Styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

Møteinnkalling

Til

Styringsgruppen for
Norm for informasjonssikkerhet i helse- og omsorgssektoren

Møteinnkalling

Møtetidspunkt:	**Torsdag 09.03.2023 kl. 9.00-15.15**
Sted:	Digitalt på Teams

Sak	Sakstittel / kommentar / forslag til vedtak
01/23 09.00	**Godkjenning av innkalling og dagsorden** **Forslag til vedtak:** *Styringsgruppen godkjenner innkalling og dagsorden*
02/23	**Godkjenning av referat fra møte 21.11.22** **Forslag til vedtak:** *Styringsgruppen godkjenner referatet*
03/23 09.10	**Sekretariatet orienterer, inkludert status på startede prosjekter** • Veileder for leverandører • Revisjon av skyveileder • Artikkel om zero trust • «Kan jeg bruke dette her?» Artikkel med råd til små virksomheter ved kjøp og bruk av web-løsninger • Artikkel om risiko og KI • Sikkerhetsleder- og PVO-samling • Kurs og webinar 2023 • Passord og passordhåndtering • KINS-strategisamling • Normkonferansen – her ønsker vi innspill på tema og foredragsholdere • Møtekalender 2023 • mm.
09.50	**Pause**
04/23 10.10	**Drøftingssak: Strategi 2023-2025** Strategi for Normen 2023-2024 er vedlagt. Forhold i Norge og i verden for øvrig endres raskt. Strategi for Normen ble påbegynt januar 2022. Sekretariatet for Normen ønsker å løfte spørsmålet om det allerede nå er behov for å justere og prioritere momenter? Redaksjonskomiteen for Normen løfter frem to viktige momenter. Økt fokus på • beredskap og digital sikkerhet, blant annet som følge av en mer usikker verdenssituasjon

	• digital hjemmeoppfølging og pasientmedvirkning, blant annet som følge av trangere økonomiske tider og bemanningssituasjonen (Helsepersonellkommisjonen) Sekretariatet ønsker innspill på • Er det allerede nå er behov for å justere og prioritere momenter i strategien? • Hva skal i så fall tas bort eller prioriteres ned?
05/23 12.00	**Beslutningssak: Handlingsplan 2023** Den foreløpige handlingsplanen for 2023 er omfattende. Det må gjøres noen prioriteringer før Handlingsplan 2023 vedtas. Vedlagt foreløpig handlingsplan, utkast handlingsplan og prioritering gjort av Normens redaksjonskomite. Sekretariatet vil fasilitere en prioritering og drøfting av denne. Styringsgruppens medlemmer bes forberede seg på hvilke aktiviteter fra handlingsplanen de mener det er viktig å prioritere. Det vil deretter lages et endelig forslag til Handlingsplan 2023 i møtet. **Forslag til vedtak** *Styringsgruppen for Normen godkjenner Handlingsplan for Normen 2023*
Ca 11.20	**Lunsj**
06/23 12.00	**Orienteringssak: Felles Interregional Klassifiseringsmodell** Helseregionene har sammen jobbet med en felles informasjonsklassifiseringsmodell. Behovet for en felles modell har kommet frem gjennom samarbeid på tvers i forbindelse med implementeringen av Microsoft 365. Regionene har delt innhold, planer og erfaringer ettersom mye av implementeringen har likhetstrekk i alle regionene. Informasjonssikkerhet i skyen er høyaktuell og helseregionene jobber med å konkretisere og tilpasse sine informasjonssikkerhetsmodeller for å dekke de nye utfordringene som skyen bringer. Prosjektet kommer for å orientere om arbeidet og presentere sine tanker om at dette kan bli et faktaark i Normen eller lignende.
07/23 12.20	**Godkjenning: Oppstart faktaark "Integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen?»** Se underlagsdokument «7-23 Beskrivelse av prosjekt Integritet hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen» **Forslag til vedtak** *Styringsgruppen for Normen godkjenner at det settes i gang et arbeid for å utarbeide et faktaark som beskrevet i dokumentet «Beskrivelse av prosjekt «Integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen?» (dette dokumentet). Styringsgruppen for Normen sender innspill til deltakere i referansegruppen til sekretariatet.*
13.00	**Pause**

Styringsgruppen for Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

08/23 13.15	**Drøfting: Flytskjema forskning** Normens styringsgruppe vedtok i desember 2021 at det skulle utvikles en kortversjon av forskningsveilederen. Dette ble i juni 2021 endret til at det skulle utvikles et flytskjema som beskrev avgjørende steg i prosessen med å planlegge, gjennomføre og avslutte et forsknings-, utviklings-, eller kvalitetssikringsprosjekt. Arbeidet er nå i sluttfasen og et utkast til flytskjema med tilhørende veiledning ble den 10.02.2023 sendt til Datatilsynet, Helsedirektoratet, Statens legemiddelverk, de Regionale komiteene for medisinsk og helsefaglig forskning, NEM (klageinstans), Helsedata, samt Personverntjenester i Sikt (Kunnskapssektorens tjenesteleverandør). Disse aktørene er bedt om å gi en tilbakemelding på konkrete juridiske spørsmål og aktuell praksis innen deres forvaltningsområde eller knyttet til saksbehandling. Frist for å gi tilbakemelding er 1. mars. Innspill innarbeides i forkant av styringsgruppemøtet og presenteres i forbindelse med saksfremleggelse. Vedlagt i saken er flytskjema og veiledningstekst slik det er oversendt til disse instansene. Innspill fra styringsgruppa fra behandling av saken innarbeides i en endelig versjon som sendes til styringsgruppa i etterkant av møtet, med forslag om at Flytskjema til forskningsveilederen kan godkjennes via epost innen to uker. Vi ønsker at styringsgruppen gir innspill på utforming og innhold i flytskjemaet og gir oss tilbakemelding på om vi gjennom dette møter målsetningene om å gi enklere og mer tilgjengelig veiledning til bruk for prosjektledere. **Forslag til vedtak:** *Flytskjema forskning og tilhørende veiledning sendes Styringsgruppen for Normen til godkjenning på epost når innspill er innarbeidet. Frist for godkjenning er to uker.*
13.45	**Pause**
09/23 14.00	**Godkjenning: Revisjon/videreutvikling av forskningsveilederen** Se underlagsdokument «9-23 Videreutvikling av forskningsveilederen» **Forslag til vedtak** 1. *Under forutsetning av at flytskjema og tilhørende veiledning godkjennes av styringsgruppa, vedtar 1. styringsgruppa at forskningsveilederen revideres i tråd med arbeidsgruppas forslag som beskrevet i dokumentet «Revisjon/videreutvikling av forskningsveilederen» (dette dokumentet)* 2. *Styringsgruppen ønsker at samarbeidet med SIKT utforskes videre.*
10/23 14.40	**Drøftingssak: Evaluering av Mandat for styringsgruppen og Forvaltningsmodell for Normen, samt oppfølging av kartlegging**

	Nytt Mandat for styringsgruppen med tilhørende vedlegg og Forvaltningsmodell for Normen ble vedtatt i 2020. Sekretariatet vurderer at er hensiktsmessig med en evaluering i år. I dette arbeidet kan man også se om det er momenter fra kartleggingen som ble gjort i fjor som må tas med. Sekretariatet foreslår at blir tema på det fysiske møtet i juni og at sekretariatet får i oppdrag å forberede og fasilitere en workshop der styringsgruppen og sekretariatet kan jobbe med dette. Etter dette kan det konkluderes på om vi bør evaluere Mandat for styringsgruppen og Forvaltningsmodell for Normen.
11/23 15.00	**Eventuelt**
Senest 15.15	**SLUTT**

NORMEN STRATEGI 2023-2025

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten –sektorens felles krav, verktøy og arena for informasjonssikkerhet og personvern

Normen skal

- styrke og forenkle arbeidet med informasjonssikkerhet og personvern
- bidra til at virksomheter som følger Normen har egnede tekniske og organisatoriske tiltak på plass
- fremme samhandling gjennom tillit i helse- og omsorgssektoren
- fremme en balansert tilnærming til konfidensialitet, tilgjengelighet, integritet og robusthet
- bidra til å understøtte gode helsetjenester, god pasientsikkerhet, kvalitetssikring, helsepersonellets læring, godt personvern og pasientens helsetjeneste

Overordnet strategi

Normen skal opprettholde og forbedre sin relevans og sektorens tillit, gjennom å ha

- relevante og oppdaterte krav
- målrettet og oppdatert veiledning av høy faglig kvalitet
- målrettede og nyttige kompetansehevingsaktiviteter

Helse- og omsorgssektorens behov skal alltid være førende for Normen.

