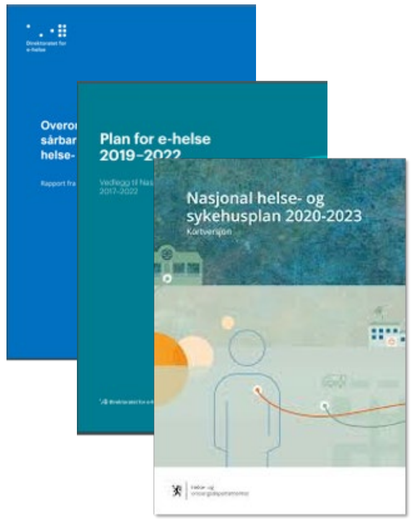
Direktoratet for e-helse

Strategi for digital sikkerhet i helse- og omsorgssektoren
Strategiske områder pr 02.02.22

Strategiens temaområder



Sektorspesifikke behov

- ✓ Trusselbilde
- ✓ Sikkerhetsbehov som følger av teknologisk utvikling og digitalisering i sektoren
- ✓ Forutsetninger og særtrekk ved sektoren

Tydeliggjøre sikkerhetsbehov

Identifisere strategiske virkemidler

Tydeliggjøre roller og ansvar

Temaer i strategien

Sektorspesifikke temaer

- Sikker samhandling
- Sikker digital hjemmeoppfølging
- Sikkerhet i leverandørkjeden

Tema fra den nasjonale strategien

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

Strategiens formål og målsettinger

Formål

Alle virksomheter i helse- og omsorgssektoren legger til rette for forsvarlig helsehjelp gjennom sikker digitalisering i et risikobilde i endring

Målsettinger

- Ansvar og roller med betydning for digital sikkerhet i og mellom sektorens virksomheter er avklart, kjent og ivaretatt.
- Det er høy tillit til hvordan sektoren ivaretar digital sikkerhet, både fra innbyggere og pasienter og mellom samhandlende virksomheter.
- Sektoren ivaretar sikkerhet i lange og komplekse digitale verdikjeder.
- Virksomhetene i sektoren har tilstrekkelig evne til å ivareta digital sikkerhet, understøttet av en robust digital infrastruktur og felles tjenester, ressurser og standarder.
- Virksomhetene evner å effektivt ta i bruk fremskridende teknologier på en sikker måte og er robuste i møte med et risikobilde i endring.

Strategiske områder

Strategiske områder

NUIT 19.11

Strategiske områder

- Satsning på øvelser
- Økt kontroll av etterlevelse
- Felles kompetansetiltak
- Styrket informasjonssikkerhet i leverandørforhold
- Godkjenningsordninger
- Felles ordninger, ressurser og tjenester for å understøtte og avlaste mindre virksomheter

Gjeldende arbeidsversjon av strategien:

Felles kompetansetiltak

Overordnet beskrivelse

- For å sikre en effektiv forbedring av sikkerhetskompetanse og –kultur i hele sektoren (også i små virksomheter), bør det utvikles felles kampanje- og kompetanseressurser som sektoren kan dele og ta i bruk.
- Ressursene må tilpasses de ulike aktørene i sektoren med hensyn til å arbeidsoppgaver og forutsetninger.

- Et mulig tiltak er at det etableres et kompetanseprogram innen digital sikkerhet for hele helse- og omsorgssektoren. Programmet kan utvikle og forvalte virkemidler og læringsressurser tilpasset sektorens behov, og må ses i sammenheng og samvirke med andre nasjonale kompetansetiltak.
- 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.

På dette strategiske området vil det være viktig å ha fokus på videreutvikling og forbedring av allerede iverksatte tiltak, for eksempel:
- Digital sikkerhet som kompetansemål i helseutdanningen
- RHFenes planer om kartlegging av sikkerhetskultur med påfølgende tiltak

Et naturlig første steg på dette området vil være at det gjennomføres en kartlegging av behov i sektoren, og en plan for gjennomføring av tiltak.

Forventede effekter

- ✓ Digital sikkerhet oppfattes som en del av etablert sikkerhetskultur og relateres til det å yte forsvarlig helsehjelp
- ✓ Bedret tillitsforhold mellom virksomheter
- ✓ Riktige ressursprioriteringer
- ✓ Reduksjon av atferd som bidrar til å svekke IKT-sikkerheten.

Hvem gir dette området effekt for?

Dette strategiske området vil gi stor effekt for både små og store virksomheter.

Økt kontroll av etterlevelse

Overordnet beskrivelse

I arbeidet med strategien har det kommet hyppige innspill om at det er behov for å vite mer om etterlevelse i sektoren.

