Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge (HMN)

Versjon 0.9

Versjonsnummer	**Dato**	**Behandling/endring**	**Godkjent av**
0.9	28.10.2021	Fremlegg for styret	
1.0			

1 Definisjoner

Begreper	Forklaring
Styringssystem	De aktiviteter, systemer og prosesser som tas i bruk for å planlegge, gjennomføre, evaluere og korrigere virksomheten slik at den samsvarer med krav fastsatt i lover, standarder, avtaler og forpliktende retningslinjer.
Informasjonssikkerhet	Informasjonssikkerhet dreier seg om å håndtere risiko relatert til Helse Midt-Norges informasjonsverdier og behandling av personopplysninger.
Personvern	Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Personvern er også en samlebetegnelse for rettsregler som særlig tar sikte på vern for individet.
HMN	Forkortelse for Helse Midt-Norge, som inkluderer alle helseforetakene i, i regionen
Kultur	Kultur er hvordan samspillet mellom verdier, holdninger og tanker, som deles av individer i en virksomhet, påvirker deres atferd. Dette blir her sett i sammenheng med informasjonssikkerhet og personvern, ofte kalt «informasjonssikkerhetskultur»

2 Formål og omfang

Formålet med dette dokument er å etablere mål og strategi for informasjonssikkerhet og personvern som del av Helse Midt-Norges (HMN) regionale styringssystem for fagområdene. Videre er formålet å beskrive ledelsens intensjon og engasjement, som skal gi grunnlag for systematisk arbeid med informasjonssikkerhet og personvern. Dokumentet spesifiserer også de overordnede prinsipper, roller og ansvar for hvordan informasjonssikkerhet og personvern skal ivaretas i HMN. Dokumentet gir de overordnede føringene til alle underliggende dokumenter og prosesser.

Dette dokumentet gjelder for all informasjonsbehandling i HMN, både manuell og maskinell, analog og digital, lagret og kommunisert. Dokumentet skal gi felles rammer og retning for enhetlig arbeid med informasjonssikkerhet og personvern i HMN.

3 Målgruppe

Innhold og føringer i dette dokumentet gjelder alle som behandler eller forvalter informasjon som ansatt eller på oppdrag for Helse Midt-Norge. I det etterfølgende er disse referert til som «medarbeidere». Innholdet og føringene kan gjøres gjeldende for tredjeparter og leverandører gjennom avtaler.

4 Roller og ansvar for informasjonssikkerhet og personvern

Informasjonssikkerheten og personvernet skal ivaretas gjennom tydelige roller og ansvar.[1]

Ansvar og myndighet for informasjonssikkerhet og personvern skal følge det ordinære linjeansvaret. Virksomheten v/administrerende direktør er dataansvarlig for all behandling av helse og person-

[1] Organisering, roller og ansvar for informasjonssikkerhet er nærmere beskrevet i styringssystemets dokument NO 04 – Organisering av informasjonssikkerhets og personvernarbeidet i Helse Midt-Norge.

opplysninger med tilknytning til virksomheten. Administrerende direktør er videre endelig ansvarlig for informasjonssikkerhet og personvern i egen virksomhet. Videre gjelder følgende:

- Administrerende direktør er ansvarlig for innhold og godkjenning av dette dokumentet.
- Ledere på alle nivåer har ansvar for etterlevelse av dokumentet i egen enhet.
- Ledere på alle nivå er ansvarlig for å opprettholde en kultur som kontinuerlig bevisstgjør og forebygger brudd på konfidensialiteten, tilgjengeligheten og integriteten ved behandling av personopplysninger.
- Alle medarbeidere er ansvarlig for å etterleve de dokumentene i styringssystemet som er relevant for sin rolle i virksomheten.
- Alle medarbeidere er ansvarlig for å rapportere uønskede hendelser, avvik og svakheter i informasjonssikkerheten

5 Mål for informasjonssikkerhet og personvern

Det overordnede målet for informasjonssikkerheten er at

- informasjon, systemer og tjenester er tilgjengelig ved behov (tilgjengelighet)
- informasjon ikke endres utilsiktet eller av uvedkommende (integritet)
- informasjon ikke blir kjent for uvedkommende (konfidensialitet)

For å oppnå dette må organisasjonen og informasjonssystemene være motstandsdyktige mot trusler, være i stand til å oppdage og reagere på hendelser, samt ha evne til raskt å gjenopprette normaltilstand etter en hendelse(robusthet). Videre gjelder følgende mål:

- Helse Midt-Norge skal ivareta konfidensialitet, integritet og tilgjengelighet til informasjonsverdiene i henhold til gjeldende lover, forskrifter, føringer fra myndighetene, samfunnsoppdraget og informasjonseiernes interesser. Kontinuerlig oppfølging, evaluering og forbedring av styringssystemet for informasjonssikkerhet og personvern skal sikre at dette blir ivaretatt. Norm for informasjonssikkerhet og personvern i helsesektoren (Normen) skal følges.
- Informasjonssikkerhet og personvern skal være en integrert og naturlig del i alle prosesser, tjenester og systemer ved Helse Midt-Norge
- Hensynet til informasjonssikkerhet og personvern skal være en integrert del av all virksomhetsstyring i HMN
- Informasjonssikkerhets- og personvernarbeidet skal være risikobasert. Risikovurderinger skal gjennomføres jevnlig og ved endringer som har betydning for informasjonssikkerheten og personvernet.

Ved målkonflikter skal det legges stor vekt på å ivareta helseberedskap og pasientsikkerhet. Mål-konflikter skal håndteres i henhold til gjeldende risikostyringsprosess og ansvarsmatrise.

6 Strategi og prinsipper for informasjonssikkerhet og personvern

Alle helseforetak i regionen skal ha et relevant og oppdatert styringssystem for informasjonssikkerhet og personvern basert på lov, forskrift og anerkjent standard og bransjenorm. Helseforetakene skal benytte

Helse Midt-Norge RHF sine styringsdokumenter supplert med foretaksinterne dokumenter, slik at det overordnet er en samlet og lik håndtering av informasjonssikkerhet i regionen.
Styringssystemet for informasjonssikkerhet og personvern skal være en del av internkontrollen for helhetlig risikostyring i helseforetakene. I dette ligger krav fra ledelsen at:

- krav til informasjonssikkerhet og personvern skal kommuniseres i styrende dokumenter, og at lederlinjen er ansvarlig for systematisk bruk av risikovurderinger.
- organisering, roller og ansvar, samt krav om tilstrekkelig kompetanse innen informasjonssikkerhet og personvern skal være klart definert.
- helseforetakene har god oversikt og kontroll over sine informasjonsverdier og de høyeste risikoene knyttet til disse
- virksomheten har tilstrekkelige ressurser og tiltak for å beskytte informasjon og informasjonssystemer, samt for å håndtere uønskede hendelser
- virksomheten har kontroll med tilganger og at tilgang til systemer og informasjon kun gis til medarbeidere etter vurdering av tjenstlig behov og i samsvar med taushetsplikten.
- risikoreduserende tiltak velges basert på risikovurderinger, vesentlighet, kost-nytte-vurderinger og ledelsens føringer for risikohåndtering, samt et effektivt sikkerhetsarbeid
- Sikringstiltakene skal være brukervennlige, tilpasset øvrige arbeidsprosesser og innrettet slik at de i minst mulig grad medfører merarbeid for brukere
- risikostyring innen informasjonssikkerhet følger den ordinære risikostyringen i Helse Midt-Norge og at det utformes akseptkriterier slik at avgjørelser om aksept av risiko kan tas på riktig ledernivå med et tilstrekkelig beslutningsgrunnlag.
- det føres oversikt over behandlinger av personopplysninger, samt sørger for at all registrering og bruk av helse- og personopplysninger er i overensstemmelse med taushetsplikten, følger alle personvernprinsipper iht. lovverket og at grunnlaget for databehandlingen er vurdert og godkjent.
- krav til informasjonssikkerhet og personvern er ivaretatt når det benyttes databehandlere og dokumenteres i databehandleravtaler for alle behandlinger der Helse Midt-Norge engasjerer en databehandler eller selv opptrer som databehandler.
- opplæring og arbeid med informasjonssikkerhetskultur og personvern er et prioritert område for å etterleve krav i mål og strategi for informasjonssikkerhet. Sikkerhetsarbeidet skal også være basert på intern og ekstern tilgjengelig kunnskap om trusler, sårbarheter, metoder og beste praksis
- det jobbes med kontinuerlig forbedringsarbeid og systematisk oppfølging av avvik i henhold til gjeldene avviksrutiner for å skape en god rapporterings- og læringskultur. Samt at evaluering, jevnlige revisjoner og jevnlige gjennomganger av at styringssystemet fungerer som tilsiktet. Ledelsen skal minst en gang i året gjennomgå virksomhetens aktiviteter innen informasjonssikkerhet og personvern.