NORMEN STRATEGI 2023-2025

STRATEGISKE FOKUSOMRÅDER OG INITIATIVER

1 Forenkling, nyttige verktøy og kompetanseheving

- Jobbe målrettet med kompetanseheving gjennom blant annet å se veiledningsmateriell og kompetanseheving i sammenheng
- Være tilgjengelig og i tett dialog og samarbeid med sektoren og andre relevante aktører
- Normens veiledningsmateriell skal holdes oppdatert
- Utvikle og forvalte nyttige verktøy på normen.no og ha gode informative nettsider
- Legge til rette for arenaer for erfaringsdeling, samarbeid og deling av maler og vurderinger

2 Prioriterte temaområder

- Tilpasset veiledning til sektorens små virksomheter
- Sette fokus på sikkerhetskultur gjennom alle Normens virkemidler
- IKT-beredskap og hendelseshåndtering
- Være premissleverandør og gi tilpasset veiledning på anskaffelser og leverandøroppfølging
- Legge til rette for og gi veiledning til å understøtte digital samhandling, bruk av ny teknologi og arbeidsformer
- Videreutvikle veiledningsmateriell på forskning
- Følge med på og tilpasse til kommende EU-regelverk, inkludert EHDS

3 Sektorens felles kravsett til informasjonssikkerhet og personvern

- Utvikle og forvalte gode verktøy for oppfølging av etterlevelse av Normen
- Bidra til at helse – og personopplysninger behandles slik at det understøtter pasientsikkerhet og forsvarlig pasientbehandling
- Tydeliggjøre og markedsføre hva Normen er
- Samarbeid, koordinering og kobling med andre veiledningsaktører, kontrollinstanser og krav/rammeverk

Endrede forutsetninger for Normens strategi 2023-2025?

Foreløpig handlingsplan 2023:
Ferdigstille (nyutvikling eller revisjon)

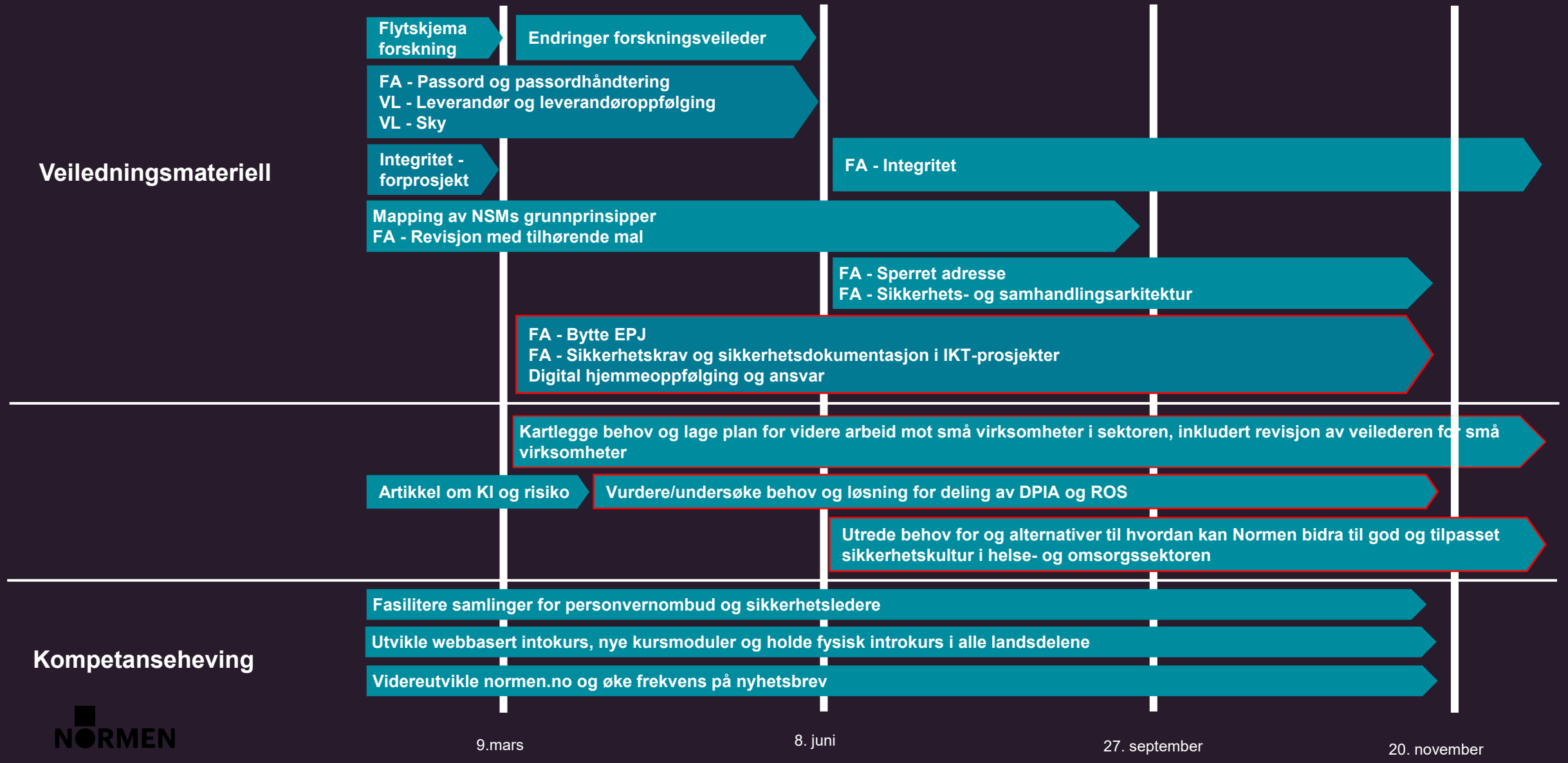
- Leverandørveileder
- Forskningsveileder
- Pasientsikkerhet/integritet/kvalitet
- Skyveilederen
- Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)
- Passord og passordhåndtering (faktaark 31)
- Sperret adresse i Folkeregisteret (faktaark 55)
- Faktaark 53 - Bytte EPJ
- Faktaark 37 - Sikkerhetskrav og sikkerhetsdokumentasjon i IKT-prosjekter
- Faktaark 6 – Revisjon
- Faktaark 20 a,b,c

Foreløpig handlingsplan 2023:
Utrede og utvikle

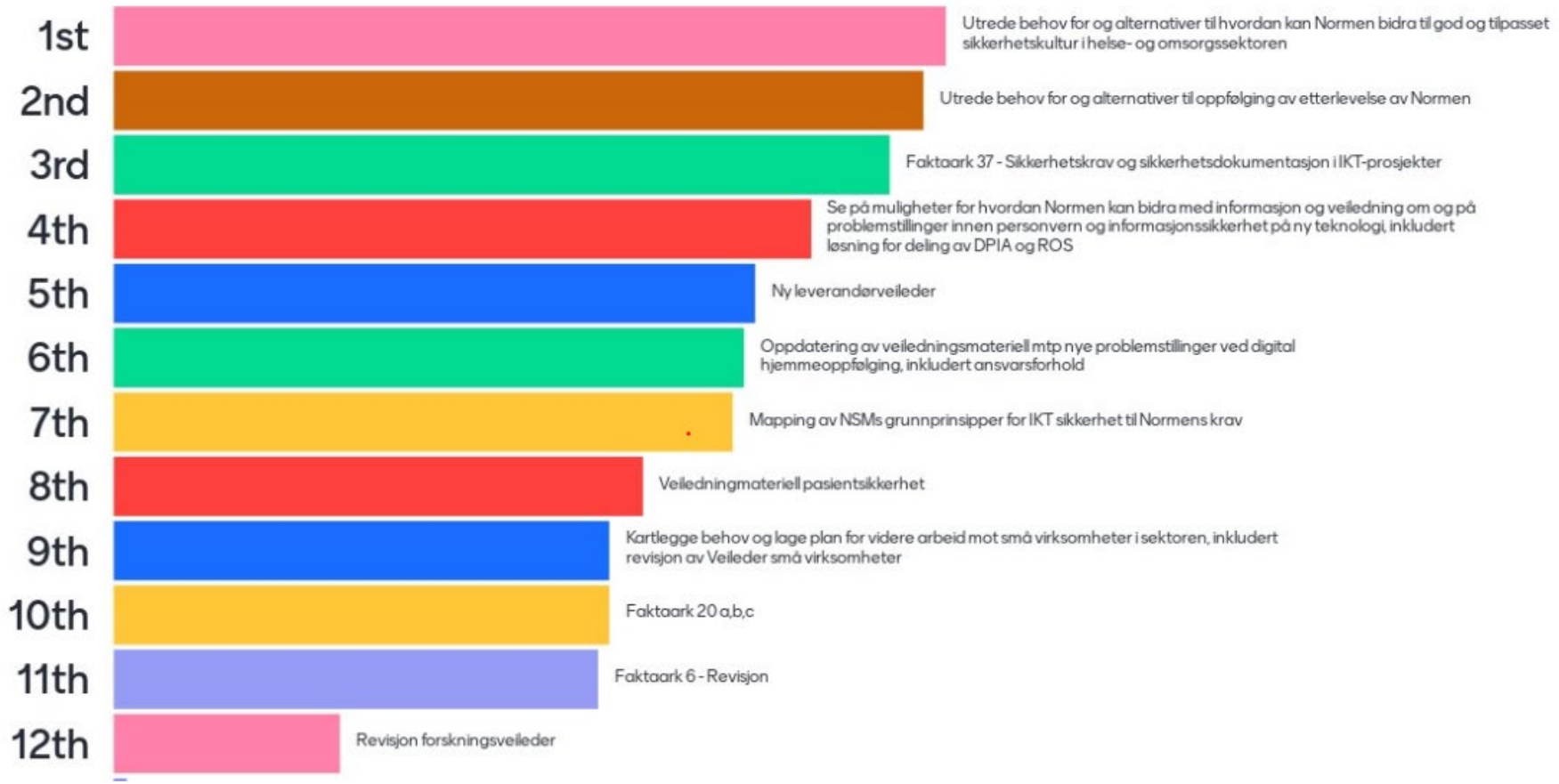
- Utrede behov for og alternativer til oppfølging av etterlevelse av Normen
- Kartlegge behov og lage plan for videre arbeid mot små virksomheter i sektoren, inkludert revisjon av Veileder små virksomheter
- Utrede behov for og alternativer til hvordan kan Normen bidra til god og tilpasset sikkerhetskultur i helse- og omsorgssektoren
- Se på muligheter for hvordan Normen kan bidra med informasjon og veiledning om og på problemstillinger innen personvern og informasjonssikkerhet på ny teknologi, inkludert løsning for deling av DPIA og ROS
- Mapping av NSMs grunnprinsipper for IKT sikkerhet til Normens krav
- Undersøke muligheten for å lage «Intro Normen» til et webbasert åpent kurs
- Oppdatering av veiledningsmateriell mtp nye problemstillinger ved digital hjemmeoppfølging, inkludert ansvarsforhold
- Avholde PVO-nettverksmøte i samarbeid med Datatilsynet

