling, kompetansespredning og diskusjon rundt framtidige løsninger og bruk av felleskomponenter.

2.4 Avdekke og håndtere digitale angrep

Tiltakene skal understøtte det overordnede målet om at helse- og omsorgssektoren har em bedre evne til å avdekke og håndtere digitale angrep.

Eksisterende tiltak 4.1: HelseCERT og Nasjonalt Beskyttelsesprogram
Ansvarlig: Norsk Helsenett ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: HelseCERT er helse- og omsorgssektorens nasjonale senter for informasjonssikkerhet. HelseCERTs oppgave er å styrke sektorens evne til å oppdage, forebygge og håndtere ondsinnede inntrengingsforsøk og andre uønskede IKT-hendelser. HelseCERT skal spre kunnskap om IKT-trusler og beskyttelsesmekanismer og kontinuerlig monitorere trafikken i Helsenettet. Gjennom Nasjonalt Beskyttelsesprogram, som er en gratis tjeneste for medlemmer av Helsenettet, utfører HelseCERT blant annet monitorering, informasjonsdeling og forebygging, bistand til hendelseshåndtering, sårbarhetsoversikt og inntrengningstesting. HelseCERT videreutvikler NBPs eksisterende sensorplattform, sårbarhetsskanning, øvrige tjenester og utvider kapasitet til sikkerhetstesting av aktører i sektoren i henhold til endringer i trusselbildet.

Tiltak 4.2: Styrke HelseCERT som et sektorvis responsmiljø
Ansvarlig: Norsk Helsenett ved HelseCERT
Relevant for: Hele sektoren
Beskrivelse: HelseCERT styrkes som et sektorvis responsmiljø som er tilgjengelig for å støtte virksomheter i både primær- og spesialisthelsetjenesten med rådgivning og koordinering ved hendelser. HelseCERT etablerer tett samarbeid med nasjonale sikkerhetsmyndigheter for å sikre rettidig og gjensidig informasjonsflyt mellom nasjonale sikkerhetsmiljøer.

Tiltak 4.3: Inkludere håndtering av IKT-sikkerhetshendelser i nasjonal helseberedskapsplan
Ansvarlig: Helse- og omsorgsdepartementet / Helsedirektoratet

Relevant for: Hele sektoren
Beskrivelse: Nasjonal helseberedskapsplan videreutvikles og styrkes på området håndtering av IKT-sikkerhetshendelser.

Tiltak 4.4: Nasjonale IKT-beredskapsøvelser innen helse- og omsorgssektoren
Ansvarlig: Helse- og omsorgsdepartementet/Helsedirektoratet
Relevant for: Hele sektoren
Beskrivelse: Helse- og omsorgsdepartementet/Helsedirektoratet legger til rette for nasjonale IKT-beredskapsøvelser med formål å trene forretningskontinuitet i de lange digitale verdikjedene i helsesektoren minimum en gang annethvert år.

Tiltak 4.5: Åpenhet og evaluering av uønskede digitale hendelser
Ansvarlig: Den enkelte virksomhet og HelseCERT
Relevant for: Hele sektoren
Beskrivelse: Ved innføringen av NIS-direktivet i norsk lov vil det være varslingsplikt ved alvorlige IKT-hendelser. Evaluering av større IKT-sikkerhetshendelser i sektoren skal gjennomføres, og erfaring skal som hovedregel deles med resten av sektoren og mot nasjonale sikkerhetsmyndigheter. HelseCERT vil være koordineringspunkt for helse- og omsorgssektoren.

Tiltak 4.6: Statistisk logganalyse
Ansvarlig: Helse Sør-Øst (HSØ), NHN (drift)
Relevant for: Helse Sør-Øst på kort sikt, andre regioner på sikt.
Beskrivelse: Gjennom helsenorge.no har pasienten enkel tilgang til sin innsynslogg, og kan se hvem som har gjort oppslag i pasientjournalen. Det har imidlertid manglet et verktøy som gjør at helseforetakene systematisk kan kontrollere alle oppslag for å avdekke urettmessige oppslag. Prosjektet skal etablere teknisk løsning og rammeverk for kontroll av oppslagslogger i elektronisk pasientjournal. Målet er å identifisere uvanlige oppslag som videre må vurderes manuelt. Løsningen vil etableres for helseforetakene i Helse Sør-Øst, og skal også kunne skaleres opp som et tilbud til andre helseregioner. Drift av løsningen er derfor lagt til Norsk Helsenett. Prosjektet skal etter planen være ferdigstilt i 2022.