Dette området involverer et bredt spekter av mulige tiltak, for eksempel:

- Økt fokus på internrevisjon og sikkerhetstesting i virksomhetene
- Egenvurdering
- Karlegging av modenhetsnivå for implementering av ledelsessystem for informasjonssikkerhet (ISMS)
- Revisjon med veiledning
- Tilsyn

Sagt i NUFA: «Vi har en ordning som sjekker kvalitet på laboratoriene hos fastlegene - vi trenger en tilsvarende ordning på informasjonssikkerhet»

Også på dette området vil et første steg være en utredning om hva en ordning kan omfatte, inklusive en kartlegging av behov i sektoren.

Forventede effekter

- ✓ Tydeliggjøring og avklaring av roller og ansvar, gjennom kontinuerlig evaluering og forbedring
- ✓ Økt modenhet innen internkontroll og risikostyring (proaktiv forbedring)
- ✓ Økt bevissthet om og bedre kontroll med måloppnåelse inne digital sikkerhet
- ✓ Utbedring av manglende eller mangelfulle sikkerhetstiltak

Hvem gir dette området effekt for?

Dette strategiske området vil gi stor effekt for hele sektoren.

Satsing på øvelser

Overordnet beskrivelse

Dagens trussel- og risikobilde krever at sektorens virksomheter må være forberedt på å håndtere ulike digitale hendelser.

Øvelser er et effektivt verktøy, ved at det legger opp til
- omsetting av teori i praksis
- avdekking av mangler
- evaluering og utbedring.

Behovet for flere øvelser knyttet til informasjonssikkerhet er blant annet påpekt av Riksrevisjonen.

- Det må signaliseres tydelige forventninger til at virksomhetene skal planlegge, gjennomføre og evaluere øvelser, samt aktivt benytte erfaringene i sitt løpende forbedringsarbeid.
- Øvelser må prioriteres, og det må stilles nødvendige ressurser til disposisjon.
- Satsingen omfatter en kombinasjon av at digital sikkerhet øves særskilt, og som del av større øvelser.
- Økt satsing på øvelser både internt i de enkelte virksomhetene, innad i helseregionene, i samarbeid med leverandører og nasjonalt med ulike aktører

Det første steget på dette strategiske området vil være å utarbeide en overordnet plan for øvelser i sektoren.

Forventede effekter

- ✓ Tydeliggjøring og avklaring av roller og ansvar
- ✓ Forbedrede beredskapsplaner
- ✓ Øving på og forbedring av ferdigheter, samarbeid og kommunikasjon
- ✓ Avdekking og forbedring av teknologiske og organisatoriske sårbarheter
- ✓ Økte ferdigheter og bevissthet

Hvem gir dette området effekt for?

Dette strategiske området vil ha stor effekt på sektoren som helhet.

Styrket informasjonssikkerhet i leverandørforhold

Overordnet beskrivelse

- Sikkerhetsnivået i sektoren er avhengig av sikkerhetshåndteringen hos leverandører.
- Både leverandører og bestillere etterlyser tydeligere og standardiserte sikkerhetskrav og nasjonale føringer for risikoaksept i anskaffelser.

- Mange av virksomhetene i sektoren har utfordringer ved utøvelse av tilstrekkelig god sikkerhetsstyring, inkludert kravstilling/ evaluering ved anskaffelser, gode risikovurderinger og leverandørkontroll.
- Ulik tolking av krav og manglende tilsyn ser ut til å være problematisk i forbindelse med å oppnå effektive anskaffelser og innovasjon.

- Det er behov for å utvikle felles krav til styring og oppfølging av leverandører.
- Viktig å bidra til at det stilles samme krav til like tjenester ved hjelp av standardiserte kravsett og ressurser som kan gjenbrukes på tvers av virksomheter.

- Et mulig konkret tiltak er støtte til virksomheter ved anskaffelser og bruk av ny teknologi gjennom tilgang til felles ressurser som RoS-analyser og DPIA.

- Et første steg på dette området kan være å utarbeide felles krav til styring og oppfølging av leverandører, og finne mekanismer for gjenbruk av prosesser knyttet til RoS og DPIA.

- Et mulig tiltak er også godkjenningsordninger av produkter og tjenester som tas i bruk
    - kan omfatte et bredt spekter av mekanismer fra frivilling selvdeklarering til obligatoriske sertifiseringsordninger.
    - nødvending med utredning på flere områder, bl.a. omfang, kravsett, juridiske forhold og EU-rett.

