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

Referat

Til
Styringsgruppen for
Norm for informasjonssikkerhet i helse- og omsorgssektoren

Møteinnkalling

Møtetidspunkt: **Torsdag 08.06.2023 kl. 9.00-15.30**
Sted: Fysisk, Direktoratet for e-helse, Skøyen

Virksomhet/Organisasjon	Representant	Til stede/ forfall
Apotekforeningen		Forfall
Den norske legeforening	Petter Hurlen	Til stede
Den norske tannlegeforening	Camilla Hansen Steinum	Til stede
Den offentlige tannhelsetjenesten	Steinar Løgith Aase	Til stede
Norsk farmaceutisk forening		Forfall
Norsk fysioterapeutforbund		Forfall
Norsk psykologforening		Forfall
Norsk sykepleierforbund		Forfall
KS	Suhail Mushtaq	Til stede
	Arne Ingebrigtsen (leder)	Til stede
KiNS	Harald Torbjørnsen	Til stede
Helse Midt-Norge RHF	Laila Eikeset	Til stede
Helse Nord RHF	Ida-Kristin Martinussen	Til stede
Helse Sør-Øst RHF	Jon Holden	Til stede
Helse Vest RHF	Lars Erik Baugstø-Hartvigsen	Til stede
Private helsevirksomheter (representert ved Fürst)	Christian Bülow-Larsen	Til stede

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

Folkehelseinstituttet	Pål Solerød	Til stede
Direktoratet for e-helse	Kåre Ljungmann	Til stede
Helsedirektoratet	Caroline Ringstad Schultz	Til stede
Norsk Helsenett	Andre Meldal	Til stede
Observatører		
Digitaliseringsdirektoratet	Katrine Aam Svendsen	Til stede
FFO – funksjonshemmedes fellesorganisasjon	Lilly Ann Elvestad	Til stede frem til 1355
IKT-Norge	Amund Lundgård	Til stede
Melanor	Mats Skretting (ResMed)	Til stede
NAV	Trond Simensen	Til stede
NSM		Forfall
WSO		Forfall
Senior Norge		Forfall

Sak	Sakstittel / kommentar / forslag til vedtak
12/23 09.00	**Godkjenning av innkalling og dagsorden** **Styringsgruppens vedtak:** *Styringsgruppen godkjenner innkalling og dagsorden.*
13/23	**Godkjenning av referat fra møte 08.03.23** **Styringsgruppens vedtak:** *Styringsgruppen godkjenner referatet*.
14/23 09.15	**Sekretariatet orienterer, inkludert status på startede prosjekter** • Endringer i helseforvaltningen: Direktoratet for e-helse virksomhetsoverdras til Helsedirektoratet og FHI, sekretariatet for Normen flyttes til Helsedirektoratet (denne orienteringen ble gjennomført av Direktoratet for e-helses direktør Mariann Hornnes, klokken 11.00). • Kurs og webinar • Faktaark Integritet • Mapping ISO og Normen • Normkonferansen

	• m.m Sekretariatet presenterte, se presentasjon. **Diskusjon/spørsmål:** - Det er viktig å promotere aktiviteter som arrangeres i tilknytning til Normkonferansen tidlig (som pre-Normkonferansen), slik at de som er tilreisende kan ordne med transport og hotell i god tid. - Faktaark Integritet: Viktig å ikke bare ha tekniske ressurser involvert, helsefaglige ressurser vel så viktig. Legeforeningen bidrar gjerne. **Styringsgruppens vedtak:** *Styringsgruppen tar sekretariatets orientering til etterretning.*
15/23 09.30	**Drøftingssak: Foreløpig plan for arbeid med små virksomheter** Se vedlagte presentasjon. Sekretariatet ønsker innspill på: 1. Hvordan skal vi avgrense «små helsevirksomheter»? • Er dere enige i at små kommuner ikke dekkes? • Andre avgrensninger vi bør gjøre? 2. Er et hensiktsmessig startpunkt å starte med å arrangere en workshop? • Hvem bør delta? 3. Når det gjelder å få kontakt med små helsevirksomheter for kartlegging: • Har dere innspill til hvordan vi kan få tak i de små virksomhetene? • Har dere noen erfaringer vi kan bygge på i å gjøre en slik kartlegging? • Finnes det noen etablerte strukturer/kanaler for å nå ut til de små virksomhetene? 4. Hva tenker dere om de to kartleggingsalternativene vi skisserer • Alt. 1: spørreundersøkelse • Alt. 2: snakke med noen utvalgte virksomheter 5. Deltagere til referansegruppe knyttet til kartleggingsaktivitetene **Diskusjon/innspill:** - Enighet om at små kommuner ikke dekkes av veilederen. - Se på begrepet «små helsevirksomheter» og hvordan andre benytter det (som Legeforeningen osv.). - Vurdere å se på forskjeller mellom ulike små virksomheter med ulike behov: legekontor med egen server/«fulldriftet» av journalleverandør, private/kommunale, etc. - Veileder OM små virksomheter heller enn FOR? Det er pågående diskusjoner om sendingsmetoder for pasientdata, en veileder bør omtale slike spørsmål. Avtalespesialister som leverandører til RHFene bør også omtales. - Workshop er hensiktsmessig startpunkt. - Målrettet kontakt med små virksomheter er nok best. Fysioterapeutforbundet, Tannlegeforeningen, Legeforeningen, Fürst bidrar