Utkast handlingsplan Normen 2023 – til vedtak etter prioritering

Sekretariatet trenger prioritering, minimum av aktivitetene med rød ramme



Redaksjonskomiteens prioritering av handlingsplan 2023



Integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen? (Faktaark)

Sekretariatet foreslo i styringsgruppemøte (SG møte) 25.11.20 å utvikle et faktaark med tema **«gode og sikre informasjonssystemer ved ytelse av helsehjelp"**. Saken ble fremmet i forbindelse med drøfting av handlingsplan for 2021.

I SG møte 2.06.2022 ble det vedtatt å etablere et forprosjekt.

Strategi for Normen slå fast at vi skal jobbe med å «Bidra til at helse – og personopplysninger behandles slik at det understøtter pasientsikkerhet og forsvarlig pasientbehandling». Temaer er prioritert inn i Handlingsplan 2023.

Hva er problemet?

Helsepersonell er helt avhengige av og prisgitt ulike IT-verktøy og systemer når man samhandler om å yte forsvarlig helsehjelp.

Det er viktig at systemene evner å formidle den informasjon helsepersonell trenger, og med den grad av nyanse og sikkerhet som anses som helsefaglig nødvendig og tilstrekkelig. Det er viktig, både for effektivitet og pasientsikkerhet, å sikre at budskapet kommer uforandret frem fra avsender til mottaker, dvs. at integriteten ivaretas.

Systemene må være tilrettelagt for god informasjonsflyt innad i virksomheter, og mellom ulike virksomheter og nivåer i helsetjenesten og gi korrekt og gyldig informasjon i brukersituasjoner i hele behandlingsforløp. Digital informasjonsbehandling skal være bidragsyter til forsvarlig helsehjelp og ikke utgjøre en fare for pasientsikkerheten.

Noen aktuelle problemstillinger:

- Informasjonssystemer som forandrer helseinformasjon for å tilpasse den til forskjellige standarder for formidling.
- Informasjonssystemer som forhindrer helsepersonell fra å formidle den informasjon med den grad av nyanser og kompleksitet som de mener er helsefaglig nødvendig.
- Informasjon som slettes fordi man ikke har metoder for å sikre at den når frem til rett person
- Helsepersonell som forhindres fra å rette feil de oppdager i informasjonen, selv når systemet understøtter versjonshåndtering slik at tidligere versjoner er tilgjengelige
- Systemer som ikke støtter versjonshåndtering, slik at tidligere versjoner slettes når det foretas rettinger
- Avveiing mellom teknologiens behov for «semantisk interoperabilitet» og helsepersonells behov for nyansert helsefaglig dialog
- Informasjonssystemer som fjerner den kontekst som er nødvendig for å tolke helseinformasjon forsvarlig
- Informasjonssystemer som hindrer helsepersonell i å dokumentere funn når de benytter nød-tilgang («blå-lys»).

- Personell med tilgang (både teknisk personell og helsepersonell) som forsøker å skjule feil ved å endre eller slette informasjon
- Tekniske forhold som kan føre til endring eller sletting av helseinformasjon
- Kopier av helseinformasjon som ikke rettes når originalen rettes (ukontrollert redundans).
- Informasjon som mangler nødvendig kontekst for helsefaglig vurdering av gyldighet, inkludert metadata

Hva vil vi oppnå?

Gjennom arbeidet skal vi bidra til at sektoren kan foreta en balansert tilnærming til konfidensialitet, integritet og tilgjengelig, slik Normen uttrykker det.

Vi ønsker å oppnå

1. Økt kunnskap og bevissthet om risiko for skade på pasient dersom IT-systemene ikke gir effektiv og uforandret formidling av informasjon i brukersituasjoner i hele behandlingsforløpet og kunnskap om aktuelle tiltak for å redusere risikoen.

2. Økt kunnskap og bevissthet om effektivitetstap og risiko for skade på pasient i digitale informasjonsbehandlingen som bidrar til:
   - Økt tillit til digital informasjonsbehandling
   - Økt helhetlig risikobasert tilnærming ved anskaffelser, innføring og bruk av IT-systemer.

3. Økt egenevne til å håndtere årsaker til uønskede hendelsene/forholdene i informasjonsbehandling som kan føre til pasientskader.

Forslag til løsning:

Utarbeide et nytt faktaark: Faktaark integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen?

Faktaarket vil omhandle faktorer som kan utgjøre en risiko for integriteten og tiltak som kan gjøres for å redusere denne risikoen. IT-systemers evne til å formidle informasjon uforandret fra helsepersonell til helsepersonell vil være sentral. I tråd med Normen ellers vil faktaarket se på alle forhold, ikke kun de tekniske. Det er viktig å synliggjøre sammenheng mellom informasjonssikkerhet, personvern og pasientsikkerhet.

Prosjektet vil primært fokusere på tekniske og organisatoriske forhold som utilsiktet vil kunne være en trussel for integriteten, inkludert forhold som hindrer helsepersonell å formidle det budskap de mener er nødvendig for å yte forsvarlig helsehjelp. Beskyttelse mot uautorisert endring eller sletting anses i mindre grad å være en utfordring ettersom eksisterende tilgangsstyring i stor grad dekker dette.

Når kopier av informasjon formidles mellom systemene, kan det også oppstå problemstillinger knyttet til kopienes gyldighet (kontrollert og ukontrollert redundans/kopiering). Det er naturlig å se dette i sammenheng med problemer knyttet til integritet. Andre problemer knyttet til gyldighet, og spesielt helsefaglige vurderinger av informasjonens gyldighet, faller utenfor rammen av dette faktaarket.

Faktaarket vil også komme inn på enkelte problemstillinger knyttet til gyldighet, avgrenset til problemer knyttet til kopier av informasjon (redundans).

Stikkord på relevant innhold i faktaarket:

- Beskrivelse av utfordringsbildet (blant annet med momentene i punktlisten innledningsvis i dette dokumentet)
- Oversikt over begreper og regelverk

Dersom det gjennom arbeidet blir identifisert behov for endringer i annet veiledningsmateriell, relevant her er risikoveilederen, eller i selve Normen, løftes det til styringsgruppa.

Det foreslås et faktaark og dette vil være førende for hvor dypt inn i enkelte problemstillinger vi vil gå. Problemstillingene som skisseres i dette dokumentet er omfattende og et viktig moment i arbeidet vil være å forsøke å jobbe frem et kortfattet og konkret veiledningsmateriell med gode eksempler.

Gjennomføring

Prosjektet gjennomføres i tråd med Normens forvaltningsmodell.

Det opprettes en ny referansegruppe med følgende kompetanse:

- Helsefaglig kompetanse og kjennskap til sektorens behov og problemer, med god forankring i helsepersonells hverdag
- Juridisk kompetanse med kjennskap til relevante deler av lov- og regelverk, inkludert EU-rett
- Teknisk kompetanse både når det gjelder teknologi generelt og standarder for informasjonsformidling spesielt.
- Kompetanse som bidrar til å beskrive ønsket resultat, angi gevinstene og hvordan realisere gevinstene

‘

Leveranse

Leveransetidspunkt er avhengig av styringsgruppens prioritering av handlingsplan 2023.

Slik situasjonen er pr i dag så innstiller sekretariatet på at referansegruppe dannes i løpet av våren og at utvikling av faktaarket starter med lav arbeidsintensitet frem til neste styringsgruppemøtet i juni og økt arbeidsintensitet etter dette.

Forslag til vedtak

Styringsgruppen for Normen godkjenner at det settes i gang et arbeid for å utarbeide et faktaark som beskrevet i dokumentet «Beskrivelse av prosjekt «Integritet – hvordan sikre at informasjonen formidles uforandret i pasientbehandlingen?» (dette dokumentet). Styringsgruppen for Normen sender innspill til deltakere i referansegruppen til sekretariatet.

Jeg skal starte nytt prosjekt

1. FORMÅL
Beskriv formålet med prosjektet

2. DATA
Kartlegg hvilke data prosjektet trenger for å oppnå formålet

3. PERSONOPPLYSNINGER?
Vurder om prosjektdataene er å anse som personopplysninger,
og i så fall hvilken type

4. ROLLER OG ANSVAR
Avklar hvem som bestemmer og har ansvar for databehandlingen i prosjektet.
Hvilke institusjon(er) avgjør hvorfor og hvordan personopplysninger behandles?