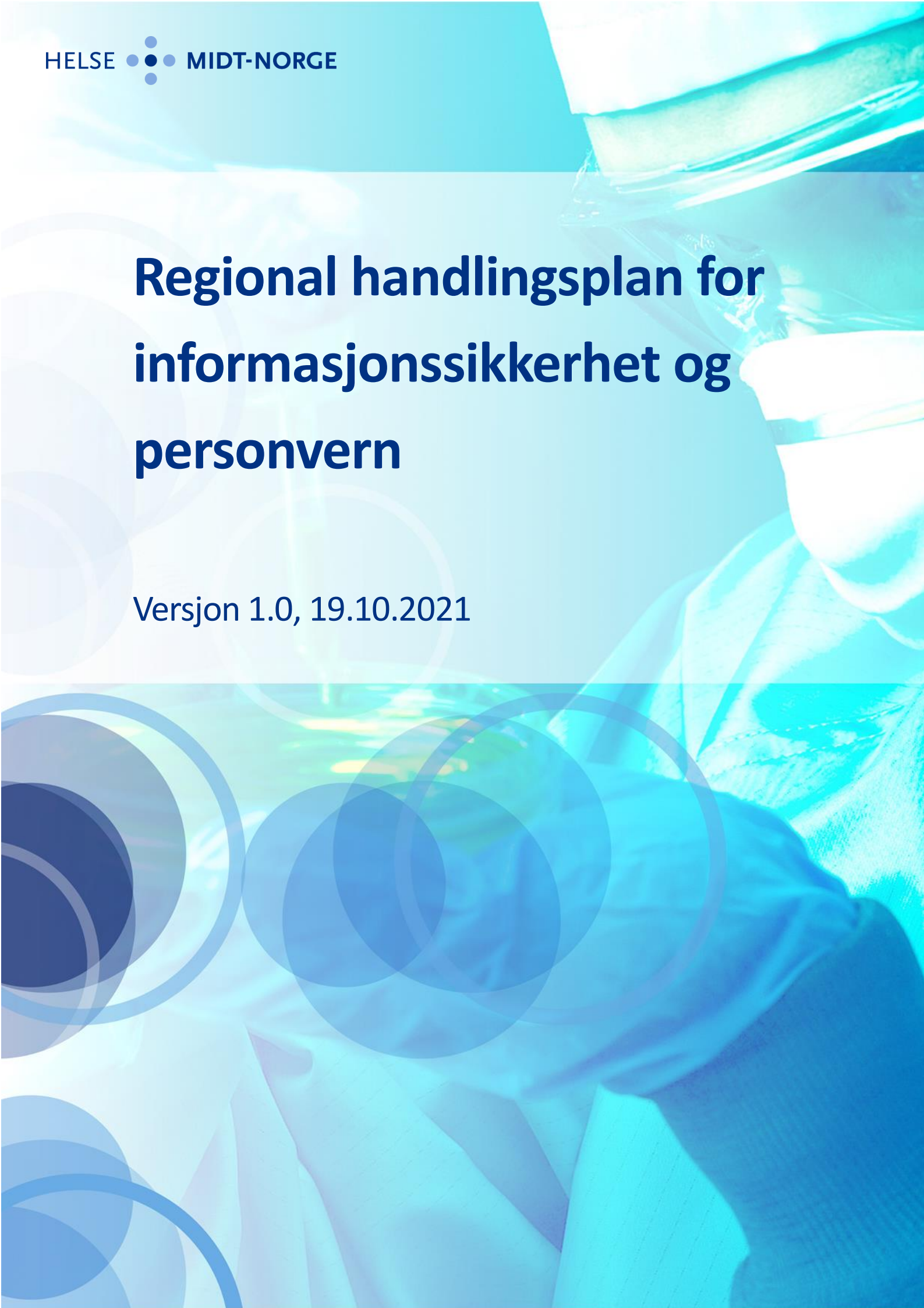
Helseforetakene skal samarbeide for å effektivisere og styrke informasjonssikkerhetsarbeidet på tvers og for å ivareta likeverdige tjenestetilbud. Dette skal skje gjennom samarbeidsforum, informasjonsutveksling og ved å utnytte felles løsninger.

- Måloppnåelse innen informasjonssikkerhet og personvern, samt effekt av tiltak skal måles og rapporteres til ledelsen, slik at hvert helseforetak og Helse Midt-Norge RHF kan vurdere måloppnåelse på ulike nivå.
- Helse Midt-Norge RHF kan i foretaksmøtet gi regionale rammer og føringer for ivaretakelsen av informasjonssikkerhet og personvern i regionen.

