HELSE MIDT-NORGE

Organisering av informasjonssikkerhet og personvern i Helse Midt-Norge

Versjon 2.0, 15.12.2021

Dokumenteier:

Dokumentet er gyldig til:

Innholdsfortegnelse

Revisjonshistorikk:

Versjon	Dato	Behandling/endring	Godkjent av
1.0	20.01.2021	Første godkjente versjon	Direktørmøte
1.9	09.12.2021	Oppdatert versjon for godkjenning	
2.0	15.12.2021	Godkjent versjon	Direktørmøte

1 Definisjoner og begreper

Forklaring/definisjoner av forkortelser, ord og begreper benyttet i dokumentet:

Begreper	**Forklaring/definisjon**
Helseforetakene	Der begrepet helseforetakene benyttes i dette dokumentet menes alle helseforetak i Helse Midt-Norge inkludert Hemit HF.
Dataansvarlig	Den som er ansvarlig for behandling av helseopplysninger etter personvernforordningen artikkel 4 nr.7. (jfr. Pasientjournalloven §2)
Databehandler	Den (en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ) som behandler personopplysninger på vegne av den behandlingsansvarlige (jfr. personvernforordningen artikkel 4 nr.8.
Virksomhet	Der begrepet virksomhet benyttes i dette dokumentet menes Helse Møre og Romsdal HF, Helse Nord-Trøndelag HF, St.Olavs hospital HF, Sykehusapotekene i Midt-Norge HF, Hemit HF og Helse Midt-Norge RHF

2 Innledning

I følge Norm for informasjonssikkerhet og personvern i helse- og omsorgsektoren (Normen); «*skal virksomhetens øverste ledelse sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre nødvendige oppgaver for å ivareta ansvaret for informasjonssikkerhet og personvern. Oppgavene kan utføres av egne ansatte eller av eksterne*.

Virksomheten skal beslutte hvilke roller og funksjoner for informasjonssikkerhet og personvern som er nødvendig. Det skal være tydelig hvem som er ansvarlig, og hva de er ansvarlig for. Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres relevante ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger.»

3 Formål

Formålet med dette dokument er å beskrive organiseringen av det utøvende sikkerhetsansvar og myndighetsforhold vedrørende informasjonssikkerhet og personvern for virksomhetene i Helse Midt-Norge.

4 Omfang og målgruppe

Krav og føringer i dette dokumentet gjelder for alle virksomheter og nivå i foretaksgruppen og inngår som del i det regionale styringssystemet for informasjonssikkerhet og personvern.

Målgruppen for dokumentet er alle som behandler eller forvalter informasjon som ansatt eller på oppdrag for Helse Midt-Norge.

5 Retningslinjer for organisering av informasjonssikkerhet og personvern

Dokumentet «Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge» beskriver det overordnede ansvar for informasjonssikkerhet og personvern i Helse Midt-Norge. I dette dokumentet (*Organisering av informasjonssikkerhet og personvern i Helse Midt-Norge*) beskrives roller, ansvar og myndighet for informasjonssikkerhet og personvern slik at dette skal være tydelig for medarbeidere i ulike deler av og nivåer i virksomheten.

Ansvarsstrukturen som beskrives i dette dokumentet tilpasses den enkelte virksomhets struktur.

Informasjonsbehandling som skjer med hjemmel i pasientjournalloven, helseregisterloven, helseforskningsloven, personopplysningsloven med flere, er linjestyrte aktiviteter, hvor administrerende direktør har ansvaret for informasjonssikkerheten gjennom sin rolle som øverste leder for den dataansvarlige virksomhet. Informasjonssikkerhetsleder, systemeiere og andre i egen organisasjon svarer dermed for administrerende direktør i foretaket i samsvar med sin rolle.

5.1 Virksomhetenes ansvar og myndighet

5.1.1 RHF sitt ansvar

Helse Midt-Norge RHF skal sørge for tilfredsstillende informasjonssikkerhet og personvern i regionen og tilrettelegge for at helseforetakene kan sikre etterlevelse av Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge.

Helse Midt-Norge RHF har ansvar for at foretaksgruppen har et regionalt styringssystem for informasjonssikkerhet og personvern og at styringssystemet kontinuerlig videreutvikles og forvaltes.

Helse Midt-Norge RHF skal påse at helseforetakene og Helseplattformen AS har et forsvarlig styringssystem og god informasjonssikkerhet.

Helse Midt-Norge RHF kan i foretaksmøter gi regionale rammer og føringer for ivaretakelsen av informasjonssikkerhet og personvern i regionen.