5. TYPE PROSJEKT OG BEHANDLINGSGRUNNLAG
Basert på formålet, kartlegg hvilken type prosjekt du/dere etablerer.
Finn deretter ut hva som gir prosjektet lov (rettslig grunnlag) til å behandle personopplysninger.

6. DATAFLYT OG SIKKERHET
Beskriv dataflyt og sett inn sikkerhetstiltak.

7. DELE DATA?
Avklar om prosjektet skal dele data med andre, underveis eller etterpå.
Hvis ja, avklar om mottaker trenger personopplysninger.
Hvis ja, avklar hva som er formålet med delingen og hva er mottakers rolle?

8. VARIGHET. HVA SKJER MED PERSONOPPLYSNINGENE ETTERPÅ?
Anslå hvor lenge prosjektet trenger å behandle personopplysninger for å oppnå formålet.
Avklar hva dere skal gjøre med personopplysningene i datamaterialet når prosjektet er avsluttet.
Avklar om publikasjoner fra prosjektet vil være anonyme eller inneholde personopplysninger.

9. INFORMASJON TIL DEN REGISTRERTE
De registrerte har rett til informasjon. Utarbeid informasjon til de registrerte.
Eller dokumenter at vilkår for unntak er tilstede.

10. REGISTRERTES RETTIGHETER
De registrerte har rett til innsyn (kopi), retting og sletting, og rett til å trekke samtykket, eller reservasjon.
Organiser prosjektet slik at de registrerte kan utøve sine rettigheter.

11. PERSONVERNKONSEKVENSVURDERING (DPIA)
Vurder om den planlagte behandlingen av personopplysninger medfører høy risiko for den registrerte.
Hvis ja, gjennomfør DPIA.

12. TILLATELSER
Søk nødvendige tillatelser.

13. AVTALER
Etabler nødvendige avtaler

14. DOKUMENTASJON
Sørg for at din institusjon protokollfører prosjektet og arkiverer dokumentasjon på at behandlingen av personopplysninger er lovlig.

15. KLART FOR DATAINNSAMLING

Nå kan data-innsamlingen starte

Revisjon/videreutvikling av forskningsveilederen

1. **Endringer i forskningsveilederen**

I forbindelse med utforming av flytskjema til forskningsveilederen, har arbeidsgruppen notert seg en del forbedringspunkter og korrigeringer som vi mener er nødvendige å foreta. I tillegg foreslår arbeidsgruppa at forskningsveilederen omstruktureres slik at den følger samme kronologi som flytskjemaet/gangen i et prosjekt. Dette samsvarer også i stor grad med oppbygningen av personvernregelverket.

Siden veilederen først og fremst er rettet til forskere, er det viktig at det er enkelt for dem å lese og finne fram til det de trenger. Forskerne leser gjerne veilederen for å finne ut konkret hva de må gjøre og tenke på i et prosjekt, helst i kronologisk rekkefølge. Veilederen kunne med fordel "rendyrkes" enda mer mot dette i formen/oppsettet.

Arbeidet kan gjennomføres av eksisterende arbeidsgruppe og vil ikke være for omfattende.

Strukturelle grep:

- Når flytskjemaet er ferdig, bruke det som disposisjon for veilederen.
- Flytte enkelte passasjer slik at de kommer på relevant sted og man reduserer behovet for gjentakelser. Dette gjelder blant annet de begrepene som ligger i en egen del om begreper og definisjoner.
- Avgrense innholdet til det som er strengt tatt nødvendig for prosjektleder å kjenne til. Det som ligger til virksomhetens ansvar bør tas ut.
- Anonymisering bør imidlertid nevnes flere steder, da det også vil kunne være relevant i oppstarten av et prosjekt.

Nytt innhold/forbedringer:

- Vurdere å endre tittel på veilederen slik at den også dekker kvalitetssikring, f.eks. slik: "Veileder i personvern og informasjonssikkerhet i forskning og kvalitetssikring i helsesektoren"
- Oversikt over Relevante regelverk (1.4.1) bør også nevne Forskrift om befolkningsbaserte helseundersøkelser og Bioteknologiloven, muligens også Forskningsetikkloven.
- Biobankloven heter nå Behandlingsbiobankloven og er kanskje ikke så relevant (i så fall bare hvis biomateriale skal utleveres til forskning/kvalitetssikring)?
- Veilederen kan utdypes noe når det gjelder behandlingsgrunnlag. Det kan være oversiktlig med eget underkapittel om allmennhetens interesse (GDPR art. 6 nr. 1 e) og relevante unntak i GDPR art. 9 nr. 2 (g, h, i, j), der de supplerende grunnlagene kommer med, og forklare mer om hva nødvendige garantier kan være. Art. 9 nr. 2 e) bør kanskje også nevnes kort. Samt få med at Forskrift om befolkningsbaserte helseundersøkelser kan utgjøre supplerende rettsgrunnlag for behandling av personopplysninger i den type undersøkelser.

Språklige forbedringer:

- Gjøre om til punktlister i stedet for fulltekst der det er hensiktsmessig
- Omskrive for å unngå gjentagelser av lange ord/begreper i samme avsnitt (eks. "helse- og personopplysninger", "behandling av personopplysninger", navn på lover)
- Legge lovhenvisninger i fotnoter, i stedet for inne i teksten

2. Samarbeid med Sikt – Kunnskapssektorens tjenesteleverandør

Arbeidsgruppa har siden november bestått av Inger Anne Tøndel (sekretariatet), Ane Hessen Hjelle (seksjon juridisk, Ehelse), Inga Brautaset (Sikt – Kunnskapssektorens tjenesteleverandør), samt Marie S. Schildmann (sekretariatet). Bidraget fra Sikt har vært betydelig både med tanke på faglig kompetanse og ressursbruk. Vi ser at dette samarbeidet er svært nyttig og at både Normen og Sikt som viktige veiledningsaktører til forskningssektoren vil være godt tjent med et videre samarbeid. Vi har også startet en dialog med KiNS om et tilsvarende samarbeid.

Forskernes tilbakemeldinger til oss som veiledningsaktører handler i stor grad om at de ønsker et bedre samarbeid oss imellom, og at vi kan veilede med utgangspunkt i et felles veiledningsmateriell. Vi ser også at vi med enkle grep kan gjøre forskningsveilederen relevant for forskere uavhengig av fagfelt og sektor. Det er ønskelig at Normens forskningsveileder kan være utgangspunktet for både Sikt, KiNS og vår egen veiledning.

Både Sikt og Normen ønsker å imøtekomme behovet som forskerne har. Det vil være hensiktsmessig for et videre samarbeid å avtalefeste bidrag inn i en arbeidsgruppe som kontinuerlig sørger for et kunnskapsgrunnlag for å holde forskningsveilederen oppdatert og relevant. Sekretariatet ønsker å jobbe videre med å få på plass en slik avtale.

Forslag til beslutning

1. *Under forutsetning av at flytskjema og tilhørende veiledning godkjennes av styringsgruppa, vedtar 1. styringsgruppa at forskningsveilederen revideres i tråd med arbeidsgruppas forslag som beskrevet i dokumentet «Revisjon/videreutvikling av forskningsveilederen» (dette dokumentet)*

2. *Styringsgruppen ønsker at samarbeidet med SIKT utforskes videre.*

Veiledende mal – vedlegg til flytskjema

Denne malen gir veiledning om hvordan du kan gjennomføre prosjekter innen forskning/kvalitetssikring for å oppfylle lovpålagte krav til personvern og informasjonssikkerhet. Den er ment som et supplement til Normens forskningsveileder.

Vi minner om at du må følge retningslinjer ved din institusjon. Mange institusjoner har et meldeskjema du må fylle ut og en forskningsavdeling du kan rådføre deg med. Tilhører du en institusjon som bruker Sikt personverntjenester, skal du sende meldeskjema til Sikt. Du får da råd og veiledning tilpasset ditt prosjekt om alt i malen her, og institusjonen din får dokumentasjon om prosjektet. Uansett rutiner ved din institusjon, vil malen her fungere som støtte og veiledning.

Når du bruker malen i prosjektet ditt, anbefaler vi at du er grundig i beskrivelse og vurdering i hvert punkt. Dette for å unngå følgefeil i de neste stegene, og risiko for ulovlig behandling av personopplysninger. Husk at du må gå igjennom alle stegene før du starter behandlingen av personopplysninger. Vær også oppmerksom på at institusjonen din har en 72 timers frist ved eventuelle avvik ved behandling av personopplysninger. Derfor er det viktig at du sier ifra til institusjonen din så snart som mulig hvis du oppdager det kan foreligge slike avvik, også i planleggingsfasen, hvis du f.eks. har startet behandling av personopplysninger og hoppet over et av stegene.

1. FORMÅL

Beskriv formålet med prosjektet

Beskriv og vurder formålet:

- Forklar problemstilling og sentrale forskningsspørsmål du vil undersøke i prosjektet.

Husk:

- Formålet må være **klart definert, nøyaktig, fullstendig og rimelig** (for en forskningsinstitusjon)
- Formålet må beskrives **så spesifikt som mulig**.