Tiltak 4.7: Evaluere Logg over innsyn i journal
Ansvarlig: Avklares
Relevant for: Helse Nord, Helse Vest og Helse Sør-Øst
Beskrivelse: Pasienter ved helseforetak i Helse Nord, Helse Vest og Helse Sør-Øst har gjennom helsenorge.no digital tilgang til loggen som viser hvem som har gjort oppslag i sin

pasientjournal. Pasientmedvirkning kan være en viktig mekanisme for å avdekke potensielt urettmessige innsyn i journal, og blir enda viktigere med innføring av dokumentdeling. Dette fordrer at pasienten har kjennskap til at løsningen eksisterer og tilstrekkelig informasjon til å kunne vurdere oppslagene. Det bør utføres en evaluering av om løsningen er kjent blant pasienter, om innholdet i loggen er forståelig og om det er behov for tilpasninger for å gi økt verdi av løsningen.

2.5 Bekjempe data- og IKT-relatert kriminalitet

Det foreslås ingen spesifikke tiltak innen dette området for helse- og omsorgssektoren. Anmeldelse og rapportering til øvrige myndigheter er et viktig tiltak som den enkelte virksomhet bør vurdere ved hendelser.

3 Anbefalte tiltak for å øke virksomheters egenevne

MERKNAD V0.7: Ytterligere henvisninger vil legges til i ferdigstillingen av dokumentet. Kom gjerne med innspill til relevant veiledningsmateriell det bør henvises til.

Dette kapittelet består av 10 grunnleggende tiltak som hver enkelt virksomhet i helse- og omsorgssektoren bør gjennomføre. Anbefalingene er de samme som Del 2 av *Tiltaksoversikt til nasjonal strategi for digital sikkerhet*, og for en beskrivelse av tiltakene bør det ses til dette dokumentet. Tiltakene bygger på *NSMs Grunnprinsipper for IKT-sikkerhet*[4].

Til hvert tiltak er det videre lagt ved henvisninger til relevant veiledningsmateriell som helsevirksomheter kan støtte seg på for å implementere tiltakene. Virksomhetene bør særlig se til nåværende versjon av Normen[5], og mindre virksomheter bør starte med *Veileder for små helsevirksomheter*[6].

1. Ledelse

Digitaliseringsdirektoratets Veileder om helhetlig styring av informasjonssikkerhet
Digitaliseringsdirektoratets Veileder om Styring og kontroll
For kommunal sektor: Normens veileder Kommuneguide til Normens veiledere og faktaark
Normen kapittel 2

2. Risikostyring

Normen kapittel 3
Normens Faktaark 5 – Fastsette nivå for akseptabel risiko
Normens Faktaark 7 - Risikovurdering

3. Kartlegg verdikjeder, informasjonsverdier, utstyr og brukertilganger

[4] NSMs Grunnprinsipper for IKT-sikkerhet 2.0

[5] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren versjon 6.0

[6] Veileder for små virksomheter

Normen kapittel 3.3, 3.4, 3.5, 5.2, 5.3

Normens Faktaark 4 – Kartlegge og klassifisere systemer

4. Inkluder digital sikkerhet i virksomhetskulturen

Digitaliseringsdirektoratets veiledning til Kompetanse- og kulturutvikling innen informasjonssikkerhet

Normen kapittel 5.1

For kommunal sektor: Kompetansepakke for kommuner og fylkeskommuner (KS)

