

Referat Styringsgruppemøte i Normen

Til Styringsgruppen for Norm for informasjonssikkerhet i helse- og omsorgssektoren

Møtetidspunkt: **Onsdag 27.09.2023 kl. 9.00-12.00**

Sted: **Digitalt møte**

Virksomhet/Organisasjon	Representant	Til stede/ forfall
Apotekforeningen	Kenneth Bjørnstad	Til stede
Den norske legeforening	Petter Hurlen	Til stede
Den norske tannlegeforening		Forfall
Den offentlige tannhelsetjenesten	Steinar Løgith Aase	Til stede
Norsk farmaceutisk forening	Hanne Sandberg	Til stede
Norsk fysioterapeutforbund	Henrietta Richter	Til stede
Norsk psykologforening		Forfall
Norsk sykepleierforbund	Jo Cranner (vara)	Til stede frem til 11.05.
KS		Forfall
	Arne Ingebrigtsen (leder)	Til stede
KINS	Harald Torbjørnsen	Til stede
Helse Midt-Norge RHF	Stein Gilde	Til stede , frem til 11.00
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
Folkehelseinstituttet		Forfall
Direktoratet for e-helse	Kåre Ljungmann	Til stede
Helsedirektoratet	Caroline Ringstad Schultz	Til stede
Norsk Helsenett	Marit Larsen Haar	Til stede
Observatører		
Digitaliseringsdirektoratet	Siri Beisvåg Rom	Til stede
FFO – funksjonshemmedes fellesorganisasjon	Arnfinn Aarnes	Til stede frem til 10.30
IKT-Norge	Amund Lundgård	Til stede
Melanor	Mats Skretting (ResMed)	Til stede
NAV		Forfall
NSM		Forfall
WSO		Forfall
Senior Norge	Rune Andersen	Til stede

Sak

Sakstittel / kommentar / forslag til vedtak

23/23 Godkjenning av innkalling og dagsorden

09.00 Styringsgruppens vedtak:

Styringsgruppen godkjenner innkalling og dagsorden

24/23 Godkjenning av referat fra møte 08.06.23

Styringsgruppens vedtak:

Styringsgruppen godkjenner referatet

25/23 Sekretariatet orienterer, inkludert status på startede prosjekter, inkludert

09.10

- Kurs og webinar
- [Normkonferansen](#)
- Faktaark Integritet
- Mapping ISO og Normen
- Kartlegging av små virksomheter
- Videre arbeid med revisjon av forvaltningsmodell og mandat for styringsgruppa

Spørsmål/diskusjon:

Små virksomheter:

- Styringsgruppa stiller spørsmål ved hvem som blir invitert til workshop om hvordan man sikrer spredning blant deltakere, og viktigheten av å opplyse om kompensasjon. De som melder seg på er kanskje ikke de som bruker veilederen i det daglige.
- NHN spør om hvilken fase veilederen skal fokusere på, for eksempel oppstart og drift.

Normkonferansen:

- CISO-samling: Hva med de som ikke har CISO, kan også de som har CISO-oppgaver også delta? Tittel er ikke avgjørende, det bør presiseres.
- Personvernsamling bør også rette seg mot fagansvarlig personvern og fagansvarlig informasjonssikkerhet.
- KINS tilbyr seg å markedsføre Normkonferansen i sitt neste nyhetsbrev

Faktaark integritet

- Krevende løp med kort tid. Prøv å beskrive noen av de konkrete erfaringene fra sektoren. Dette vil være til hjelp uansett.

Mapping ISO

- Helse Vest har lagt til grunn ny ISO-standard i sitt styringssystem og tar gjerne et møte om dette.
- KiNS sitt styringssystem er også oppdatert og tar også gjerne en prat.
- Refleksjon fra HSØ om prioritering: Dette vil være et generelt arbeid, viktig å fremme det som er spesifikt for helsesektoren. Bør omforene dette arbeidet med Dig.dir og NSM.

26/23

Direktoratet for e-helses anbefaling til prioriterte tiltak innen digital sikkerhet – innspill til oppfølging i videreutvikling av Normen.

10.00

Se vedlagte toppnotat.

Jan Gunnar Broch presenterte på vegne av Direktoratet for e-helse.

Spørsmål/diskusjon:

- Helse Nord takker for gode oppdateringer fra dette arbeidet.

10.30

Pause

27/23

Handlingsplan 2024

10.45

Se vedlagt forslag til handlingsplan. Forslaget er basert på innspill fra redaksjonskomiteen og sekretariatet. Forslaget drøftes på dette møtet og styringsgruppen gir sine innspill til handlingsplanen. Endelig handlingsplan besluttet på styringsgruppemøtet i november.

Medlemmene i styringsgruppen bes forberede innspill til prosjekter og satsingsområder som de mener skal være med i handlingsplanen for 2024, basert på Normens strategi 2023-2025.