HELSE MIDT-NORGE

Regional handlingsplan for informasjonssikkerhet og personvern

Versjon 1.0, 19.10.2021



Innholdsfortegnelse

Versjon	Dato	Behandling/endring	Godkjent av
0.9	14.10.2021	Utkast for godkjenning i Helse Midt-Norge	
1.0	19.10.2021	Versjon 1.0 oversendt HOD	Eierdirektør Helse Midt-Norge RHF

1 Innledning

Foretaksmøtet i Helse Midt-Norge RHF behandlet 14. januar 2021 temaet informasjonssikkerhet. Foretaksmøtet viste til Dokument 3:2 (2020–2021) Riksrevisjonens kontroll med forvaltningen av statlige selskaper, gjennomført i 2019. Foretaksmøtet viste til betydningen av at Riksrevisjonens undersøkelse om helseforetakenes forebygging av angrep mot sine IKT-systemer følges opp.

I protokollen fra foretaksmøtet fikk Helse Midt-Norge RHF flere oppdrag innen informasjonssikkerhet, herunder å utarbeide en regional handlingsplan for arbeidet med informasjonssikkerhet som også omfatter langsiktige tiltak. Planen presenteres på felles tertialoppfølgingsmøte i oktober 2021.

I dette dokumentet beskrives regional handlingsplan for informasjonssikkerhet og personvern i Helse Midt-Norge med tiltak for perioden 2021 til og med 2022. Handlingsplanen er utformet med tiltak beskrevet innenfor fire prioriterte hovedområder og ett område for samling av enkelttiltak. Dette er nærmere beskrevet i kapittel 3 nedenfor. Handlingsplanen skal gjennom innhold og prosess sørge for at alle oppdragene innenfor informasjonssikkerhet fra foretaksmøtet oppfylles.

2 Mål

Helse Midt-Norge skal ivareta konfidensialitet, integritet og tilgjengelighet til informasjonsverdiene i henhold til gjeldende lover, forskrifter, føringer fra myndighetene, samfunnsoppdraget og informasjonseiernes interesser. Kontinuerlig oppfølging, evaluering og forbedring av styringssystemet for informasjonssikkerhet og personvern skal sikre at dette blir ivaretatt.

Organisasjonen og informasjonssystemene skal være motstandsdyktige mot trusler, være i stand til å oppdage og reagere på hendelser, samt ha evne til raskt å gjenopprette normaltilstand etter en hendelse.

Informasjonssikkerhet og personvern skal være en integrert og naturlig del i alle prosesser, tjenester og systemer i Helse Midt-Norge. Informasjonssikkerhets- og personvernarbeidet skal være risikobasert. Risikovurderinger, herunder trusselvurderinger, skal gjennomføres jevnlig og ved endringer som har betydning for informasjonssikkerheten og personvernet.

I arbeidet med informasjonssikkerhet og personvern skal det legges stor vekt på å ivareta helseberedskap og pasientsikkerhet.

Tiltakene i denne handlingsplanen skal bidra til at målene nås og at arbeidet med informasjonssikkerhet og personvern videreføres som kontinuerlig prosess.

3 Tiltak

I dette kapittelet beskrives de tiltak som er iverksatt og/eller vil bli iverksatt som en del av Regional handlingsplan for informasjonssikkerhet og personvern i Helse Midt-Norge.

3.1 Videreutvikling av Regionalt styringssystem for informasjonssikkerhet og personvern

En første versjon av regionalt styringssystem for informasjonssikkerhet og personvern i Helse Midt-Norge er godkjent Q1 2021. Dette som følge av at regionen tidligere i liten grad har hatt felles dokumenter som beskriver hvordan informasjonssikkerhet og personvern skal ivaretas i foretaksgruppen, noe som også ble påpekt i Riksrevisjonens revisjonsrapport 2020-2021. Videreutvikling og implementering av det regionale styringssystemet er viktige tiltak i denne regionale handlingsplanen.

Etablere dokumentstruktur i regionalt styringssystem	
Beskrivelse:	Etablere struktur for dokumentasjonen av regionalt styringssystem for informasjonssikkerhet og personvern i Helse Midt-Norge.
Status:	Forslag til referansemodell for overordnet struktur for styringssystemet er utarbeidet. Referansemodellen skal inngå som en del av regionalt styringssystem.
Tidsperiode:	2021
Ansvarlig:	Helse Midt-Norge RHF

Utarbeide og implementere overordnet styrende dokument for informasjonssikkerhet og personvern i Helse Midt-Norge.	
Beskrivelse:	Utarbeide overordnet styrende dokument for informasjonssikkerhet og personvern i Helse Midt-Norge som beskriver ledelsens føringer, roller og ansvar, mål og strategi, samt viktige prinsipper og krav.
Status:	Dokument *Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge* er utarbeidet og skal legges fram for godkjenning i styret i Helse Midt-Norge RHF i desember 2021, etter forutgående behandling i foretaksstyrene
Tidsperiode:	2021
Ansvarlig:	Helse Midt-Norge RHF