	gjerne med å finne representanter. Sekretariatet sender ut e-post i etterkant av møtet.
16/23 09.45	**Beslutningssak: Veileder i informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren v1.0** Dokument vedlagt. **Diskusjon:** - HUKI-matrisen er et utgangspunkt/eksempel, hensikten er at den tilpasses på oppstartsmøte. Det bør presiseres tydeligere, med en liten infoboks eller lignende. - Lenker til lovhenvisninger i dokumentet når det kommer på web. Helse Vest sender over forslag til flere henvisninger på relevante standarder innledningsvis. Forslagene er: - Relevante ISO-standarder for informasjonssikkerhets- og personvern - CIS Critical Security Controls - GDPR - Nyttig for leverandører og de som yter tjenester, viktig og riktig at det er avgrensninger mot skyveileder. Sekretariatet gjennomfører de diskuterte endringene redaksjonelt. **Styringsgruppens vedtak:** *Styringsgruppen for Normen godkjenner Veileder i informasjonssikkerhet og personvern for leverandører til helse- og omsorgssektoren v1.0*.
17/23 10.00 *(inkludert pause fra 1010-1020)*	**Beslutningssak: Revisjon veileder informasjonssikkerhet og personvern i forsknings- og kvalitetsprosjekter v3.0** Dokument vedlagt. Et fokusområde i revisjonen har vært å gjøre veilederen mer brukervennlig. Et viktig strukturelt grep som er gjort for å få til det, er at veilederen nå enda tydeligere enn tidligere følger gangen i et typisk forsknings- og kvalitetsprosjekt kronologisk, slik det også er gjort i flytskjema. I teksten retter vi oss til prosjektleder, men det er presisert at veilederen kan brukes av andre prosjektmedarbeidere, personvernressurser og andre støttefunksjoner. Det er lagt vekt på å få til en praktisk tilnærming, og det er gjennomgående inntatt flere eksempler i teksten. Videre er det brukt et enklere språk med kortere setninger. Tidligere var veilederen rettet mot forskning, og særlig helseforskning. Veilederen har nå fått et bredere «virkeområde» og omtaler nå ulike former for forsknings- og kvalitetsprosjekter, samt litt om registre. Dette har vært et viktig grep for å få frem skillet mellom prosjekttyper, som har vært etterlyst i arbeidsgruppe og i andre tilbakemeldinger vi har fått. I forlengelsen at utvidelsen er det gitt en mer grundig beskrivelse av behandlingsgrunnlagene, og det er inntatt flere behandlingsgrunnlag enn tidligere. Vi har likevel kun omtalt de behandlingsgrunnlagene som er mest relevant i forsknings- og kvalitetsprosjekter.

Veilederen retter seg fortsatt mot helse- og omsorgssektoren, men vil ha overføringsverdi til *forskning* i andre sektorer.

Innholdet i veilederen er i all hovedsak videreført og skrevet om i revisjonen, med unntak av feil og enkelte punkter knyttet til gjennomføring av helseforskningsprosjekter (organisering og etiske vurderinger etter helseforskningsloven, som ikke berører personvern og informasjonssikkerhet). Vi har også innarbeidet de faglige innspillene vi fikk i forbindelse med utviklingen av flytskjema fra blant annet Datatilsynet, Helsedirektoratet, Helsedataservice, REK/NEM, SLV og SKDE.

Det er et tydeligere fokus på personvern og informasjonssikkerhet. Det er f.eks. avgrenset mot organisering av helseforskning og spørsmål knyttet til immaterialrett.

Nb! Noen henvisninger kan mangle lenker, dette legges inn ved publisering.