5. Leverandørkontroll

Normen kapittel 5.7

Normens Faktaark 36 – Fjernaksess mellom leverandør og virksomhet

6. Sikker konfigurasjon

Norsk Helsenetts anbefalte sikkerhetstiltak

Normen kapittel 5.4

Normens Faktaark 21 - Sikkerhetskopi

7. Kontroll på nettverk og systemkomponenter

Norsk Helsenetts anbefalte sikkerhetstiltak

Normen kapittel 5.5

Normens Faktaark 26 – Sikring av trådløs teknologi

Normens Faktaark 34 – Håndtering av lagringsmedia

8. E-post og websikkerhet

Normen kapittel 5.5

Normens Faktaark 19 – Tiltak for å hindre ondsinnet programvare

9. Tilgangskontroll

Normen kapittel 5.2

Normens Veileder tilgangsstyring

Normens Faktaark 14 - Tilgangsstyring

Normens Faktaark 47 - Autorisasjonsregister

10. Hendelsesberedskap

Nasjonal helseberedskaplan

Normen kapittel 5.8 og 5.9

Normens Faktaark 11 – Nødprosedyrer ved bortfall av IKT

NSMs Rammeverk for håndtering av IKT-hendelser

4 Vedlegg

4.1 Oversikt over tiltak i kapittel 2

1. Forebyggende digital sikkerhet

ID	Tiltak
1.1	Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
1.2	Stille krav til etterlevelse av Normen
1.3	Videreutvikling av og opplæring gjennom Normen
1.4	Stille krav til risikobasert tilnærming
1.5	Bistand til sektoren gjennom Digital Beskyttelse i Dybden
1.6	Styrke sentral og regional sikkerhetsmonitorering
1.7	Styrket sikkerhetstesting gjennom HelseCERT
1.8	VDI-samarbeid med nasjonale sikkerhetsmyndigheter
1.9	DNS-tjenester for medlemmer av Helsenett servertjeneste
1.10	Etablere felles satsning for sikring av IOT-løsninger
1.11	Utarbeide felles IKT-sikkerhetskrav til anskaffelser av medisinsk utstyr
1.12	Stille felles krav til IKT-teknologileverandører i helse- og omsorgssektoren
1.13	Direktoratet for e-helse som fagmyndighet for sektoren
1.14	Årlig rapportering om trusselbildet
1.15	Nasjonal e-helsemonitor
1.16	Kartlegge sikkerhetstilstand i små virksomheter

2. Digital sikkerhet i kritiske samfunnsfunksjoner

ID	Tiltak
2.1	Videreutvikling av Helsenettet
2.2	Ferdigstille arbeid knyttet til ny sikkerhetslov
2.3	Etablere en oversikt over kritisk infrastruktur i helse- og omsorgssektoren
2.4	Stille krav til leverandører av kritisk IKT-infrastruktur
2.5	Videreutvikle høytilgjengelige løsninger for nasjonale e-helsetjenester
2.6	Videreutvikle høytilgjengelige løsninger regionalt
2.7	Etablere samhandlingsarena for kritisk infrastruktur
2.8	Styrke IKT-tilsyn av kritisk infrastruktur

3. Kompetanse

ID	Tiltak
3.1	Etablere et felles kompetanseprogram for helse- og omsorgssektoren
3.2	Stille krav om sikkerhetsopplæring
3.3	Sikre sikkerhetsopplæring innen helsefaglige utdanninger
3.4	Etter- og videreutdanning
3.5	Normkonferansen
3.6	Nasjonalt kompetanseforum for IKT-sikkerhet i helse- og omsorgssektoren

4. Avdekke og håndtere digitale angrep

ID	Tiltak
4.1	HelseCERT og Nasjonalt Beskyttelsesprogram
4.2	Styrke HelseCERT som et sektorvis responsmiljø
4.3	Inkludere håndtering av IKT-sikkerhetshendelser i nasjonal helseberedskapsplan
4.4	Nasjonale IKT-beredskapsøvelser innen helse- og omsorgssektoren
4.5	Åpenhet og evaluering av uønskede digitale hendelser
4.6	Statistisk logganalyse
4.7	Evaluere Logg over innsyn i journal

4.2 Analyse av eksisterende og foreslåtte tiltak

MERKNAD V0.7: Prosjektet skal gjennomføre en analyse av de eksisterende og foreslåtte tiltakenes dekning opp mot NSMs grunnprinsipper og delmål innen de fem områdene. Analysen vil ta for seg hvorvidt tiltakene understøtter mindre virksomheter tilstrekkelig og dekning nasjonalt. Gap og områder som ikke dekkes tilstrekkelig vil tas med videre i prosessen og adresseres i strategiarbeidet. Analysens funn planlegges inkludert som vedlegg til tiltaksoversikten

Direktoratet for e-helse

Besøksadresse
Verkstedveien 1
0277 Oslo

Postadresse
Postboks 6737
St. Olavs plass
0130 OSLO

Til	Møte 3/21
Dato	10.06.2021
Saksnummer	19/21
Type	Drøfting

Fra	Jon Helge Andersen
Saksbehandler	Siv Ingebrigtsen

Nasjonal e-helseportefølje – status og planer

Forslag til vedtak

Nasjonalt e-helsestyre tar status for nasjonal e-helseportefølje til orientering. Nasjonalt e-helsestyre ber Direktoratet for e-helse ta med seg innspill gitt i møtet i det videre arbeidet.