Utarbeide og revidere temaspesifikke dokumenter som inneholder krav, føringer og retningslinjer	
Beskrivelse:	Utarbeide og revidere temaspesifikke dokumenter som beskriver krav, føringer, retningslinjer og prinsipper for sentrale områder innenfor rammen av det regionale styringssystemet for informasjonssikkerhet og personvern. Herunder planlegge og prioritere hvilke dokumenter som skal utarbeides og revideres.
Status:	Det er startet et arbeid med å vurdere hvordan etablerte dokumenter i regionalt styringssystem skal håndteres og tilpasses i henhold til ny dokumentstruktur. Videre er det gjort vurderinger av hvilke temaspesifikke styrende dokumenter som skal utarbeides og prioriteringen av disse. Arbeidet med de høyest prioriterte dokumentene er igangsatt.
Tidsperiode:	2021-2022
Ansvarlig:	Helse Midt-Norge RHF

Utarbeide og revidere felles regionale veiledninger, maler, rutiner og prosedyrer	
Beskrivelse:	Utarbeide og revidere felles regionale dokumenter som skal understøtte operasjonaliseringen av mål, strategi, krav og føringer fra de styrende dokumenter.
Status:	Etableringen av temaspesifikke krav, føringer og retningslinjer vil være retningsgivende for hvilke regionale veiledninger, maler, rutiner og prosedyrer som skal revideres eller utarbeides.
Tidsperiode:	2021- 2022.
Ansvarlig:	Helse Midt-Norge RHF

Kartlegging av dagens situasjon opp mot ISO 27001 og Normen	
Beskrivelse:	Kartlegge dagens situasjon og modenhet i virksomhetene opp mot kravene i Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) og krav i ISO/IEC 27001:2017 Resultatet av en slik kartlegging vil gi en status på virksomhetenes modenhet i forhold til kravene i Normen og ISO 27001. Dette vil videre gi grunnlaget for konkrete tiltaksplaner for økt samsvar med kravene.
Status:	Helse Nord-Trøndelag vil i løpet av Q4:2021 starte en revisjon av informasjonssikkerheten. Erfaringen fra gjennomføringen av denne revisjonen vil gi innspill til gjennomføringen for de øvrige virksomhetene.

Tidsperiode:	2021- 2022
Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

Forbedring av kontrolltiltak og rapportering på informasjonssikkerhet og personvern	
Beskrivelse:	Det skal etableres tiltak som sørger for at revisjoner, risikovurderinger, avvikshåndtering, endringshåndtering, logging, sikkerhetstesting og lignende blir en del av den løpende oppfølgingen av informasjons-sikkerhet og personvern i virksomhetene. Dette skal gi grunnlaget for rapportering på informasjonssikkerhet og personvern og skal benyttes i evaluering og forbedringsarbeid. Krav til rapportering må beskrives med utgangspunkt i et definert informasjonsbehov og implementeres slik at ledelsen får tilstrekkelig informasjon om sikkerhetstilstanden i egen virksomhet. Krav til løpende gjennomføring av revisjoner, risikovurderinger, avvikshåndtering, endringshåndtering og sikkerhetstesting må beskrives slik at virksomheten har tilstrekkelige kontrolltiltak. Kravene og tiltakene skal beskrives i styringssystemets dokumentasjon.
Status:	Ikke startet som tiltak under handlingsplanen, men det er gjort et arbeid med kravstilling til rapportering fra IKT leverandør til foretak. Videre er det gjort tiltak på rapportering til styret innenfor hvert helseforetak.
Tidsperiode:	2022
Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

3.2 Kompetanse, holdninger og kultur

Riksrevisjonen påpeker i sin rapport fra undersøkelsen av helseforetakenes forebygging av angrep mot sine IKT systemer, at det er svakheter i sikkerhets-atferden til de ansatte i helseforetakene og hos IKT leverandørene. For å utbedre disse svakhetene iverksettes følgende tiltak i planperioden:

Gjennomføring av bevisstgjøringstiltak for alle medarbeidere	
Beskrivelse:	Det skal anskaffes en plattform som understøtter bevisstgjørings og opplæringsaktiviteter innenfor informasjonssikkerhet og personvern. Plattformen inneholder ferdigdefinerte opplæringsmoduler med mulighet for tilpasninger. Det skal gjennomføres bevisstgjøringskampanjer med innhold og oppfølging i årshjul for informasjonssikkerhet.