Diskusjon:

- Hjemmelsgrunnlag helseregisterloven § 19 a eller b? Dialog etableres med Helsedirektoratet for å avstemme (lovfortolkende myndighet). Endringen håndteres redaksjonelt.
- KiNS fremhever at miljøer utover helse- og omsorg i kommunene/ fylkeskommunene også egentlig trenger en slik forskningsveileder. De delene av veilederen som er generelt for forskningsprosjekter vil brukes også av de som arbeider på områder utenfor helse- og omsorg.

Styringsgruppens vedtak:
Styringsgruppen for Normen godkjenner Veileder i personvern og informasjonssikkerhet i forsknings- og kvalitetsprosjekter v3.0 slik den er fremlagt, med endringer etter avklaring av helseregisterloven § 19 a eller b.

07/23 10.30

Beslutningssak: Mapping NSMs grunnprinsipper for IKT-sikkerhet og Normen

Dokument vedlagt.

Sekretariatet for Normen har utarbeidet utkast til mapping mellom NSMs grunnprinsipper for IKT-sikkerhet v.2.0 og krav i Normen.

Hovedformålene med mappingen har vært å foreta en grovanalyse for å identifisere hvilke av grunnprinsippene (inkludert mål og anbefalte tiltak) som ikke er dekket i Normen, og for å være til hjelp for virksomhetene til å se sammenhenger.

NSMs grunnprinsipper for IKT-sikkerhet er i de fleste tilfeller mer detaljert i sin beskrivelse enn kravene i Normen, og i mange tilfeller formulert annerledes.

Normens krav vil derfor i de fleste tilfellene ikke være fullt ut dekkende, og det er flere gråsoner for tolkningsrom. Mappingen er et utgangspunkt for å forstå sammenhengene, og må ikke tolkes til å være uttømmende.

Diskusjon:

- Cybersikkerhetsforskriften – hvordan vil den påvirke den normerende rollen til NSM i forhold til det som kommer fra EU? Ennå ikke kjent, NSM tar dette med i betraktningen mtp. tidspunkt for oppdatering av grunnprinsippene.
- Vurdere grafisk fremstilling for fremtiden, sett i sammenheng med hvordan mappingen blir brukt i praksis.
- Fremheve viktigheten av å velge tiltak basert på identifisert risiko. Dette bør inkluderes i presentasjonen av mappingen.
- Fortsette å se på krav som ikke er dekket eller delvis dekket i Normen, og hvordan dette skal presenteres. Tema for neste handlingsplan.
- Dokumentet er svært omfattende slik det er nå. Bør vurdere å ta mapping ut i eget dokument dersom det blir mye brukt.

Styringsgruppens vedtak:
Styringsgruppen for Normen godkjenner Mapping NSMs grunnprinsipper for IKT-sikkerhet og Normen. Mappingen publiseres i dokumentbiblioteket til Normen. Sekretariatet vurderer redaksjonelt om det skal publiseres sammen med andre mappinger eller om det opprettes en egen dokumentside. Mappingen publiseres sammen med teksten over her i innkallingen.

Dersom det kommer innspill på endringer etter publisering, kan sekretariatet gjøre redaksjonelle endringer dersom det er endringer av lite prinsipiell karakter. Det samme gjelder dersom NSM oppdaterer grunnprinsippene og det medfører små endringer.

Det tas inn en setning om at tiltak skal vurderes basert på risiko.

Sekretariatet jobber videre med å se på krav som ikke er dekket eller delvis dekket i Normen.

19/23
10.50

(inkludert innlegg fra direktør e-helse fra 1100-1110, ref. sak 14/23)

Beslutningssak: Veileder i bruk av skytjenester til behandling av helse- og personopplysninger v. 3.0.

Dokument vedlagt.

Sekretariatet har foretatt en mindre oppdatering av Normens skyveileder. Endringene består hovedsakelig i oppdatering og omstrukturering av eksisterende tekst, og kan dermed ser mer omfattende ut enn det som er tilfellet.

Oppdateringene består i:

- Flytting over til ny mal
- Oppdatering eller sletting av utdaterte illustrasjoner, referanser og kilder.
- Omstrukturering av eksisterende tekst i ny struktur.
- Noe tilleggstekst om blant annet Zero Trust, bruk av Normens krav i anskaffelser og kontrollspørsmål til leverandører, og overføring av personopplysninger utenfor EU/EØS.

I tillegg er det laget et nytt vedlegg med et eksempel på en modell for informasjonsklassifisering. Dette er basert på arbeidet som er gjort med informasjonsklassifisering i de regionale helseforetakene. Formålet med vedlegget er å illustrere hvordan informasjonsklassifisering i samhandlingsløsninger kan gjøres og vise frem etablert praksis. Teksten i vedlegget forvaltes av Sykehuspartner.