5.1.2 Helseforetakenes ansvar

Helseforetakene har et selvstendig ansvar for informasjonssikkerhet og personvern i eget foretak, herunder at foretaket har et forsvarlig styringssystem. Helseforetakene ved administrerende direktør er dataansvarlig for all behandling av helse- og personopplysninger med tilknytning til virksomheten. Bruk av databehandler endrer ikke foretakets selvstendige ansvar for informasjonssikkerhet.

5.1.3 Hemits (IKT-leverandørs) ansvar

Hemit som IKT-leverandør og databehandler har ansvar for at virksomhetenes informasjonssystem er tilgjengelig og fungerer iht. tjenesteavtalen. Dette innebærer at Hemit har plikt til å etablere og vedlikeholde en infrastruktur som understøtter informasjonsbehandlingen som avtalt. Forpliktelsene reguleres gjennom databehandleravtale som skal inngås med Hemit i forkant for overlevering av personopplysninger som skal forvaltes på vegne av virksomheten.

Hemit skal sikre tilstrekkelig åpenhet rundt informasjonssikkerhet slik at helseforetakene kan ivareta sitt ansvar.

Ved avvik skal Hemit varsle dataansvarlig i henhold til databehandleravtale og tjenesteavtaler.

Hemit skal ha myndighet til å gjennomføre nødvendige tiltak for å sikre infrastrukturen ved sikkerhetshendelser. Beslutningsprosess og varsling for slike tiltak skal være beskrevet i tjenesteavtalen og beredskapsplaner.

Hemit skal ha myndighet til å avvise implementering/oppstart av systemer eller utstyr som medfører uakseptabel risiko for andre virksomheter i foretaksgruppen. Beslutningsprosess for en slik vurdering, skal være beskrevet i tjenesteavtalen.

5.1.4 Helseplattformen AS sitt ansvar

Helseplattformen AS skal ha et forsvarlig styringssystem for informasjonssikkerhet som er i henhold til krav i lov og forskrift, Normen og ISO 27001, som minimum tilfredsstiller kravene stilt i styringssystem for informasjonssikkerhet og personvern i Helse Midt-Norge

Helseplattformen AS skal sikre tilstrekkelig åpenhet rundt informasjonssikkerhet slik at kundene kan ivareta sitt ansvar.

5.2 Roller og ansvar for informasjonssikkerhet og personvern i Helse Midt-Norge

Nedenfor er beskrevet roller og ansvar knyttet til informasjonssikkerhet og personvern i virksomhetene i Helse Midt-Norge. En virksomhet kan velge å navngi rollene annerledes, men alt ansvar beskrevet for de ulike rollene skal være dekket.

En person kan inneha flere roller. F.eks. vil Administrerende direktør også ha rollene leder og medarbeider.

Oppgaver som følger av roller og ansvar i dette dokumentet beskrives på et lavere nivå i dokumentasjonen av styringssystemet.

5.2.1 Administrerende direktør

Administrerende direktør for helseforetakene og Helse Midt-Norge RHF har følgende ansvar:

- Er ansvarlig for at kravene i Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge blir implementert og etterleves i virksomheten
- Har det øverste ansvar for databehandling i virksomheten, herunder ansvarlig for å bestemme formålet med databehandlingene og ha dokumentert oversikt over disse.
- Gi de nødvendige føringer for krav og innhold i styringssystemet for informasjonssikkerhet og personvern, samt ha ansvaret for at dette blir implementert, vedlikeholdt og fulgt opp på en systematisk og tilstrekkelig måte i hele virksomheten.
- Har ansvar for organiseringen av sikkerhetsarbeidet. Herunder sørge for å etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse på informasjonssikkerhet og personvern til å gjennomføre nødvendige oppgaver for å ivareta ansvaret
- Har ansvaret for at det finnes oppdaterte prosedyrer for tilgang til helse- og personopplysninger
- Er ansvarlig for at virksomhetsledelsens gjennomgang gjennomføres minst årlig
- Har ansvar for vurdering av risiko og for aksept av risiko
- Er ansvarlig for at det inngås skriftlige avtaler med IKT-leverandør/ databehandler med krav til sikkerhetsnivå, tjenestenivå og forvaltning
- Er ansvarlig for at det utvikles handlingsplaner som sørger for kontinuerlig arbeid med sikkerhetskultur og opplæring innen informasjonssikkerhet og personvern.