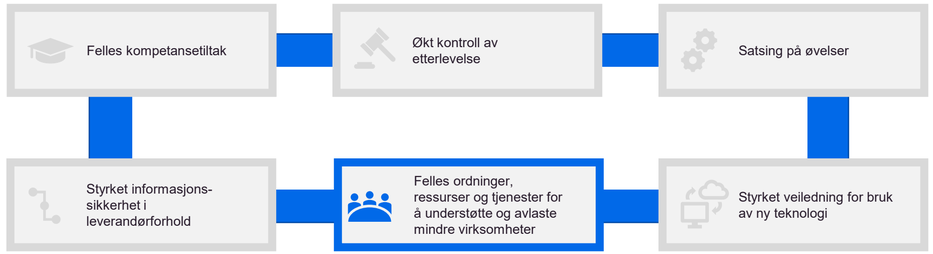
Forventede effekter

- ✓ Høyere kvalitet og færre uklarheter ved anskaffelser
- ✓ Helhetlig styring og oppfølging av leverandører
- ✓ Aktiviteter i forbindelse med anskaffelser gjøres tilgjengelig for felleskapet som utgangspunkt for gjenbruk.
- ✓ Mer effektiv tidsbruk og redusert belastning på hver enkelt virksomhet.

Hvem gir dette området effekt for?

Dette strategiske området vil ha stor effekt på sektoren som helhet.

Felles ordninger, ressurser og tjenester for å understøtte og avlaste mindre virksomheter



Overordnet beskrivelse

Det bør identifiseres og etableres felles ordninger, ressurser og tjenester på områder der felles satsing forventes å gi verdi for bredden av mindre virksomheter i sektoren. Eksempler er:

- Felles utarbeidelse av ROS & DPIA (f.eks. ved ny teknologi, nye løsninger)
- Identifisere kapasiteter for kompetanseheving
- Deteksjon og hendelseshåndtering
    - Etablering av felles deteksjonsmuligheter / sentral logginnsamling for avdekking av ondsinnet aktivitet i mindre virksomheter.
    - Felles retningslinjer og tydeliggjøring av godkjente kapasiteter for hendelseshåndtering

Det iverksettes også tiltak for å øke kjennskapen til og forståelsen av de etablerte tjenester og ressurser som eksisterer i dag (f.eks Normen). Det forutsettes at belastningen på virksomhetene ikke øker vesentlig.

Strategien vil bidra til bedre understøttelse av de små virksomhetene i sektoren, ved å gi bedre oversikt over eksisterende felles ordninger, ressurser og tjenester som allerede eksisterer, samt ved å etablere nye der behov.

Startpunktet vil være en kartlegging av sikkerhetstilstand og –behov i små virksomheter.

Forventede effekter

- ✓ Bedre kjennskap til og bruk av felles ordninger, ressurser og tjenester
- ✓ Effektivisering og økt kvalitet i sikkerhetsrelaterte prosesser i virksomhetene
- ✓ Mer hensiktsmessig bruk av tid og ressurser i de små virksomhetene
- ✓ Bedre beslutningsgrunnlag for å opprette/etablere tjenester som sektoren har behov for
- ✓ Økt kompetanse innen digital sikkerhet i de små virksomhetene

Hvem gir dette området effekt for?

- Strategien vil gi stor effekt for små virksomheter, og også for mindre kommuner.
- Strategien kan gi noe effekt for HF og større virksomheter ved å bidra til tillit i samhandling.
- Strategien kan gi noe effekt for leverandører, ved mer konsekvent kravstilling og risikovurdering, og raskere ibruktagelse av tjenestene.

Styrket veiledning for bruk av ny teknologi

Overordnet beskrivelse

Den teknologiske utviklingen skjer raskt og gir stadig nye muligheter for utvikling av bedre og mer effektive helsetjenester. Noen eksempler på er:

- Bruk av skytjenester er et område som tilbyr skalerbare løsninger med funksjonalitet og innebygget sikkerhet som ikke kan sammenlignes med lokale installasjoner.
- Kunstig intelligens, maskinlæring, IoT og sensorteknologi er andre fremskridende teknologier som vil kunne ha stor betydning for den fremtidige helsetjenesten.
- Å ta i bruk ny teknologi på en sikker måte stiller krav til kompetanse og evne til å vurdere risikoer og avhengigheter

- Derfor bør det ***gjennomføres felles vurderinger og utarbeides tilpassede veiledninger for bruk av fremskridende teknologier***.
- De fleste av sektorens virksomheter vil stå ovenfor de samme utfordringene ved bruk av nye teknologier, og må vurdere mange av de samme risikoene og forholdende.

Forventede effekter

- ✓ Ved å legge til rette for felles vurderinger og utarbeidelse av prinsipper vil tiden frem til implementering av nye løsninger reduseres.
- ✓ Dette vil kunne bidra til bedre helsetjenester og økt pasientsikkerhet for innbyggerne.

Hvem gir dette området effekt for?

- Vil avhenge av hvilke deler av sektoren som styrket veiledning rettes mot, men særlig mindre virksomheter vil kunne ha god nytte av dette strategiske området.