Hensikt med saken

Hensikten med saken er å:

1. Orientere om status nasjonal e-helseportefølje nå og om nasjonal e-helseportefølje for 2022
2. Drøfte utvalgte utfordringer i porteføljen

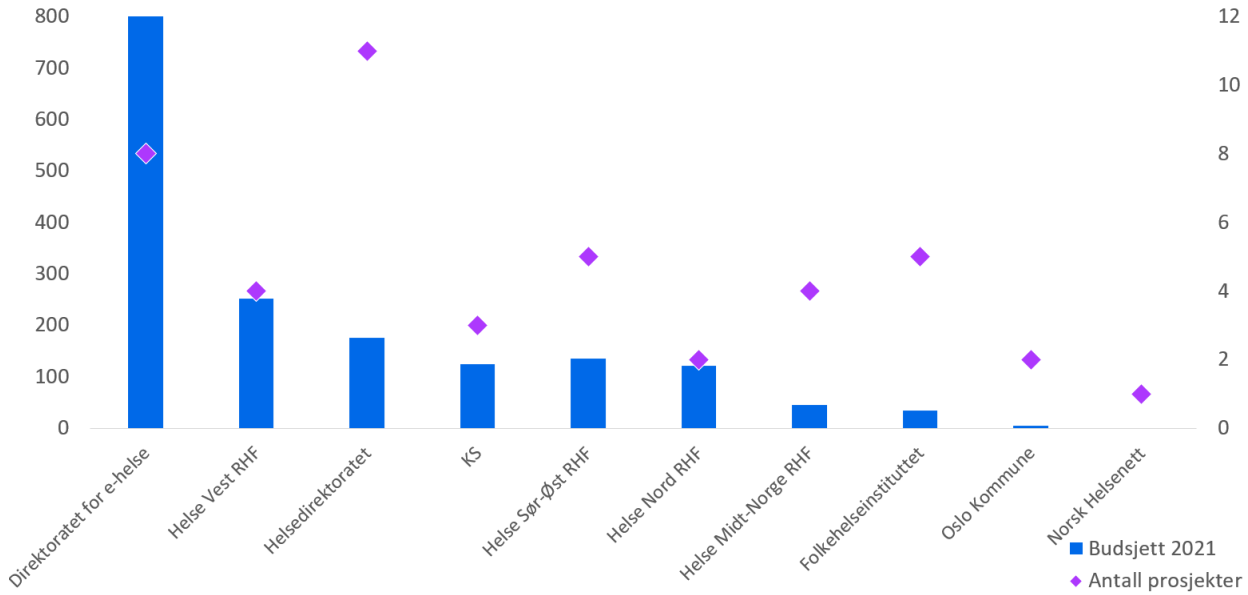
Bakgrunn

1. Nasjonal e-helseportefølje

Status nasjonal e-helseportefølje

Nasjonal e-helseportefølje består av 45 prosjekter med et budsjett på 1,72 milliarder (april 2021). Fire prosjekter er meldt ut av porteføljen, Helsedirektoratet har fullført prosjektet *Innsyn og tilgjengeliggjøring NPR og KPR,* og meldt ut prosjektene *Oppfølgingsteam og Primærhelseteam* da e-helseutviklingen er ferdigstilt. Folkehelseinstituttet har meldt ut *Nasjonal laboratorieløsning* da *NILAR* i *Helhetlig samhandling* (Direktoratet for e-helse) dekker området. Planen i veikartet følges.

Figuren nedenfor viser antall prosjekter per aktør, samt aktørenes samlede prosjektbudsjett:



Figur 1: Antall prosjekter og samlet prosjektbudsjett i 2021 (millioner kroner) per aktør

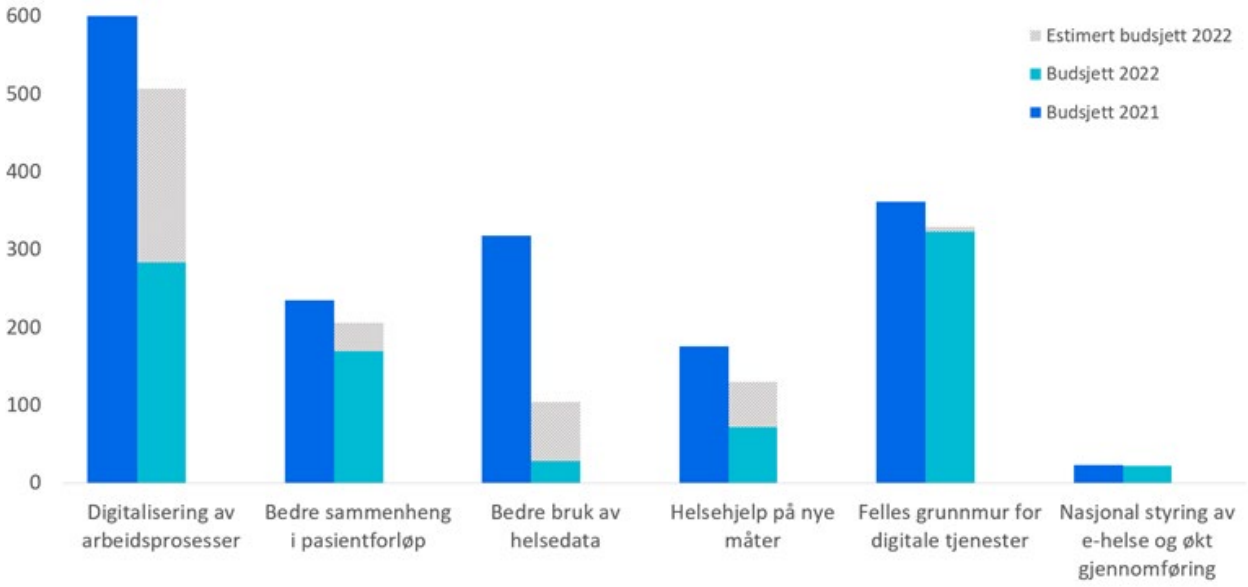
Trenden med en økende andel prosjekter som har gul status har snudd, og ved denne innmeldingen har 54% av prosjektene gul status mot 61% i januar 2021.