Spørsmål/diskusjon:

- Først har innspill handlingsplanen for i år: Laboratoriene er i kontakt med små virksomheter til vanlig. Er opptatt av sikkerhetskultur, og må veilede de små på dette. Små V har ofte ikke noen egen sikkerhetskultur. Ønsker å fremheve dette perspektivet inn i arbeidet.
- NHN: Hvordan utfordres ansvar knyttet til digital hjemmeoppfølging?
- KS: Digitale verdikjeder blir mer komplekse, KI har tatt mye plass. I hele verdikjeder vil den som leverer tjenester prøve å oppnå en markedsfordel ved å implementere KI i sin del av kjeden. Spår at KI kommer til å bli viktig, og at man bør se på hvordan det påvirker Normen. Det er store mengder datadeling som skjer uten at brukere er klar over det. EHDS vil endre landskapet vi opererer i. Digital hjemmeoppfølging skjer ikke bare i kommunene, blir også mer vanlig i spesialisthelsetjenesten.
- E-helse: Støtter KS om KI og digital hjemmeoppfølging. Sekretariatet har en del basisoppgaver som bør gå igjen i alle handlingsplaner, med veiledere osv. på toppen av det.
- Helse Nord mener det er viktig å ha en handlingsplan som støtter at Normen er aktuell og tidsriktig. Man bør se på teknologisk utvikling, og KI og digital hjemmeoppfølging bør prioriteres høyt. Etterlyser data- og dokumentdeling i handlingsplanen. Hvordan kan man bruke erfaringene som man har innhentet så langt?
EDHS og NIS2 viktig, i tillegg AI Act, her er det viktig å balansere fokus på den teknologiske og den regulatoriske siden.
Små virksomheter er viktig, samt muligheter for å kontrollere etterlevelse av Normen.
Ved angrep så har man ofte sviktet på de grunnleggende tiltakene.

- Furst: Normen kan ha en god innvirkning på KI gjennom begrepsavklaring. Hva er AI og hva er IKKE AI?
- Sykepleierforbundet støtter prioritering av KI og viktigheten av at Normen er tett på utviklingen og på implementeringen .
Ta videre opp kompetanseutvikling i utdanningen (retos (1, 2,3)): et krav er at kandidaten skal ha kjennskap til informasjonssikkerhet. Viktig at Normen er relevant i utdanningen av helsepersonell.
- Sekretariatet spiller inn at det er vanskelig å finne en vei inn, hvordan kan man gå frem? Oppfordrer SG til å komme med innspill til hvordan dette kan realiseres. Dig.dir sender en e-post om dette.
- Furst mener man kan oppnå mye ved å gå gjennom PVO for å få en god opplæringskultur, også mot helsepersonell. Hvordan kan de forstå IS og PV i en praktisk kontekst?
KiNS får mange henvendelser om NIS, støtter tilnærmingen om hva Normen skal være fremover.
- NHN: Viktig å også huske på de «gamle trendene», for eksempel sky. Flere vil gå i sky fremover, og det vil påvirke leverandørpøpfølging og de digitale verdikjedene, samt hvordan man stiller krav til leverandører. Vil være viktig å fortsette å holde skyveilederen oppdatert. Viktig å kravstille innebygget sikkerhet og personvern. Støtter Nord sitt innspill om å «fix the basics». Hva er det helt grunnleggende tiltakene for å være robuste og forberedte?
- Dig.dir: Positivt å være i fremkant om nye regelverk. Positivt om fokus på ny teknologi.
- Helse Sør-Øst: Viktig å holde fast på gode møteplasser, både om gamle og nye ting. Diskusjoner som kan påvirke politikk, herunder risiko og KI, kan være verdt å prioritere. Helse har kanskje en annen inngang enn resten av forvaltningen, det er kanskje ikke like avgjørende med krav til forklarbarhet her.
Leveransekjeder: Få frem behovet for dybdeforsvar. Få frem forståelsen av at kjeden er mye lengre enn man ofte tror.
Etterlevelse og kravstilling inn mot MTU viktig. Med nytt utstyr følger nye utfordringer. Noen leverandører inngår avtaler direkte mot pasient, det medfører nye utfordringer. Noe mer om Zero Trust? For eksempel deep fakes viser at man har et dårlig tillitsanker.
- Legeforeningen: Fint med fokus på integritet. Enig med fokus på EHDS, her må man følge med enn så mange. Bemerk at EU er opptatt av pasientperspektivet, mens Norge kanskje er mer opptatt av myndighetsperspektivet. Løfter utfordringen med automatiske Oversettelser av pasientdata og integritet.
Det er vanskelig å oppdatere alle dokumentene, vi må tenkte mer over hva vi skal ta vekk og prioritere hardere.
Veiledning er ofte monolog, sektoren etterspør dialog.
- IKT Norge: Løfter frem EHDS. Fra leverandørperspektivet: øker pasientens disposisjonsrett over egne opplysninger, som vil bli større enn nåværende pasientrettigheter.
SaaS-modeller er økende, i tillegg til KI.

- SG-leder/KS: i hvilken grad stiller vi med kapasitet på informasjonssikkerhet på konferanser og andre fora? Ta med dette under kompetansehevingsaktiviteter i handlingsplan.

Skulle vi invitert KI-prosjektet inn til neste SG? Hvordan kan Normen bidra?

Saksgrunnlag til neste gang: tilbakemeldinger på eksisterende veiledningsmateriell.

27/23 Eventuelt

12.00 SLUTT