Tips:

- Vær grundig med formålsbeskrivelsen. Den er førende for alle vurderingene du skal gjøre under.
- Formålet avgjør hvordan og hvilke personopplysninger prosjektet kan behandle. Manglende samsvar kan føre til ulovlig behandling.
- Det kan være vanskelig å endre/utvide formål senere, særlig hvis det er vanskelig å nå dem du forsker på og behandler personopplysninger om (**de registrerte**).

- ♦ Formålet kan beskrives bredere/mer overordnet i større studier og registre der data skal brukes i flere delprosjekter med ulike problemstillinger. Men "forskning" er for vidt, formålet må avgrenses til et forskningsområde.

2. DATA

Kartlegg hvilke data prosjektet trenger for å oppnå formålet.

Beskriv og vurder datamaterialet du vil samle inn:

- ➢ **Utvalgskriterier**. Hvilke kategorier av personer skal prosjektet ha opplysninger om?
- ➢ **Sårbare personer**? Kan noen i utvalget ha vansker med å ivareta rettighetene sine, pga. sykdom, livssituasjon, skjev maktrelasjon til deg/institusjon el.? F.eks. barn, pasienter, asylsøkere, ansatte.
- ➢ **Datakilder**. Hvor og hvordan innhenter prosjektet opplysninger?
  - fra den registrerte selv: gjennom intervju, spørreskjema, notater, observasjon etc.
  - og/eller fra andre kilder: journal, helseregister, SSB, institusjon, annet forskningsprosjekt, medisinsk utstyr, etc.
- ➢ **Dataomfang.** Beskriv ca. antall personer, antall og detaljgrad på variabler, hvor ofte opplysninger skal innhentes, og om data fra ulike kilder skal kobles på personnivå.

Husk:

- ➢ **Dataminimering**: prosjektet kan kun samle inn opplysninger som er adekvate og relevante for formålet.
- ➢ Hvis du henter data fra andre kilder enn direkte fra den registrerte må:
  - den som utleverer ha rettslig grunnlag (personvernforordningen og norsk lov)
  - og utleveringen må følge regler om taushetsplikt (samtykke, dispensasjon eller lovhjemmel)
- ➢ Hvis prosjektet skal bruke/utvikle innovativ teknologi, eller hente data fra tekniske løsninger, medisinsk utstyr el. bør du rådføre deg med ressurser ved din institusjon (IT, jurister, medisinskteknisk personell) for å avklare om – og på hvilken måte - prosjektet er teknisk/juridisk mulig å gjennomføre.

3. PERSONOPPLYSNINGER?

Vurder om prosjektdataene er å anse som personopplysninger, og i så fall hvilken type.

Vurder:

- Tenk på alle data som skal brukes i prosjektet fra start til slutt, uavhengig av format. Og les definisjonene under.
- Skal prosjektet behandle personopplysninger?
- Hvis nei, trenger du ikke gå videre. Men søk REK hvis prosjektet innebærer helseforskning på mennesker, selv om kun anonyme opplysninger.
- Hvis ja, vurder om prosjektet skal behandle:
  - særlige kategorier personopplysninger
  - personopplysninger om straffedommer eller lovovertredelser
  - og/eller taushetsbelagte personopplysninger

Husk:

- **Personopplysninger** behandles hvis det på noen måte være mulig å knytte dataene til en enkeltperson, f.eks. via:
  - navn, fødselsnummer, adresse, telefonnummer, epost, samtykkeerklæring osv.
  - bakgrunnsinformasjon som tid, sted, institusjon, alder, kjønn, stilling, diagnose osv.
  - kode som viser til en koblingsnøkkel hos deg eller andre (f.eks. liste med prosjekt-ID og navn, eller pasientnummer og fødselsnummer)
  - bilde, video, lydopptak
  - IP-adresse, nettidentifikator
  - lokasjonsdata, bevegelses-/adferdsmønstre
  - biometri (f.eks. iris, fingeravtrykk, ansikt, ganglag)
  - humant biologisk materiale eller genetiske analyser (av arvestoff)
- **Særlige kategorier personopplysninger** er data om rasemessig/etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning, fagforeningsmedlemskap, genetikk, biometri, helseforhold og/eller seksuelle forhold/orientering. Begrepet "helseforhold" tolkes vidt.
- **Personopplysninger om straffedommer/lovovertredelser** er data om at en person er mistenkt, siktet, tiltalt eller dømt for straffbar handling.
- **Taushetsbelagte personopplysninger** er data om personer fra kilder som har lovpålagt eller avtalefestet taushetsplikt om opplysningene.

4. ROLLER OG ANSVAR

Avklar hvem som bestemmer og har ansvar for databehandlingen i prosjektet.
Hvilke institusjon(er) avgjør hvorfor og hvordan personopplysninger behandles?

Vurder:

- Er din institusjon:
  - **Dataansvarlig alene** – bestemmer formål og midler alene (evt. samarbeidspartnere har liten/ingen innflytelse)
  - **Felles dataansvarlig –** bestemmer formål og midler (helt eller delvis) sammen med en eller flere andre institusjoner
  - **Databehandler –** bestemmer ikke/lite over formål og midler, men behandler personopplysninger på instruksjon fra andre

Husk:

- Det er institusjonen, ikke den enkelte forsker, som bestemmer over databehandlingen og hvilken rolle institusjonen har.
- Hvis rollen til din institusjon er uklar, kontakt ressurser ved din institusjon i god tid før oppstart av datainnsamling.
- Roller og ansvar må kartlegges for å finne ut hva din institusjon må sikre/dokumentere, og hvilke avtaler dere må ha med evt. samarbeidspartnere.
- Ved felles behandlingsansvar: ta en felles gjennomgang av flytskjemaet og dokumenter stegene sammen.

5. TYPE PROSJEKT OG BEHANDLINGSGRUNNLAG

Basert på formålet, kartlegg hvilken type prosjekt du/dere etablerer.
Finn deretter ut hva som gir prosjektet lov (rettslig grunnlag) til å behandle personopplysninger.

Kartlegging av **prosjekttype** er nødvendig for å finne ut **hvilke lover** prosjektet må følge, og **hvilke tillatelser** man må ha før oppstart.
All behandling av personopplysninger reguleres av EUs personvernforordning og den norske personopplysningsloven. For noen formål (type prosjekt) vil helselover gjelde i tillegg. Hver behandling av personopplysninger må ha rettslig grunnlag, og oppfylle vilkår i aktuelle lover og forskrifter, for å være lovlig.

Vurder:

- Definer først prosjekttype ut fra formålet. Og velg deretter det rettslige grunnlaget som passer for ditt prosjekt.
- Bruk tabellen under, som viser de vanligste rettsgrunnlagene i forskning og kvalitetssikring.
- Vær oppmerksom på at prosjektet må følge vilkårene i det rettslige grunnlaget, og lovene som gir det rettslige grunnlaget.
- Du bør beskrive og dokumentere konkret hvordan prosjektet oppfyller vilkårene, og hvorfor du mener det aktuelle rettslige grunnlaget skal brukes.

Type prosjekt	**Rettslig grunnlag personvernforordningen (GDPR)**	**Aktuelle nasjonale rettslige grunnlag**
Helseforskning Forskning på mennesker, helseopplysninger eller humant biologisk materiale der formålet er å fremskaffe ny kunnskap om helse og sykdom.	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekkes tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*
	Alle disse kriteriene må være oppfylt... ✓ *Er nødvendig for forskning* ✓ *Gjør tiltak som ivaretar registrerte rettigheter og friheter* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 e) og art. 9 nr. 2 j) Merk: Forskningsetisk godkjenning fra REK etter er nødvendig, men ikke tilstrekkelig. Slik REK-godkjenning er et krav etter helseforskningsloven og	...og et av disse kriteriene må være oppfylt: ❑ *Nødvendig for forskning + tiltak for å ivareta registrerte + rådført PVO* - Personopplysningsloven §§ 8 og 9 ❑ *REK dispensasjon fa taushetsplikt* – Helsepersonelloven § 29 ❑ *Helsedataservice og REK dispensasjon fa taushetsplikt* - Helseregisterloven § 19 e) ❑ *REK-vedtak om viderebehandling* - Helseforskningsloven § 15

	et tiltak for å ivareta registrerte, men gir ikke i seg selv et rettslig grunnlag for behandling av personopplysninger.	
Annen forskning Forskning der formålet ikke er å fremskaffe ny kunnskap om helse og sykdom. (f.eks. helsetjenesteforskning)	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekkes tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*
	Alle disse kriteriene må være oppfylt.... ✓ *Er nødvendig for forskning* ✓ *Gjør tiltak som ivaretar registrerte rettigheter og friheter* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 e) og art. 9 nr. 2 j)	...og et av disse kriteriene må være oppfylt: ❑ *Nødvendig for forskning + tiltak for å ivareta registrerte + rådført PVO* - Personopplysningsloven §§ 8 og 9 ❑ *REK dispensasjon fa taushetsplikt* – Helsepersonelloven § 29 ❑ *Helsedataservice og REK dispensasjon fra taushetsplikten* - Helseregisterloven § 19 e)
Kvalitetssikring på tvers av virksomheter Formålet er å kontrollere og sammenligne kvaliteten av diagnostikk, behandling og annen helsehjelp gir forventede resultater og oppfyller kvalitetskrav: - på tvers av virksomheter - og/eller ved innhenting av opplysninger fra helseregistre.	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekkes tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*
	Alle disse kriteriene må være oppfylt.... ✓ *Rettslig forpliktelse* ✓ *Nødvendig for å yte/forvalte helse-/sosialtjenester* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 c), jf. nr. 3 og art. 9 nr. 2 h), jf. nr. 3	...og et av disse kriteriene må være oppfylt: ❑ *Helsedirektoratet dispensasjon fa taushetsplikt* – Helsepersonelloven § 29 ❑ *Helsedirektoratet dispensasjon fra taushetsplikten* - Helseregisterloven § 19 e)
Intern kvalitetssikring Formålet er å kontrollere at diagnostikk, behandling og annen helsehjelp gir forventede resultater og oppfyller kvalitetskrav: - innenfor en virksomhet	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekkes tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*