Nasjonal portefølje 2022

Korona-pandemien preger fortsatt behovene, motivasjonen og mulighetene innen digitalisering. I 2020 så man at digitaliseringstiltak ble prioritert og forsert for å kunne håndtere pandemien. Flere av tiltakene så man effekten av umiddelbart, og det var tydelig et digitalt taktskifte og høy endringsvilje i helse- og omsorgssektoren. På mange måter har pandemien fremskyndet digitaliseringen i helsesektoren, samtidig som pandemien har hatt forsinkende effekt på medisinske behandlinger.

Per april 2021 ser det ut til at nasjonal e-helseportefølje i 2022 vil bestå av 35 prosjekter. Dette inkluderer ett prosjektforslag hvor oppstart ikke er bekreftet. Det er 11 prosjekter som er forventet avsluttet i 2021. I tillegg til prosjektkandidaten *Legemidler fra institusjon* (Folkehelseinstituttet), er det forventet oppstart av aktiviteter innen strategiområdet "Bedre bruk av Helsedata" og "Felles grunnmur for digitale tjenester".

Innmeldt budsjett for 2022 er på rundt 897 millioner, men 16 prosjekter har så langt ikke oppgitt budsjett for det kommende året. Det kan komme endringer i planer og prioriteringer for flere av aktørene, også grunnet pandemihåndtering og resultatet av digitaliseringen som har skjedd under pandemien.



Drøfte utvalgte utfordringer i porteføljen

Det er behov for å drøfte følgende utfordringer med NUIT.

1. Forsinkelser i SAFEST og utfordringer med leveranse av virkestoffdata

Det jobbes videre med utfordringene på legemiddelområdet. Det jobbes videre med utfordringene på legemiddelområdet. En analyse av *SAFEST prosjektet i legemiddelverket* viser at det er behov for utvidelser av budsjett og gjennomføringstid, og det er ikke avklart videre løp for å håndtere dette. Ettersom prosjektets rammer må endres og det er høy risiko for manglende tilslutning til utvidelsene melder prosjektet rød status.
Forsinkelsen medfører at *SAFEST* ikke kan levere virkestoffdata som planlagt. Man ser på en midlertidig løsning for Helseplattformen som leveres fra Program Kodeverk og Terminologi. Endret omfang vil også påvirke prosjektene Program kodeverk og terminologi (PKT), Helseplattformen, HELIKS, FRESK og Klinisk legemiddelsamhandling.

2. Felles kommunal journal

I prosjektet Felles kommunal journal, tidligere Akson, er arbeidet med å planlegge, anskaffe og innføre en felles journalløsning for kommunale helse- og omsorgstjenester utenfor Midt-Norge startet. Målet er å gi personell i kommunale helse- og omsorgstjenester brukertilpassede og mer effektive løsninger for tildeling, administrasjon, ytelse og dokumentasjon av helsehjelp.

Prosjektet utforsker muligheten for en løsning basert på en åpen plattform som samler og tilgjengeliggjør all relevant pasientinformasjon via standardiserte kommunikasjonsprotokoller. Det legges til grunn et tydelig skille mellom informasjon og funksjonalitet. En felles løsning for journalføring i kommunene betyr altså ikke at alle skal bruke det samme systemet levert av én leverandør, og det er prosjektets målsetting at leverandørmarkedet skal konkurrere fritt om å levere funksjonelle løsninger som i sum dekker en kommunes behov for å ivareta krav om journalføring. KS skal nå etablere et eget selskap som skal utvikle plattformen for å realisere en felles kommunal løsning.