Status:	Årshjul for opplærings- og bevisstgjøringsaktiviteter er etablert for 2021 og 2022. Det er planlagt temaspesifikke aktiviteter for hvert kvartal, som skal videreføres som kontinuerlige aktiviteter. Plattform for gjennomføring av løpende opplæringsaktiviteter er under anskaffelse. Dette tiltaket skal også inkludere tilpassede informasjonsaktiviteter mot ulike grupper, f.eks. ledere.
Tidsperiode:	2021 – 2022. Årshjul skal videreføres og kontinuerlig oppdateres
Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

Opplæring for medarbeidere med fagansvar for informasjonssikkerhet og personvern	
Beskrivelse:	Det skal gjennomføres opplæring tilpasset medarbeidere som har fagansvar innenfor informasjonssikkerhet og personvern. Dette er opplæringstiltak som har som formål å vedlikeholde og oppdatere kompetansen innenfor fagområdet og kunnskapen om utvikling og endring i trusselbildet.
Status:	Kontinuerlig
Tidsperiode:	2021-2022
Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

Opplæring for medarbeidere med definerte roller i styringssystem for informasjonssikkerhet og personvern	
Beskrivelse:	Opplæring av medarbeidere med ansvar for oppfølging av rutiner, prosesser og prosedyrer i tilknytning til styringssystemet for informasjonssikkerhet og personvern. Opplæringen skal bidra til at de roller som har styrende, utøvende og kontrollerende oppgaver innenfor omfanget av styringssystem for informasjonssikkerhet og personvern, er kjent med sine oppgaver og sitt ansvar, samt at de har tilstrekkelig kunnskap til å utføre sine oppgaver.
Status:	Ikke startet
Tidsperiode:	2021-2022
Ansvarlig:	Helse Midt-Norge RHF og det enkelte HF

Gjennomføre kultur-undersøkelse innen informasjonssikkerhet og personvern i virksomheten	
Beskrivelse:	Gjennomføre en undersøkelse av kulturen for informasjonssikkerhet og personvern i virksomheten, med den hensikt å påvise sårbarheter og foreslå tiltak. I tillegg vil en gjentagelse av undersøkelsen med bestemte intervaller gi et bilde på utviklingen i kulturen for

	informasjonssikkerhet og personvern, samt måle om de gjennomførte tiltak har hatt den ønskede effekt.
Status:	Sykehusapotekene i Midt-Norge HF og Hemit har gjennomført slike undersøkelser. Det skal gjennomføres felles undersøkelser for foretakene i regionen. Disse bør bygge på erfaringer fra Sykehusapotekene og Hemit.
Tidsperiode:	2022
Ansvarlig:	Helse Midt-Norge RHF

3.3 Tekniske tiltak

Det ble i 2019 startet et arbeid med å lukke svakheter og sårbarheter basert på tidlig tilgang til resultatene fra Riksrevisjonenes undersøkelse. Arbeidet har pågått fram til i dag og det gjenstår kun et fåtall tiltak med lavere prioritet.

For å sikre en systematisk tilnærming til arbeidet med informasjonssikkerhet og personvern som bygger på «beste praksis» og standarder skal NSM grunnprinsipper benyttes i det videre arbeidet med tekniske tiltak.

Sluttføre og lukke tekniske tiltak for sårbarheter i riksrevisjonsrapporten	
Beskrivelse:	Sluttføre og lukke de tekniske tiltak som ble iverksatt som følge av sårbarheter påvist i riksrevisjonsrapporten (2020-2021).
Status:	De prioriterte tiltak som ble planlagt er fullført og under kontroll. Det gjenstår kun noen enheter innenfor enkelte tiltak som skal ferdigstilles. Noen av tiltakene vil håndteres som del av det kontinuerlige forbedringsarbeidet.
Tidsperiode:	2021-2022
Ansvarlig:	Hemit og de enkelte foretak avhengig av tiltak.

Gjennomføre gap analyse mot NSM grunnprinsipper	
Beskrivelse:	Gjennomføre gap analyse av nåsituasjonen opp mot NSMs grunnprinsipper for IKT- sikkerhet for å vurdere virksomhetenes modenhet, samt vurdere og prioritere tiltak for å redusere risiko og øke modenheten innenfor IKT-sikkerhetsarbeidet. Analysen skal også omfatte relevant Medisinsk-teknisk utstyr (MTU/MU). Basert på gap analysen skal det utarbeides ny tiltaksplan (eller veikart) for tekniske tiltak basert på resultatet fra gap analysen og øvrige identifiserte tiltak.
Status:	Ikke startet
Tidsperiode:	2022

Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

3.4 Medisinsk-teknisk utstyr (MTU)

Riksrevisjonsrapporten peker på en rekke utfordringer og sårbarheter knyttet til Medisinsk-teknisk utstyr (MTU) i helseregionene. Det er satt i gang et arbeid i Helse Midt-Norge for å bedre informasjonssikkerheten og personvernet knyttet til medisinsk-teknisk utstyr. I det videre arbeidet er følgende tiltak prioritert:

Ferdigstille arbeidet med å tydeliggjøre ansvar for MTU	
Beskrivelse:	Ferdigstille arbeidet med tydeliggjøringen av ansvar for MTU. Herunder beskrive og implementere tjenestemodeller med tilhørende ansvarsmatriser (HUKI) for ulike kategorier av MTU utstyr. Ansvar og rollebeskrivelser må også integreres i de styrende dokumenter i styringssystem for informasjonssikkerhet og personvern.
Status:	Pågår
Tidsperiode:	2021
Ansvarlig:	Helse Midt-Norge RHF

Ferdigstille klassifisering/kategorisering av MTU med bakgrunn i Normens veileder for MTU.	
Beskrivelse:	Ferdigstille det påbegynte arbeidet med å kategorisere MTU med bakgrunn i Normens veileder i personvern og informasjonssikkerhet - medisinsk utstyr versjon 2.0. Sikre at registreringen av MTU og kategoriseringen av dette, omfatter slikt utstyr i samtlige av virksomhetene/foretakene i regionen.
Status:	Pågår nasjonalt arbeid opp mot programvare produsent (Medusa).
Tidsperiode:	2021 -2022
Ansvarlig:	Hvert enkelt foretak

Ferdigstille risikovurderinger for de ulike relevante kategorier av MTU	
Beskrivelse:	Ferdigstille det pågående arbeidet med risikovurderinger av relevante kategorier av MTU/MU og de egenskaper og bruksscenarier som gjelder for disse.
Status:	Pågår arbeid for å få gjennomført dette på en ensartet måte nasjonalt. Helse Midt-Norge er en av pådriverne i denne prosessen.
Tidsperiode:	2021 -2022

Ansvarlig:	Hvert enkelt foretak

Utarbeide retningslinjer for MTU	
Beskrivelse:	For å sikre at arbeidet med MTU har de nødvendige føringer, samt å sørge for at det blir en integrert del av arbeidet med informasjonssikkerhet og personvern i virksomheten, anbefales det å vurdere utarbeidelse av en egen retningslinje for MTU. Innspill til føringer i en slikt dokument kan bla. hentes fra «Normens veileder i personvern og informasjonssikkerhet – medisinsk utstyr». Alternativt skal det sørges for at viktige krav og føringer knyttet til MTU er dekket opp av de øvrige retningslinjer i styringssystemet. Kravet til egen retningslinje for MTU må derfor veies opp mot om dette kan beskrives og ivaretas tilstrekkelig i øvrige retningslinjer.
Status:	Ikke startet
Tidsperiode:	2021-2022
Ansvarlig:	Helse Midt-Norge RHF og de enkelte HF

3.5 Andre tiltak

I protokollen fra foretaksmøtet fikk Helse Midt-Norge RHF en rekke oppdrag innen informasjonssikkerhet. Nedenfor listes tiltak som skal løse de oppdrag som ikke er besvart innenfor de fire hovedområdene som er beskrevet ovenfor i plandokumentet. Her listes også andre relevante tiltak innenfor informasjonssikkerhet som skal gjennomføres.

Delta i samarbeidsforum med de andre regionale helseforetakene, Direktoratet for e-helse og Norsk helsenett SF	
Beskrivelse:	Det er opprettet et samarbeidsforum med de andre regionale helseforetakene, Direktoratet for e-helse og Norsk helsenett SF, for å styrke erfaringsoverføring på tvers, og for å identifisere egnede nasjonale og interregionale tiltak for å styrke informasjonssikkerheten i helseforetakene og forebygge angrep mot IKT-systemene. Dette innebærer blant annet øvelser, revisjoner, sårbarhetsskanning og penetrasjonstesting. Forumet skal gi anbefalinger til hvordan kriterier for å akseptere risiko innen informasjonssikkerhet bør utformes.
Status:	Det er gjennomført to møter og er planlagt ytterligere et møte i 2021.
Tidsperiode:	Løpende
Ansvarlig:	Helse Sør-Øst RHF er ansvarlig for innkalling og møteledelse. Helse Midt-Norge RHF er ansvarlig for deltakelse fra vår region.