- eller flere virksomheter med felles journalsystem. Gjelder kun prosjekter med journaldata fra egen virksomhet, ikke hvis data hentes fra andre institusjoner eller helseregistre.	Alle disse kriteriene må være oppfylt.... ✓ *Rettslig forpliktelse* ✓ *Nødvendig for å yte/forvalte helse-/sosialtjenester* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 c), jf. nr. 3 og art. 9 nr. 2 h), jf. nr. 3	.. og alle disse kriteriene må være oppfylt: ✓ *Plikt til å kvalitetssikre helsetjenesten* ▫ Spesialisthelsetjenesteloven §§ 2-1 a) fjerde ledd og 3-4 a) ▫ ELLER Helse- og omsorgs-tjenesteloven § 4-2 ✓ *Nødvendig for kvalitetssikring av helsehjelp* - Pasientjournalloven § 6 ✓ *Virksomhetens ledelse bestemmer at helseopplysninger kan behandles til kvalitetssikringsformål* - Helsepersonelloven § 26
Opprette medisinsk kvalitetsregister Formålet er å løpende dokumentere resultater fra helsehjelp for en avgrenset pasientgruppe med utgangspunkt i individuelle behandlingsforløp i et medisinsk kvalitetsregister.	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekkes tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*
	Alle disse kriteriene må være oppfylt.... ✓ *Er nødvendig for forskning* ✓ *Gjør tiltak som ivaretar registrerte rettigheter og friheter* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 e) og art. 9 nr. 2 j)	...og dette kriteriet må være oppfylt: ✓ Prosjektet følger Forskrift om medisinske kvalitetsregistre, og ▫ *den registrerte samtykker (*§ 3-1*)* ▫ *ELLER den registrerte har reservasjonsrett (*§ 3-2)
Etablere befolkningsbasert helseundersøkelse Det skal samles inn helseopplysninger og evt. humant biologisk materiale fra en hel befolkning/ befolkningsgruppe /et representativt utvalg, etter samtykke fra den enkelte deltaker. Formålet er videre bruk til analyser og forskning som kan gi kunnskap om befolkningens helse.	*Den registrerte samtykker* ✓ *spesifikt,* informert, *frivillig, aktivt og utvetydig* ✓ *Samtykket må dokumenteres og kan trekke samtykke tilbake* Art 6 nr. 1 a) og art. 9 nr. 2 a)	*(ikke krav om hjemmel i norsk lov)*
	Alle disse kriteriene må være oppfylt.... ✓ *Er nødvendig for forskning* ✓ *Gjør tiltak som ivaretar registrertes rettigheter og friheter* ✓ *Har hjemmel i norsk lov* Art. 6 nr. 1 e) og art. 9 nr. 2 j)	… og et av disse kriteriene må være oppfylt: ❑ Prosjektet følger Forskrift om befolkningsbaserte helseundersøkelser ❑ *Nødvendig for forskning + tiltak for å ivareta registrerte + rådført PVO* - Personopplysningsloven §§ 8 og 9

Husk:

- Merk at et samtykke fra den registrerte kan ha ulike funksjoner. Samtykke kan:

- være rettslig grunnlag for behandling av personopplysninger (som vist i tabellen over)
- være et tiltak som ivaretar den registrertes rettigheter og friheter (når rettslig grunnlag er allmennhetens interesse, jf. tabellen over)
- oppheve taushetsplikt (for opplysninger prosjektet henter fra datakilder med taushetsplikt)

➢ Hvis barn skal delta, må du vurdere hvem som kan samtykke for barnet. Hovedregelen er at foreldre (med foreldreansvar) må gi samtykke frem til barnet er 18 år. I helseforskning og helseregistre er hovedregelen at ungdom kan samtykke selv fra 16 år. I annen forskning, rådfør deg med din institusjon. Som hovedregel er det tilstrekkelig med samtykke fra en forelder, men for forskning som innebærer høy risiko for barnet, bør begge foreldre samtykke.

➢ Hvis voksne uten samtykkekompetanse skal delta, rådfør deg med din institusjon om hvordan prosjektet kan gjennomføres på lovlig måte.

Tips:

♦ Hvis du er usikker på type prosjekt, rådfør deg med din institusjon i god tid før datainnsamling.

♦ Hvis du er usikker på om prosjektet er helseforskning, kan du sende fremleggelsesvurdering til REK og få svar ila. kort tid.

♦ Det kan være vanskelig å skille større helseforskningsprosjekt fra befolkningsbasert helseundersøkelse. Rådfør deg med din institusjon eller REK.

♦ Resultater fra intern kvalitetssikring kan publiseres anonymt (se boks 8).

♦ Hvis du skal forske på, utvikle produkter eller ta i bruk utstyr som er basert på kunstig intelligens innenfor helse anbefales det å ta i bruk Helsedirektoratets «startpakke» om Kunstig intelligens i helsetjenesten.

6. DATAFLYT OG SIKKERHET

Beskriv dataflyt og sett inn sikkerhetstiltak.

Beskriv og vurder:

- Lag en konkret plan for hvordan prosjektet skal samle inn, analysere, koble, lagre, dele og sikre data. Illustrer gjerne i et flytskjema.
- Få med følgende i beskrivelse av dataflyt:
  - alle datakilder
  - alle enheter og kanaler dataene skal innom
  - om/hvordan data om enkeltpersoner fra ulike datakilder kobles
  - om personopplysninger lagres sammen med eller adskilt fra datasettet
  - hvor eventuell koblingsnøkkel lagres
  - hvem som får tilgang til personopplysninger (institusjon og rolle)
  - hvilke opplysninger de ulike mottakerne skal ha tilgang til og til hvilket tidspunkt
  - hvorfor de får tilgang
  - om publikasjoner vil inneholde anonyme eller personidentifiserende data
  - hvordan prosjektet avslutter behandlingen av personopplysninger (sletting, anonymisering eller viderebehandling).
- Beskriv og vurder sikkerhetstiltakene:
  - vurderes for hver enhet og kanal som dataene flyter gjennom
  - kan være tekniske og/eller organisatoriske
  - skal være egnet til å sikre dataene mot uautorisert deling, endring og sletting
  - må være bedre jo høyere personvernrisikoen er (se boks 11)

Husk:

- Du må følge lagringsguide og retningslinjer for informasjonssikkerhet ved din institusjon.
- Rådfør deg med din institusjon hvis du er usikker eller prosjektet bruker nytt utstyr/løsning/leverandør som ikke er godkjent ved din institusjon.
- Prosjektleder må sørge for at det finnes en løpende oversikt over hvilke navngitte personer som til enhver tid har tilgang til hvilke personopplysninger og hvorfor slik tilgang er nødvendig. Husk å oppdatere tilganger ved endringer i prosjektgruppen.

7. DELE DATA?

Avklar om prosjektet skal dele data med andre, underveis eller etterpå.

Hvis ja, avklar om mottaker trenger personopplysninger.
Hvis ja, avklar hva som er formålet med delingen og hva er mottakers rolle?

Se formålsbeskrivelsen for prosjektet ditt (boks 1), definisjonen av personopplysninger (boks 3) og roller (boks 4), og beskrivelse av dataflyt (boks 6).

Vurder:

- Hvilke tilganger som er nødvendig for prosjektformålet:
  - Hvilke personer skal få tilgang til personopplysningene i prosjektet?
  - Hvorfor trenger de tilgang til personopplysninger for å oppfylle formålet/sine oppgaver i prosjektet?
  - Hvilken rolle har de som får tilgang (kategori mottaker)?
    - ansatte ved din institusjon (behandlingsansvarlig)
    - ansatte hos fellesansvarlig institusjon
    - ansatte hos databehandler
- Om personopplysninger skal brukes til andre formål enn prosjektet:
  - Skal du eller andre bruke personopplysninger fra prosjektet til andre formål enn prosjektformålet (underveis eller etterpå)?
  - Før deling/ny bruk må du i samråd med din institusjon:
    - Sikre rettslig grunnlag for delingen. Hvilke vilkår datadelingen må oppfylle finner du i lover/forskrifter som gjelder ditt prosjekt (boks 5).
    - Ta stilling til hvilken dokumentasjon mottaker må gi til prosjektet, for at din institusjon skal kunne påvise at delingen er lovlig.
  - Hvis prosjektet skal dele data systematisk til nye formål:
    - Lag en skriftlig rutine som viser hvilke momenter dere må vurdere og hvilken dokumentasjon dere må ha før hver utlevering.
    - Sjekk at utleveringsrutinen er i samsvar med de lover/forskrifter som gjelder ditt prosjekt.
    - Det er særlig viktig før oppstart av befolkningsbaserte helseundersøkelser og medisinske kvalitetsregistre, der formålet er gjenbruk av data.
  - Institusjonen din må føre skriftlig protokoll over alle utleveringer av personopplysninger fra prosjektet. For hver utlevering må dere dokumentere mottakers rettslige grunnlag og momentene i sjekklisten under Protokoll (nederst i flytskjema).