5.2.2 Leder

Leder i denne sammenheng er ledere på alle nivåer i Helse Midt-Norge som er ansvarlig for å følge opp arbeidet med informasjonssikkerhet og personvern innenfor sine ansvarsområder, på lik linje med øvrig arbeid de som ledere er ansvarlige for.

Enhver leder er ansvarlig for å bidra til en god informasjonssikkerhetskultur gjennom at regler for informasjonssikkerhet og bestemmelser i styringssystemet følges innen eget ansvarsområde. Ledere på alle nivå må minst en gang årlig systematisk vurdere status på informasjonssikkerhetsarbeidet innenfor sine ansvarsområder.

Innenfor eget ansvarsområde, og der det er relevant, er ledere også ansvarlig for følgende:

- Gjennomføring av tilstrekkelig sikkerhetsopplæring av eget og innleid personell, slik at disse kan ivareta sitt ansvar som hører til sin rolle. Sikkerhetsinstruks skal som et minimum legges til grunn for denne opplæringen
- Å innhente taushetserklæringer for alle ansatte og innleid personell som ikke har dette regulert i lov, og påser at disse er kjent med og etterlever styrende dokumenter som regulerer brukeratferd

- Tildele og kontrollere personellets tilgang til informasjon og tjenester etter fastsatt tilgangsregime, herunder avdekke uautorisert tilgang.
- Ved behov for registre og øvrige databehandlinger innenfor eget ansvarsområde, påse at nødvendige interne og eventuelt eksterne godkjenninger er innhentet i henhold til virksomhetens interne retningslinjer
- For resultater, fremdrift og rapportering av sikkerhetsarbeidet innen eget ansvarsområde
- For at kontinuitetsplaner ved bortfall av informasjonssystemer finnes
- For risiko knyttet til sitt ansvarsområde. Herunder sørge for at nødvendige risikovurderinger gjennomføres og at identifiserte risikoer håndteres, blant annet ved at tiltak iverksettes.
- For at avvik håndteres iht. virksomhetens avviksrutiner

Dersom leder innen sitt ansvarsområde, beslutter ny eller endret behandling av personopplysninger, gjelder også følgende:

- Skal sørge for at DPIA (personvernkonsekvensvurdering) gjennomføres når dette er nødvendig i samsvar med personopplysningsloven ved ny eller endret behandling av personopplysninger
- Er ansvarlig for at all behandling av personopplysninger utføres iht. krav til innebygd personvern og personvern som standardinnstilling
- Følge virksomhetens øvrige føringer ved slike endringer.

5.2.3 Medarbeider

Med **medarbeider** menes alle som behandler eller forvalter informasjon som ansatt eller på oppdrag for Helse Midt-Norge. Den enkelte medarbeider er ansvarlig for å:

- Følge virksomhetens sikkerhetsbestemmelser inkludert Sikkerhetsinstruksen og personvernerklæringen, og bidra til en god sikkerhetskultur.
- Ha en forståelse av hva som er forventet av dem (adferd). For medarbeidere som skal ha tilgang til taushetsbelagte opplysninger, skal også grunnlag og hjemmel for oppslag i de taushetsbelagte opplysningene være forstått
- Gjennomføre opplæringsplan for fagområde informasjonssikkerhet og personvern i kompetanseportal. Søke informasjon internt ved usikkerhet eller tvil
- Bidra til forbedringsprosesser ved å gi tilbakemeldinger/foreslå endringer til styringssystemet.
- Forhindre og/eller rapportere avvik til nærmeste leder når disse oppstår, eventuelt til informasjonssikkerhetsleder og/eller personvernombud i henhold til virksomhetens avviksrutiner

5.2.4 Systemeier

Systemeier er en ansatt med særskilt ansvar for et gitt IKT-system. Hvert system har én systemeier ved hvert HF. Systemeier skal inngå i endringsstyringsprosessen hos IKT-leverandør/databehandler

Systemeier har ansvar for:

- at systemet oppfyller lovbestemte krav til tilgjengelighet, konfidensialitet, integritet og robusthet for sitt system. Dette innebærer å sørge for at systemet tilrettelegger for at all behandling av informasjon i systemet kan utføres i henhold til gjeldende krav til personvern, håndtering av avvik knyttet til systemet, og definering av tilgangsroller.
- vurdere behovet for DPIA for sitt system, og gjennomføre denne når nødvendig.
- risiko knyttet til sitt system, herunder sørge for at nødvendige risikovurderinger gjennomføres og at identifiserte risikoer håndteres, blant annet ved at tiltak iverksettes.
- å inkludere alle systemeiere for systemet i risikovurderingsarbeid og andre internkontrollaktiviteter dersom systemet er et fellessystem
- at avvik relatert til systemet håndteres iht. virksomhetens avviksrutiner
- å holde seg oppdatert på nye versjoner av systemet, sørge for at de blir risikovurdert og implementert etter behov, og samtidig beslutte gjennomføring av endringer for sitt system
- å utarbeide og inngå databehandleravtale for tjenester som faller utenfor tjenesteavtalen med Hemit