Diskusjon:
Veilederen

- Ang. innsendt innspill fra Helsedirektoratet: Kostnad ved å ta i bruk sky – bør dette fremheves mtp. at det vil være gevinster i andre enden? Helsedirektoratet fremhever at kostnadene de ønsket å fremheve var for spesifikke sikkerhetstjenester tilknyttet sky, ikke skytjenester generelt. Kan være riktig å heller fremheve at å tabR i bruk skytjenester forutsetter en annen type forvaltning, skapes et forvaltningsbehov man kanskje ikke ser innledningsvis – dette vil kanskje være viktigere enn selve kost-perspektivet. Øvrige innspill tas til følge, ingen motsetninger til sekretariatets presenterte løsninger.
- Ang. innspill om zero trust: behov for enten mer eller mindre informasjon om dette temaet? Det henvises imidlertid fra veilederen til en lengre fagartikkel på normen.no om temaet, som kan avhjelpe dette.
- Ang. øvrige innsendte innspill fra Helse Nord og Helse Vest: ingen motsetninger til sekretariatets presenterte løsninger.
- Generell kommentar fra Helse Sør-Øst om behandlingsrettede helseregister og hvordan dette skal håndteres (hva faller innunder, og tolkes dette riktig?) – uklare begreper og uklar praksis. Støttes av flere. Sekretariatet setter opp en faglig bolk om dette på neste styringsgruppemøte som startpunkt.

Vedlegget

- Ikke omforent i styringsgruppen hvorvidt vedlegget er hensiktsmessig slik det står nå. Sekretariatet fremhever at handlingsplanen kan endres dersom styringsgruppen ønsker utarbeidelse av eget faktaark.
- Sentrale spørsmål: Er det informasjonsklassifisering eller valg av sikkerhetsnivåer som er det sentrale for å beskytte informasjonen ved bruk av skytjenester? Det som presenteres i vedlegget passer kanskje ikke helt inn i resten av veilederen? Bør kanskje heller være et utgangspunkt for arbeid med klassifisering/ verdivurdering? Ikke omforent forståelse i styringsgruppen.
- Legeforeningen fremhever informasjonsklassifisering sett fra pasientperspektivet: Det er ikke gitt at pasient og de som klassifiserer ser dette på samme måte. Samme med helsepersonell.

Styringsgruppens vedtak:
Styringsgruppen for Normen godkjenner Veileder i bruk av skytjenester til behandling av helse- og personopplysninger v. 3.0, med de endringer som ble vist i møtet, se presentasjon.

Vedlegg om informasjonsklassifisering tas ut. Sekretariatet jobber videre med om det kan vises til lenken som er / skal publiseres. Arbeidet videre med informasjonsklassifisering tas opp i diskusjon om prioritering av handlingsplan 2024.

Sekretariatet gis fullmakt til å foreta redaksjonelle endringer i takt med utviklingen i EU.

1200 **Lunsj**

20/23 **Beslutningssak: Faktaark passord og passordhåndtering v3.0**
12.50

Formålet med faktaarket er å gi veiledning til hvordan virksomheten kan sikre at passord som benyttes i virksomheten er underlagt tilstrekkelig sikring.

Faktaarket har en praktisk tilnærming og inneholder beste praksis knyttet til passord og passordhåndtering.

Nb! Noen henvisninger mangler lenker, dette legges inn ved publisering.

Diskusjon:

- Innspill fra Helsedirektoratet: endringer implementert som vist i møtet.
- Innspill fra Helse Nord: endring implementert som vist i møtet.
- Bruk av *skal* eller *bør*? «Der det er mulig legges det til rette for»?
- Risiko og tilpasning til hverdagen for de som yter helsehjelp – bør man ha med mer om dette? Hvilke prosedyrer tilknyttet passord understøtter/hindrer helsepersonell?
  Sekretariatet formulerer en setning om behov for risikovurdering som reflekterer diskusjonen.
- Eventuelle øvrige mindre endringer av ikke-prinsipiell art gjennomføres av sekretariatet i forkant av publisering.

Styringsgruppens vedtak:
Styringsgruppen for Normen godkjenner faktaark 31 Passord og passordhåndtering versjon 3.0.

Sekretariatet gjør tilpasninger for å ivareta helsefaglig ansvarlighet.

22/23
13.30

Eventuelt – Valg av leder for Normens styringsgruppe

Valgkomiteen innstiller på gjenvalg av Arne Ingebrigtsen fra KS (Kristiansund kommune) som styringsgruppens leder.