Husk:

- Personer som jobber i prosjektet, kan bare få tilgang til personopplysninger hvis de trenger det for å utføre sine oppgaver.
- Enhver deling – og enhver ny bruk – av personopplysningene til nytt formål er en egen behandling. Det gjelder også hvis du selv eller andre ved din institusjon skal bruke opplysningene videre til andre formål. Følg da flytskjemaet fra start for den nye behandlingen.
- Rådfør deg alltid med din institusjon før deling/ny bruk til andre formål enn prosjektet. Da forankrer du vurderingen av at viderebehandling er lovlig.

- Hvis dere utleverer til annen institusjonen, er mottaker dataansvarlig for den videre behandlingen. Hovedoppgaven for dere er da å sikre at selve utleveringen er lovlig. Men sjekk rutiner ved din institusjon. Noen ønsker å inngå utleveringsavtale med mottaker som gir vilkår/begrensninger for videre bruk.
- Det kan være vanskelig å vurdere om prosjektendring innebærer nytt formål/prosjekt. Rådfør deg med din institusjon, eller REK hvis helseforskning.

8. VARIGHET. HVA SKJER MED PERSONOPPLYSNINGENE ETTERPÅ?

Anslå hvor lenge prosjektet trenger å behandle personopplysninger for å oppnå formålet.
Avklar hva dere skal gjøre med personopplysningene i datamaterialet når prosjektet er avsluttet.
Avklar om publikasjoner fra prosjektet vil være anonyme eller inneholde personopplysninger.

Vurder:

- Hvor lenge det er nødvendig å behandle personopplysninger for å oppnå formålet. Sett dato eller angi kriterier for når behandlingen skal opphøre.
- Avklar hva som skal skje med personopplysninger i datamaterialet når prosjektet er fullført:
  - **Slette**: *Sjekk først om dere trenger opplysningene videre pga. arkiveringsplikt eller behov for videre forskning*
  - **Anonymisere**: *Lag en plan for hvilke tiltak prosjektet må gjøre for at opplysningene faktisk er anonyme etterpå*
  - **Viderebehandle**: *Avklar til hvilke formål, og hvem som er behandlingsansvarlig*
- Avklar hva som skal skje med personopplysninger i publikasjoner fra prosjektet:
  - **Publisere anonyme opplysninger:** *Lag en plan for hvilke tiltak prosjektet må gjøre for at opplysningene faktisk er anonyme*
  - **Publisere personopplysninger:** *Avklar lovlig grunnlag for denne behandlingen av personopplysninger (samtykke er hovedregel)*

Husk:

- Personopplysninger skal ikke lagres lenger enn det som er nødvendig for formålet. Når du planlegger sluttdato er det likevel lurt å ta høyde for at det kan skje uplanlagte forsinkelser, og at det kan ta tid å innhente tillatelser, få på plass avtaler, få tilgang til data og publisere.
- Det kan også oppstå uplanlagte endringer i prosjektopplegget som kan kreve nye personvernvurderinger/tillatelser, evt. ny informasjon til de registrerte.
- Hovedregelen er at personopplysninger skal slettes når formålet er oppfylt. Men det er mulig å lagre opplysningene videre for gjenbruk i forskning på visse vilkår. Hvis det er aktuelt, er det best å planlegge dette ved prosjektstart. Rådfør deg med din institusjon.
- Anonymisering innebærer at alle personopplysninger (definert i boks 3) må slettes eller omskrives, slik at det ikke er mulig for noen å gjenkjenne enkeltpersoner i datasettet, verken direkte eller indirekte. Anonyme data kan brukes fritt. Men vær klar over at selve anonymiseringen er en behandling av personopplysninger der du må følge personvernregelverket. Rådfør deg med din institusjon.

9. INFORMASJON TIL DEN REGISTRERTE

De registrerte har rett til informasjon. Utarbeid informasjon til de registrerte.
Eller dokumenter at vilkår for unntak er til stede.

Vurder:

- Hovedregel om informasjon:
  - De du behandler personopplysninger om har rett på informasjon.
  - Du må informere før du samler inn data fra den registrerte, eller (hvis andre datakilder/ikke samtykke), innen en måned.
  - Informasjonen skal være kortfattet og lett forståelig, og må gis individuelt via kanaler der den når frem.
  - Den kan gis skriftlig eller muntlig, men du må dokumentere at – og hvilken – informasjon som er gitt.
  - Du må informere om:
    - Hvem som har ansvar for behandlingen (kontaktopplysninger til din institusjon)
    - Hvorfor (formål), hvor lenge, og på hvilket lovgrunnlag opplysningene behandles,
    - Hvem som vil få tilgang til personopplysningene (mottakere),
    - Hvilke datakilder opplysningene hentes fra
    - Hvilke rettigheter den registrerte har: innsyn/kopi, retting, sletting, protest/trekke samtykke, klage til Datatilsynet
    - Kontaktopplysninger til personvernombudet ved din institusjon
    - Lovlig grunnlag for å overføre personopplysningene ut av EU/EØS (hvis aktuelt)
    - Planer om utlevering/viderebehandling til andre formål (hvis aktuelt)
- Unntak:
  - Loven åpner for at du i enkelte situasjoner kan behandle personopplysninger uten å gi informasjon.
  - Du må da dokumentere unntakshjemmel og at vilkårene er oppfylt. Rådfør deg med din institusjon.
  - Her er de aktuelle unntakene for forskning/kvalitetssikring:
    - Den registrerte har allerede fått informasjonen
    - Utilrådelig å informere, av hensyn til den registrertes helse eller forhold til nærpersoner
    - Det er umulig eller krever uforholdsmessig stor innsats å informere
    - Informasjon vil sannsynligvis ødelegge for formålet (forskning/kvalitetssikring)
    - Behandlingsansvarlig er lovpålagt å behandle personopplysningene

- Hvis prosjektet ikke gir individuell informasjon fordi det er umulig, uforholdsmessig vanskelig, og/eller kan ødelegge forskningsformålet, må dere gi kollektiv informasjon. En måte er å publisere informasjon om prosjektet i kanaler/nettsider *som det er sannsynlig* at de registrerte leser, f.eks. en interesseorganisasjon.

Tips:

- Sikt personverntjenester har utarbeidet maler for informasjonsskriv i forskning: Informasjon til deltakarane i forskingsprosjekt (sikt.no)
- REK har utarbeidet maler for informasjonsskriv i helseforskning: Hjem - Insights (rekportalen.no)
- Vent med å sende ut informasjonsskrivene til du har fullført flytskjema.

10. REGISTRERTES RETTIGHETER

De registrerte har rett til innsyn (kopi), retting og sletting, og rett til å trekke samtykket, eller reservasjon.
Organiser prosjektet slik at de registrerte kan utøve sine rettigheter.

Vurder og legg en plan:

- Hvordan legger prosjektet til rette for at de registrerte kan utøve sine rettigheter:
  - Har den registrerte fått kontaktinformasjon til prosjektansvarlige og personvernombud, så de vet hvor de kan henvende seg?
  - Lagres data slik at prosjektet lett kan finne opplysningene om den registrerte (f.eks. via koblingsnøkkel prosjektet har tilgang til)?
  - Vet du og andre kontaktpersoner (ved egen eller samarbeidende institusjoner) hva dere skal gjøre hvis registrerte henvender seg, slik at de får rett svar innen tidsfristen?

Husk:

- Rettighetene gjelder så lenge de registrerte kan identifiseres i datamaterialet.
- Prosjektet skal ikke lagre flere personopplysninger enn nødvendig for formålet, bare for å kunne innfri rettighetene.
- Loven åpner for unntak fra rettighetene i enkelte situasjoner, men avslag må ikke gis uten begrunnelse og lovhjemmel.
- Innsyn må kun gis til den som personopplysningene gjelder, ikke til andre (f.eks. når du har data om deltager/tredjeperson og foreldre/barn).
- Feilvurdering av rettigheter kan føre til ulovlig behandling. Rådfør deg med din institusjon, særlig før du gir innsyn eller gir avslag.
- Institusjonen din har plikt til å vurdere om rettighetene skal/kan innfris, og svare den registrerte innen en måned.

11. Personvernkonsekvensvurdering (DPIA)

Vurder om den planlagte behandlingen av personopplysninger medfører høy risiko for den registrerte.
Hvis ja, gjennomfør DPIA.

DPIA er et verktøy for å kartlegge og håndtere risikoer knyttet til behandling av personopplysninger. DPIA kreves før behandlinger som sannsynligvis gir "høy risiko for de registrertes rettigheter og friheter". Datatilsynet og EUs personvernråd (EDPB) har publisert veiledere om hva som er høy risiko.