Benytte trusselvurderinger i ROS-vurderinger og ved prioritering av tiltak	
Beskrivelse:	Benytte Norsk helsenett SFs årlige rapport om trusler, trender, sårbarheter og relevante tiltak som sektoren kan benytte i sitt arbeid med risiko- og sårbarhetsvurderinger.
Status:	Hemit benytter i dag HelseCERTs situasjonsbilde og andre relevante trusselvurderinger ved oppdatering av trusselsituasjonen. Underlaget benyttes i ROS-vurderinger og for vurdering av tiltak innenfor informasjonssikkerhet. Det skal vurderes om det i 2022 skal utarbeides en egen trusselvurdering for foretaksgruppen. Dette foreslås gjennomført i samarbeid med øvrige RHF.
Tidsperiode:	Kontinuerlig
Ansvarlig:	Helse Midt-Norge RHF

Delta i arbeidet med en nasjonal strategi for digital sikkerhet i helse- og omsorgssektoren	
Beskrivelse:	Det skal utarbeides en nasjonal strategi for digital sikkerhet i helse- og omsorgssektoren. Strategien skal bygge på nasjonale føringer, spesielt den nasjonale strategien for digital sikkerhet. Arbeidet ledes av Direktoratet for e-helse og skal gjøres i samarbeid med Norsk helsenett SF, Helsedirektoratet, Helsetilsynet, kommunesektoren/KS og de regionale helseforetakene.
Status:	Arbeidet pågår. Det er levert en tiltaksliste som delleveranse til strategien.
Tidsperiode:	2021
Ansvarlig:	Helse Sør-Øst RHF har en koordineringsrolle for helseregionene. Helse Midt-Norge RHF er ansvarlig for koordinering internt i regionen.

Presentere status fra arbeidet med informasjonssikkerhet	
Beskrivelse:	Presentere status fra arbeidet med informasjonssikkerhet, herunder ledelsens årlige gjennomgang, i egne felles årlige møter, i de etablerte felles tertialoppfølgingsmøtene samt i årlig melding.
Status:	Status på arbeidet med informasjonssikkerhet ble presentert i felles tertialoppfølgingsmøte i juni. Status, samt denne handlingsplanen, skal presenteres i felles tertialoppfølgingsmøte i oktober.

	Se også tiltaket «Forbedring av kontrolltiltak og rapportering på informasjonssikkerhet og personvern» som skal sikre at ledelsen i foretaksgruppen får tilstrekkelig informasjon om sikkerhetstilstanden i egen virksomhet.
Tidsperiode:	Kontinuerlig
Ansvarlig:	Helse Midt-Norge RHF

Informasjonssikkerhetskompetanse i anskaffelser	
Beskrivelse:	Sykehusinnkjøp HF skal benytte kapasitet og kompetanse fra helseregionenes IKT-leverandører for krav til og vurdering av informasjonssikkerhet i anskaffelser.
Status:	Det interregionale AD-møtet har besluttet at Sykehusinnkjøp HF ikke skal bygge opp et egen kompetanse innen informasjonssikkerhet. Vurdering av informasjonssikkerhet og kravstilling ifm. informasjonssikkerhet i anskaffelser skal i stedet gjennomføres ved å trekke inn nødvendig kompetanse fra regionenes informasjonssikkerhetsmiljøer. Det pågår et arbeid, ledet av regionenes IKT-direktører, med å detaljere hvordan informasjonssikkerhetsmiljøene skal involveres, og hvordan deltakelsen skal fordeles mellom regionene.
Tidsperiode:	2019-2021
Ansvarlig:	De regionale helseforetakene

Forvaltning og oppfølging av leverandører	
Beskrivelse:	Informasjonssikkerhet i produkter og tjenester som anskaffes krever også forvaltning etter anskaffelsen er ferdig. Det kan for eksempel være medisinsk-teknisk utstyr eller behandlingshjelpemidler hvor leverandøren har utviklet forbedret funksjonalitet eller rettet opp feil etter anskaffelsen er gjennomført. For nasjonale anskaffelser kan det pekes på en region for å forvalte området som en anskaffelse omfatter, slik at arbeidet med risikoanalyser og oppfølging av leverandører blir mer effektivt etter anskaffelsen er gjennomført
Status:	Det pågår et arbeid, ledet av regionenes IKT-direktører, med å lage et opplegg for hvordan forvaltning av ulike områder kan fordeles mellom regionene.
Tidsperiode:	2021-2022
Ansvarlig:	De regionale helseforetakene

Regional handlingsplan for informasjonssikkerhet og personvern	
Beskrivelse:	Regional handlingsplan for informasjonssikkerhet og personvern skal være et verktøy for prioritering og koordinering av tiltak innenfor informasjonssikkerhet i regionen. Handlingsplanen skal oppdateres årlig og vise prioriterte felles tiltak de nærmeste to – tre årene.
Status:	Første versjon av regional handlingsplan er utarbeidet (dette dokumentet).
Tidsperiode:	Kontinuerlig
Ansvarlig:	Helse Midt-Norge RHF