5.2.5 Informasjonssikkerhetsleder

Informasjonssikkerhetsleder eller tilsvarende rolle (eks. CISO, osv.) har som hovedansvar å være pådriver og støtte til ledelsen og organisasjonen for øvrig i informasjonssikkerhetsarbeidet. Informasjonssikkerhetsleder må ikke være begrenset av plassering i organisasjonen med hensyn til sine oppgaver. Informasjonssikkerhetsleder skal være en nøkkelressurs i virksomhetens kontinuerlige internkontrollarbeid på informasjonssikkerhetsområdet, blant annet ved å iverksette og bistå i arbeidet med risikovurdering og -håndtering, og måling, evaluering og revisjon.

Informasjonssikkerhetsleder har ansvar for:

- at det utarbeides styrende, utførende og kontrollerende dokumenter i styringssystem for informasjonssikkerhet og personvern som bidrar til å sikre etterlevelse av vedtatte mål og strategier.
- forvaltningen av de overordnede styrende dokumenter innen ansvarsområdet
- faglig rapportering til virksomhetens ledelse innen sitt fagområde
- å kartlegge behov for, og bidra til, opplæring og bevisstgjøringsaktiviteter innen informasjonssikkerhet i virksomheten.
- å påse utvikling og vedlikehold av beredskaps-/varslingsplaner (katastrofeplan), samt kontinuitetsplaner relatert til Informasjonssikkerhet i IKT systemene
- å vurdere om nye løsninger eller endringer er innenfor akseptabelt risikonivå.
- å stille krav til, og følge opp iverksettelse av, sikkerhetstiltak innenfor det samlede IKT-området

- å påse at avvikshåndtering, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, og om nødvendig å gi pålegg om endring
- å lage årlige revisjonsplaner og sikre gjennomføring av sikkerhetsrevisjoner i virksomheten, samt rapportere planer og resultater gjennom virksomhetens etablerte kanaler for øvrig revisjonsaktivitet

5.2.6 IKT Leder

IKT-leder eller tilsvarende roller (eks. IKT Sjef, IKT Direktør el.) har ansvar for IKT i egen virksomhet. IKT-leder har ansvar for å inngå og forvalte avtaler med leverandører (Hemit HF, Helseplattformen AS og andre).

IKT-leder har ansvar for å følge opp avtalte krav med leverandørene og derigjennom sikre at leverandøren oppfyller virksomhetens krav til informasjonssikkerhet og personvern.

5.2.7 Personvernombud

Personvernforordningens artikkel 37 nr. 1 pålegger virksomhetene i Helse Midt-Norge å utpeke personvernombud (PVO). PVO skal utpekes på grunnlag av faglig kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området, i tillegg til evne til å utføre oppgavene. PVO må være uavhengig, dvs. ikke kunne instrueres om utførelsen av sine oppgaver i organisasjonen. PVO skal bidra med råd slik at virksomheten overholder personvernregelverket og kontrollere etterlevelsen av regelverket.

5.3 Regional samhandling

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.

5.3.1 Regional ledergruppe for informasjonssikkerhet og personvern

Regional ledergruppe for informasjonssikkerhet og personvern er et fagnettverk på direktørnivå som har fått sitt mandat fra Direktørmøtet.

Gruppen skal, i samarbeid med Regionalt informasjonssikkerhetsforum (RIF), bidra til regional samordning og utvikling innenfor informasjonssikkerhet og personvern i Helse Midt-Norge.

5.3.2 Regionalt informasjonssikkerhetsforum

Regionalt informasjonssikkerhetsforum (RIF) er et regionalt fagforum for informasjonssikkerhet og personvern. RIFs formål, ansvar og oppgaver er beskrevet i Mandat for Regionalt forum for informasjonssikkerhet som er vedlagt dette dokumentet.

6 Relaterte dokumenter

- Mål og strategi for informasjonssikkerhet og personvern i Helse Midt-Norge
- Mandat for Regionalt forum for informasjonssikkerhet (RIF)
- Mandat for Regional ledergruppe for informasjonssikkerhet og personvern