Prosjektet rapporterte i april rød risiko grunnet nøkkelressurser som berøres av covid-19 aktiviteter, og risiko for manglende kapasitet for allokerte ressurser til gjennomføring av prosjektet innenfor tid og med akseptabel kvalitet. Basert på gjennomgang i NUIT 30.mai vurderes status noe bedre.

3. Forprosjekt digital samhandling

I 2021 bevilget Stortinget 189 millioner kroner til å utvikle digitale samhandlingsløsninger som gjør at pasientinformasjonen kan deles sikkert og effektivt mellom aktørene i helse- og omsorgssektoren. Program digital samhandling skal ivareta arbeidet med de nasjonale løsningene for samhandling og få til god informasjonsflyt i helsetjenesten. Programmet er en utviklingsretning som gjennomføres stegvis, hvor direktoratet har fått i oppdrag å følge opp det første steget i den skisserte utviklingsretningen for perioden 2021- 2024.

Steg 1 er avgrenset til realisering av grunndata og tillitstjenester, nasjonal informasjonstjeneste for oppslag av laboratorie- og radiologisvar, samt forprosjekt og ekstern kvalitetssikring av neste steg i utviklingsretningen for helhetlig samhandling.

Dette er et sentralt program som vil påvirke digitaliseringen av hele sektoren.

4. Konseptfase for innføring av ICD-11

ICD-10 er versjonen som har vært i bruk siden 1999, og ICD-11 er nå ferdigstilt fra WHO i en internasjonal, engelskspråklig utgave. ICD-11 er oppdatert i tråd med medisinsk utvikling og tilpasset digital bruk. Et bytte fra ICD-10 til ICD-11 vil berøre hele spesialisthelsetjenesten i Norge og nasjonal helsestatistikk, og er også i bruk til innsatsstyrt finansiering og kobling til trygdeytelser. En omlegging vil være et stort og omfattende arbeid, og Direktoratet for e-helse tar sikte på å fullføre en foranalyse i 2021 for å kartlegge hovedtrekkene ved en slik innføring.

5. Drift og forvaltning

Investeringer som gjøres i Nasjonal e-helseportefølje vil som regel medføre økte drift- og forvaltningskostnader. Det er et mål at vi med nasjonal porteføljestyring skal få bedre oversikt over investeringsbeslutninger som fører til økte drift- og forvaltningskostnader i de nasjonale e-helseløsningene, samt sikre at det er samsvar og sporbarhet mellom informasjon om dette i porteføljen og tallgrunnlaget Norsk helsenett utarbeider for behandling i TBU. Dette har også fremkommet som et behov gjennom drøftinger i TBU, jf. notat av 30. april. Dette er ett av forbedringsområdene som Direktoratet for e-helse og Norsk helsenett vil jobbe med under utprøving av Porteføljestyring 2.0. Prinsipper og styringsmodell for fordeling av kostnader vil følges opp i NEHS møte i september.

6. Porteføljestyring 2.0

Direktoratet for e-helse jobber nå med utprøving av kriterier for og inndeling av segmenter for den nasjonale prosjektporteføljen i samarbeid med aktørene. Mer informasjon om Porteføljestyring 2.0 vil bli presentert i NUFA, NUIT og NEHS møter i september.

7. Innspill fra NUIT møtet 20.mai

Tilsvarende sak om status og planer for nasjonal e-helseportefølje ble drøftet i NUIT 20. mai. Representantene fra kommunal sektor etterlyste da rapportering av omstillingskostnadene for kommunene knyttet til implementering av nye e-helseløsninger. De påpekte også viktigheten av tidlig involvering i utredninger og konseptarbeid. Det ble også ytret ønske om at økonomiske forpliktelser må forankres i Nasjonalt e-helsestyre.

Vedlegg 4A – lenket opp på ehelse.no:

Nasjonal e-helseportefølje mai 2021

Til	Møte 3/21
Dato	10.06.2021
Saksnummer	20/21
Type	Drøfting

Fra	Karl Stener Vestli
Saksbehandler	Siv Ingebrigtsen

Ny nasjonal e-helsestrategi fra 2023

Forslag til vedtak

Nasjonalt e-helsestyre ber Direktoratet for e-helse ta med seg innspill mottatt i møtet i det videre arbeidet

Hensikt med saken

Direktoratet for e-helse legger frem plan for arbeidet med utvikling av ny e-helsestrategi. Denne drøftingen skal ikke dreie seg om innholdet eller mål i strategien, men prosessen knyttet til å utarbeide den og hvordan den kan/bør benyttes. Vi ønsker innspill fra Nasjonalt e-helsestyre ut fra følgende spørsmål:

- Hvilke innspill har Nasjonalt e-helsestyre til plan for arbeidet med utvikling av ny e-helsestrategi?
- Hva er det viktigste en felles nasjonal e-helsestrategi skal bidra til i årene fremover?