Styringsgruppens vedtak:
Arne Ingebrigtsen fra KS (Kristiansund kommune) velges som leder for Normens styringsgruppe for en ny periode.

21/23
13.35

Workshop for å kartlegge behov for revisjon av Mandat for styringsgruppen og Forvaltningsmodell for Normen

Styringsgruppens medlemmer bes forberede seg ved å lese Mandat for styringsgruppen og Forvaltningsmodell for Normen. Disse spørsmålene vil stå sentralt i workshopen:

- Hva fungerer bra i arbeidet med Normen?
- Hvor er det forbedringspotensial?
- Er det behov for endringer i forvaltningsmodell og mandat?
- Kan vi gjøre prosessene smidigere?

Sekretariatet for Normen vil bidra i workshopen sammen med styringsgruppen for å få frem hva som fungerer godt fra sekretariatets perspektiv og hvor vi ser forbedringspotensialet.

Workshop:

- Balansegang mellom styringsgruppens konsensus/beslutningsmyndighet vs sekretariatets autonomi.
- Legeforeningen er imponert over sekretariatet som gjør en veldig god jobb, ofte på bakgrunn av uklare signaler fra styringsgruppen, så kanskje ikke en dårlig ide å gi sekretariatet mer arbeidsrom og at styringsgruppen kan være mer prinsipiell aktør?
- FFO stiller spørsmål om det er riktig ressursbruk at alle medlemmer av styringsgruppen skal delta på alt.
- Melanor: Fra leverandørsiden er det å delta i referanse- og arbeidsgrupper veldig verdifullt for å få gode og nyttige produkter.
- HSØ: Man burde kanskje bli bedre på evaluering – spørre representanter fra sektoren mer om hvilke produkter de benytter og hvordan, heller enn bare hva de ønsker seg.
- Helse Vest: Kanskje burde man spørre de nye medlemmene spesifikt om hva ved/hvordan deltagelsen fungerer for dem?
- Legeforeningen: Når tilgjengelighet og integritet kommer mer på banen, mens det fremdeles er store mengder konfidensialitet – er det flere ting som kan saneres?
- KiNS: For KiNS er Normen en bauta, som blir vist til og støtter oss til i veldig stor grad. Noe av veiledningsmaterialet har behov for mer tilpasning til kommunesektoren, og her bidrar KiNS gjerne videre, blant annet med ressurser fra ulike kommuner/roller fra nettverket.
- Direktoratet for e-helse: I direktoratet opererer vi med ulike normeringsnivåer som gir ulike prosesser, mens vi i stor grad behandler alle saker på samme måte i SG. Kan en større differensiering være noe å tenke på?
- SG leder: Kanskje benytte ambisjonen fra utvidelsen av SG for å evaluere om målet er oppnådd?
- NAV: Bør alle saker behandles i møte, eller bør flere saker ha skriftlig/e-post-behandling? Bør også bruke muligheter til å evaluere i fremtiden, om vi oppnår det vi ønsker mht. etterlevelse.
- KiNS: Kanskje kan SG være mer strategisk heller enn detaljfokusert.
- Helse Nord: Støtter det mtp. møter – kanskje bør man be om skriftlige innspill en uke før møte, og så heller diskutere det som er stridstema eller prinsipielt i møtet.
- Helse Nord: Har fått inn GDPR i Normen, men hvordan håndterer vi de nye (endrede) sikkerhetsrelaterte lov/forskrifter som kommer de neste årene? Må få opp en god prosess for dette.
- Helse Nord: Grunnsikring er viktig både for de store og de små, her har vi nok alle noe å gå på, på tvers av sektoren.
- HSØ: Må være forsiktig med å legge opp til at avsendere/mottagere selv skal vurdere om de ulike aktørene har tilstrekkelig sikkerhet til å kommunisere.
- HSØ: Skriftlig behandling av saker – teknisk løsning for å jobbe sammen? Nyttig å se de andres innspill også mens man kommer med egne.
- Legeforeningen: Ansvar og etterlevelse. Har du ansvar for at den som tar imot kan forstå det som sendes? Dette blir relevant mht integritet. Ser dette i praksis nå.
- Helsedirektoratet: Skille mellom hvordan vi behandler saker, ta detaljer skriftlig og løfte frem det prinsipielle til møter der vi møtes fysisk? Se på muligheter for endringer i frekvens, form, etc. for å oppnå ulike mål etter det som er hensiktsmessig.

	Sekretariatet bearbeider innspillene fra workshopen, og følger opp med en-til-en samtaler med de som ønsker for å komme videre på de ulike temaene. Dette arbeidet fortsetter på neste møte i styringsgruppen.
14.25	**SLUTT**