Vurder:

- Se på kartleggingen du har gjort over. Vil behandlingen av personopplysninger i prosjektet medføre høy risiko?
- Hvis prosjektet oppfyller et eller flere av kriteriene under, eller du er usikker, bør du rådføre deg med din institusjon eller personvernombud.
- Jo flere av kriteriene som gjelder, desto mer sannsynlig at prosjektet må ha DPIA (se også Datatilsynets veileder):
  - Behandling sensitive personopplysninger (særlige kategorier, straffedommer/lovovertredelser, eller svært personlig karakter)
  - Behandling av personopplysninger i stor skala (mht. utvalgsstørrelse, mengde opplysninger, varighet, frekvens)
  - Behandling av personopplysninger om sårbare registrerte
  - Sammenstilling av datasett (f.eks. datakilder med ulike formål/behandlingsansvarlige) som overstiger den registrertes rimelige forventninger
  - De registrerte hindres i å utøve sine rettigheter
  - Innovativ bruk av ny teknologi eller organisatorisk løsning
  - Evaluering (profilering/kartlegging av personopplysninger for å analysere eller forutsi personers adferd, helseforhold, preferanser, interesser, evner, behov el.)
- Systematisk monitorering (ulike former for observasjon/sporing av personer, bl.a. på internett/offentlig område, f.eks. kameraovervåking, observasjon av internettaktivitet, lokasjonssporing og helseovervåking ved hjelp av sensorer og applikasjoner.)Hvis prosjektet trenger DPIA, følg prosedyrer ved din institusjon.

Husk:

- DPIA er en prosess, der dere beskriver den planlagte behandlingen, vurderer om den er lovlig og forholdsmessig, kartlegger risikoer, og foreslår risikoreduserende tiltak. Personvernombudet skal rådføres, før resultatet av DPIA fremlegges i et dokument for ledelsen ved din institusjon. Ledelsen vurderer om DPIA er godt nok utført, og om risikoen er akseptabel, slik at prosjektet kan starte. Hvis ikke, kan ledelsen bestemme at DPIA må revideres, eller at behandlingen må forhåndsdrøftes med Datatilsynet, eventuelt stoppes.
- Forhåndsdrøfting med Datatilsynet er påkrevd hvis personvernkonsekvensene fortsatt er for høye etter DPIA, og institusjonen ønsker å gjennomføre behandlingen av personopplysninger. Datatilsynet kan gi råd og/eller sette vilkår for behandlingen.

Tips:

- Direktoratet for e-helse har utgitt Mal og veiledning for utfylling av personvernkonsekvensvurdering (DPIA) - ehelse
- Hvis du skal melde prosjekt til Sikt, utarbeider Sikt en DPIA for prosjektet i samarbeid med deg, basert på Sikt sin DPIA-mal.

12. TILLATELSER

Søk nødvendige tillatelser

Vurder:

- Basert på kartleggingen du har gjort over, sjekk om prosjektet trenger godkjenning fra en eller flere instanser:
- Helseforskning: Forhåndsgodkjenning fra REK
- Klinisk utprøving av legemidler, medisinsk utstyr og in-vitro diagnostisk utstyr: Godkjenning fra Statens legemiddelverk (SLV)
- Humant biologisk materiale:
  - til Helseforskning, Annen forskning, Kvalitetssikring på tvers og Medisinsk kvalitetsregister: Godkjenning fra REK
  - til Intern kvalitetssikring og Befolkningsbasert helseundersøkelse: Melding til Biobankregisteret ved FHI
- Helseopplysninger fra pasientjournal eller andre behandlingsrettede helseregistre, uten samtykke
  - til forskningsformål (helseforskning og annen forskning): Dispensasjon fra taushetsplikten fra REK
  - til kvalitetssikringsformål: Dispensasjon fra taushetsplikten fra Helsedirektoratet
- Helseopplysninger fra helseregistre omfattet av Forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata:
  - Vedtak fra om tilgjengeliggjøring av helseopplysninger fra Helsedataservice
  - Vedtak om dispensasjon fra taushetsplikten for helseopplysninger fra helseregistre, eventuelt i kombinasjon med helseopplysninger fra pasientjournal eller andre behandlingsrettede registre
- Personopplysninger fra registre som ikke er omfattet av forskriften over: Vedtak fra registerforvalter
- Personopplysninger fra registre som ikke er omfattet av forskriften over: Vedtak fra registerforvalter
- Andre taushetsbelagte personopplysninger uten samtykke: Vedtak fra aktuelt fagdepartement- eller direktorat (f. eks NAV, Bufdir, UDI, SSB mv.)
- Helseopplysninger til intern kvalitetssikring: Oppdragsdokument fra virksomhetens ledelse

Husk:

- Med "samtykke" menes samtykke fra den enkelte registrerte (den som opplysningene gjelder).
- Tillatelsene over gjelder for alle typer prosjekt, med mindre annet er spesifisert.
- I noen tilfeller må du sende søknader til flere instanser. Merk da at alt du søker REK om, sendes i samme søknad.
- For intern kvalitetssikring gir oppdragsdokumentet unntak fra taushetsplikten. Du trenger derfor ikke vedtak om dispensasjon.
- Direktoratet for e-helse v/Helsedataservice har vedtaksmyndighet for følgende helseregistre: Dødsårsaksregisteret, Kreftregisteret, Medisinsk fødselsregister, Meldingssystem for smittsomme sykdommer (MSIS), System for vaksinasjonskontroll (SYSVAK), Norsk pasientregister (NPR),

Nasjonalt register over hjerte- og karlidelser, System for bivirkningsrapportering, Kommunalt pasient- og brukerregister (KPR), Legemiddelregisteret, Helsearkivregisteret.

Tips:

- ♦ Send søknader i god tid før datainnsamling. Send gjerne søknadene samtidig.
- ♦ Vær nøye med å beskrive prosjektet på samme måte i alle søknader.
- ♦ Hvis du er usikker på hvilke godkjenninger og tillatelser prosjektet trenger, kontakt din institusjon i god tid før datainnsamling.

13. AVTALER

Etabler nødvendige avtaler

Vurder:

- ➢ Vurder hvilke avtaler prosjektet må ha for behandling av personopplysninger (jf. boks 4 og 7 over):
  - Avtale om felles dataansvar - når din institusjon er felles behandlingsansvarlig sammen med en eller flere institusjoner
  - Databehandleravtale - når din institusjon er databehandler eller bruker databehandler
- ➢ Sjekk om din institusjon pålegger prosjektet å inngå andre typer avtaler i tillegg, f.eks.:
  - Avtale om utlevering av personopplysninger til ny dataansvarlig/nytt formål (uten felles dataansvar)
  - Avtale om utlevering av humant biologisk materiale - din institusjon skal utlevere eller motta humant biologisk materiale
  - Samarbeidsavtale – regulerer avtalepartenes rettigheter og plikter vedrørende andre forhold ved prosjektet, som finansiering, oppgavefordeling, publiseringspoeng, rettigheter til forskningsresultater og data mv.
- ➢ Følg prosedyrer og maler for avtaleinngåelse ved din institusjon.

HUSK:

- ➢ Rådfør deg med din institusjon hvis du er usikker på hvilke avtaler som bør inngås i prosjektet.
- ➢ Avtale om felles dataansvar/databehandler må inngås før behandling av personopplysninger starter.
- ➢ En samarbeidsavtale som ikke regulerer behandlingen av personopplysninger er ikke tilstrekkelig, hvis partene har tilgang til personopplysninger.
- ➢ Deling av humant biologisk materiale innebærer ofte behandling av personopplysninger. Materialet kan være merket med et ID-nummer eller det skal foretas analyser som gir helseopplysninger. Da er det være nødvendig å med avtaler som dekker behandling av personopplysninger.

Tips:

- Direktoratet for e-helse har utgitt mal for standard databehandleravtale med veileder: Standard databehandleravtale med veileder - ehelse
- Datatilsynets veiledning om roller og ansvar til dataansvarlig og databehandler: Behandlingsansvarlig og databehandler | Datatilsynet

14. DOKUMENTASJON

Sørg for at din institusjon protokollfører prosjektet og arkiverer dokumentasjon på at behandlingen av personopplysninger er lovlig.

Beskriv:

- I protokollen trenger institusjonen din følgende informasjon om hvordan prosjektet behandler personopplysninger:
  - hvem som er behandlingsansvarlig
  - formålet/ene (hvorfor personopplysningene behandles)
  - kategorier registrerte og typer personopplysninger,

- hvilke mottakere som får tilgang (hvis utenfor EU/EØS - oppgi land og garantier)
- tidspunkt/kriterier for når dere skal slette personopplysningene
- og sikkerhetstiltak ved behandlingen

Husk:

➢ Din institusjon trenger også mer dokumentasjon for å sikre at behandlingen av personopplysninger er i samsvar med personvernregelverket. Spør din institusjon om hvor og hvordan du skal dokumentere dette for ditt prosjekt.

15. KLART FOR DATAINNSAMLING

Etter at du nå har fullført alle stegene i malen over, kan du starte prosjektet og datainnsamlingen.
Vær oppmerksom på at hvis prosjektet endres underveis (mht. punktene over), må du foreta ny vurdering av relevante punkter.