Bakgrunn

Nasjonal e-helsestrategi er gjennom den nasjonale styringsmodellen for e-helse etablert som en felles strategi, i samarbeid med sentrale aktører i helse- og omsorgssektoren. Strategien skal angi felles retning og mål for digitalisering i sektoren, og hvordan disse bidrar til å realisere overordnede helse- og omsorgspolitiske mål. Nasjonal e-helsestrategi skal være førende for veivalg og prioriteringer som helse- og omsorgssektoren skal ta sammen.

Eksisterende nasjonale e-helsestrategi gjelder ut 2022. Strategien må oppdateres og aktualiseres slik at den kan legges til grunn for veivalg og prioriteringer fra 2023. Mye har skjedd siden den eksisterende e-helsestrategien ble utarbeidet i 2017. Arbeidet med å få på plass en ny nasjonal e-helsestrategi er satt i gang nå. Arbeidet skal skje sammen med helse- og omsorgssektoren og gjennomføres i 2021 og 2022.

Mandat for arbeidet

Oppdraget tar utgangspunkt i gjeldende strategi, men skal sørge for at den oppdateres og aktualiseres slik at den kan legges til grunn fra 2023.

Strategien skal være kunnskapsbasert. Økt kunnskap vil settes oss i stand til å gjøre bedre prioriteringer og ha bedre forutsetninger for å ta retningsvalg. Blant områder vi må undersøke nærmere er koronapandemien og helsedata viktige stikkord. Strategien må vris mer i retning av betydning for innbyggeren, vektlegge innbyggerens behov og innbyggeren som ressurs. Kunnskap fra næringsliv og forskning bør inkluderes i kunnskapsgrunnlaget, i tillegg til at det i større grad skal ta hensyn til pågående internasjonalt arbeid og strategisk tenkning.

Strategien må støtte ønsket utviklingsretning og fremme en mer bærekraftig utvikling av helse- og omsorgssektoren. Arbeidet skal sørge for at vi både tenker helhetlig og langsiktig, og samtidig peke på gevinster på veien dit. Den bør gi bedre utgangspunkt for prioritering og tydelig kommunisere hvilke valg som skal tas for felles retning for digitaliseringsarbeidet i helse- og omsorgssektoren.

Plan for arbeidet

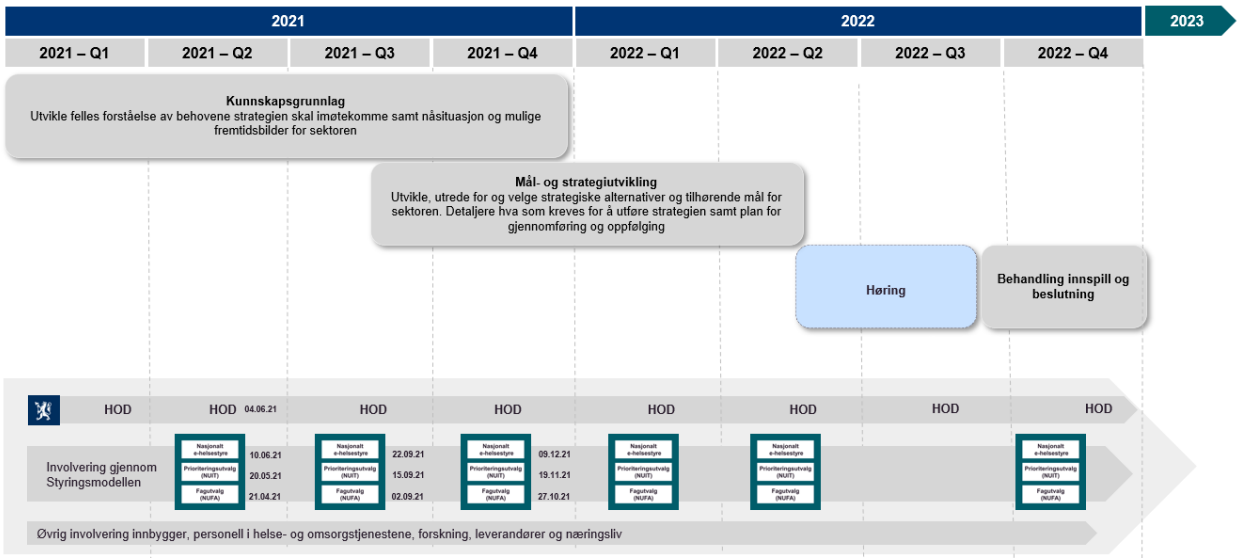
Vi legger opp til at vi i 2021 skal få på plass et oppdatert kunnskapsgrunnlag for felles forståelse av behovene strategien skal imøtekomme, nåsituasjon og mulige fremtidsbilder for sektoren.

Høsten 2021 starter vi i parallell opp arbeidet med mål- og strategiutvikling. I dette ligger at vi utvikler og tar valg om strategiske alternativer med tilhørende mål, før utkast til strategi sendes på formell høringsrunde i 2022.

Direktoratet legger opp til en prosess der helse- og omsorgssektoren, forskningsmiljø, næringsliv og innbyggere skal involveres. Som ledd i informasjonsinnhentingen nå før sommeren, gjennomfører vi i mai og juni 1:1-møter med noen NUIT-medlemmer, intervjuer med representanter for innbyggere og helsepersonell, samt en workshop hvor blant andre NUFA-medlemmer og representanter fra næringsliv og forskningsmiljø er invitert.

Vi legger opp til drøfting i NUFA, NUIT og Nasjonalt e-helsestyre i Q3 og videre tilslutning til kunnskapsgrunnlaget i Q4 i 2021. Videre har vi som plan at høringsnotat med utkast til nasjonal e-helsestrategi sendes ut på høring så tidlig som mulig i mai 2022. Høringsnotat med ny nasjonal e-helsestrategi skal i forkant av høringsrunden behandles i NUFA, NUIT og Nasjonalt e-helsestyre våren 2022.

Overordnet plan 2021-2022 for arbeidet illustreres slik:



Til	Møte 3/21
Dato	10.06.2021
Saksnummer	21/21
Type	Drøfting

Fra	Karl Stener Vestli
Saksbehandler	Mildrid Ræstad

Strategiplan for digitalisering av legemiddelområdet

Forslag til vedtak

Nasjonalt e-helsestyre drøfter saken og ber Direktoratet for e-helse ta med seg innspillene gitt i møtet i det videre arbeidet.

Hensikt med saken

Det er ønskelig å drøfte innretning på videre *prosess for forankring* av strategiplan for digitalisering av legemiddelområdet. Bakgrunn og status for arbeidet vil bli presentert som grunnlag for drøfting.

Bakgrunn

I 2021 ble ny avdeling for legemidler etablert i Direktoratet for e-helse for å styrke arbeidet på digitaliseringsdelen av legemiddelfeltet. Avdelingen er nå i gang med utarbeidelse av en strategiplan for digitalisering av legemiddelområdet. Utarbeidelsen av strategiplan er tett koblet på arbeidet med revidering av nasjonal e-helsestrategi, og inngår som underlag for pågående revidering.

Strategiplanen vil danne grunnlag for mål og prioriteringer på legemiddelområdet og bidra til realisering av helsepolitiske målsettinger. Hovedmålene i strategiplanen er utledet av de faglige målene i legemiddelmeldingen og digitaliseringsmålene i én innbygger én journal. Det pågår nå en prosess med målsettinger og tilhørende tiltak. Det er lagt opp til bred forankring og involvering fra aktører i helsesektoren. Dette gjøres dels i informasjons- og orienteringsmøter, dels i dialog- og arbeidsmøter. Direktoratet for e-helse ved avdeling legemidler er prosesseier for arbeidet, og jobber tett med Helsedirektoratet, Legemiddelverket, Folkehelseinstituttet og Norsk Helsenett (kjernegruppen). Planen baseres på sektorens samlede behov for digitalisering på legemiddelområdet og den skal bidra til å angi strategisk retning, og prioritering av planlagte og pågående e-helsetiltak av nasjonal interesse. Det vil i det videre arbeidet være den enkelte virksomhet som svarer ut hva målsettingene betyr for dem og komme med forslag til aktuelle tiltak. Deretter vil tiltakene bli foreslått en prioritering som skal benyttes i den helhetlige prioriteringen av tiltak i nasjonal e-helsestrategi/-portefølje. Strategiske og prinsipielle valg som har betydning utover ett område løftes også til nasjonal styringsmodell.

Strategiplanen vil ha flere tiltakseiere, der det er behov for godt samarbeid, deltakelse og koordinering på tvers i sektoren. Direktoratet for e-helse ved avdeling legemidler sin rolle utover å være eier for enkelt tiltak, vil være å ivareta direktoratets pådriverrolle for å:

- styrke digitalisering på legemiddelområdet for å understøtte effektiv og sammenhengende legemiddelbehandling i helse- og omsorgstjenesten.
- legge til rette for nasjonal samordning og en helhetlig og forutsigbar e-helseutvikling innenfor legemiddelområdet.