Retningslinjer for trygg bruk av KI i Helse Midt-Norge

Hurtigguide

Retningslinjene for trygg bruk av KI gjelder for alle ansatte i Helse Midt-Norge.

- **Effektivisering av drift:** KI gir muligheter for å forbedre driften og automatisere rutineoppgaver.
- **Lovlig og etisk bruk:** Bruken av KI skal være lovlig, ansvarlig, sikker, etisk og transparent.
- **Ansvar for ansatte:** Alle ansatte må sikre at deres bruk av KI er i tråd med retningslinjene.
- **Lederes ansvar:** Ledere skal gjøre retningslinjene kjent for ansatte og sørge for nødvendig opplæring, samt følge opp etterlevelse.
- **Definisjoner av KI:** Kunstig intelligens refererer til datasystemers evne til å utføre oppgaver som krever menneskelig intelligens.
- **Bruk av åpne kilder:** Bruk av åpne kilder må brukes særskilt varsomt, enkle søk gjennom nettleser er ok, personopplysninger skal ikke lastes opp.
- **Styringssystem og juridiske hensyn:** Regionalt styringssystemer for informasjonssikkerhet og personvern skal følges. KI-bruk må følge relevante lover og forskrifter, inkludert personvernlovgivning.

Bruk KI som et godt hjelpemiddel, men vær varsom og kritisk

KI-løsninger kan gi svar som virker overbevisende, men som ved nærmere undersøkelse viser seg å være unøyaktige, misvisende og i noen tilfeller usanne. Svarene KI gir skal aldri være er en erstatning for faglig skjønn eller klinisk vurdering. Selskapene som tilbyr slike tjenester, fraskriver seg uttrykkelig ethvert ansvar for svarene som gis i sine vilkår for bruk. Vær kritisk til svarene som gis av KI-løsninger.

Vær varsom rådene nedenfor gjelder generelle KI-tjenester som er åpent tilgjengelig på internett.

Du skal alltid

- huske at du er ansvarlig for KI-generert tekst du står som avsender av, eller publiserer
- se opp for unøyaktigheter, skjevheter og feilaktig informasjon
- være kritisk til om KI bryter opphavsrett, særlig for tredjepart
- tydelig merke innhold av type illustrasjoner og bilder som du har brukt generativ KI til å lage. For eksempel “Denne illustrasjonen er laget ved hjelp av KI”, i tillegg til kreditering av KI-tjenesten du har brukt
- være transparent og si fra om når du bruker en KI-generert tekst, bilde, kode eller annet

Du skal ikke

- dele sensitiv informasjon, som personopplysninger eller virksomhetskritisk informasjon
- dele brukerinformasjon, som påloggingsinformasjon og passord
- lime inn interne eller sensitive dokumenter eller utklipp fra disse
- stole på at KI sier sannheten – sjekk alltid fakta
- bruke kun KI til å ta beslutninger (spesielt ikke når det påvirker individer eller grupper av individer)

Formål med retningslinjene

Kunstig intelligens (KI) gir oss nye muligheter for å effektivisere vår drift, automatisere rutinemessige oppgaver og forbedre våre tjenester. Utviklingen innen KI skjer svært raskt. Det er viktig at vi sørger for at vi bruker KI på en lovlig, ansvarlig, sikker, etisk og transparent måte.

Helse Midt-Norge ønsker å legge til rette for bruk av relevante KI-verktøy. Vår intensjon er å tilgjengeliggjøre risikovurderte KI-løsninger som er godkjent for visse typer bruk. I de tilfeller der godkjente løsninger ikke dekker behovene, kan det i noen tilfeller være formålstjenlig å benytte åpne kilder. KI kan være en fremmed teknologi for mange. Det er derfor viktig at vi har åpenhet rundt hvor, hvordan og hvorfor KI benyttes i Helse Midt-Norge.

Retningslinjene er utarbeidet for å understøtte ambisjonsnivå for bruk av KI i HMN.

Generelle retningslinjer for bruk av KI

For all bruk av KI skal Regionalt styringssystem for informasjonssikkerhet og personvern, samt eget foretaks interne styringssystem for informasjonssikkerhet og personvern følges.

Alle som tar i bruk KI, har ansvar for at det gjøres i tråd med gjeldende lover og regler.

Når man benytter KI-generert innhold, skal man alltid ta stilling til om innholdet skal merkes, for eksempel ved bruk av KI-genererte bilder. Merking skal bidra til åpenhet og bevisstgjøring rundt bruk av KI.

Generelt skal man:

- Være kritisk til informasjon generert av KI.
- Alltid kvalitetssikre informasjon fra KI før du bruker informasjonen, dette gjelder særlig ved generativ KI. Det er særlig viktig å være bevisst på at koder og annen informasjon generert av KI kan inneholde logikkfeil eller andre sårbarheter.
- Du skal aldri stole blindt på at informasjon fra KI er korrekt, du må alltid faktasjekke opplysningene.
- Ved anskaffelse av MTU KI verktøy må gjeldende anskaffelsesprosedyre for KI følges.

Systemeiere må være særlig observante på oppdateringer som inneholder KI løsninger og sørge for at det utføres nødvendig testing og risikovurderinger før det åpnes for bruk.

Bruk av godkjente KI-løsninger

Med godkjent programvare med KI menes programvare som er risikovurdert og godkjent av Helse Midt-Norge og tilgjengeliggjort for deg via din arbeidsflate.

KI skal kun brukes til det formål det i Helse Midt-Norge er godkjent for. Enhver bruk til andre formål må kartlegges og godkjennes.

Dersom du bruker KI til å behandle personopplysninger, har du ansvar for å sørge for at behandlingen er i tråd med personvernregelverket. Du må særlig være oppmerksom på at du ikke bruker personopplysninger til andre formål enn det de er samlet inn for.

Det er ikke tillatt å benytte informasjon som er klassifisert som strengt fortrolig (Nivå 4 svart) i programvare som benytter KI, se «Krav og retningslinjer for klassifisering av informasjon i Helse Midt-Norge».

Bruk av KI kan medføre etiske utfordringer. Den som benytter KI i Helse Midt-Norge har ansvar for at sin bruk ikke er i strid med grunnleggende menneskerettigheter og «Dokument «Etiske retningslinjer Helse Midt-Norge», ID 874 - EQS».

Bruk av åpne kilder

Primært skal du kun benytte KI som er godkjent av Helse Midt-Norge og tilgjengelig via din arbeidsflate. Hvis du ikke får behovet dekt gjennom godkjent programvare, kan begrenset bruk av åpne kilder godtas. Retningslinjene under må da følges:

- Du **kan** bruke åpne kilder via nettleser til enkle søk, for eksempel på samme måte som du bruker Google og andre søkemotorer
- Du skal aldri laste opp **personopplysninger** i åpne kilder, brudd på dette er å anse som brudd på din taushetsplikt og personvernregler
- Du skal aldri dele **taushetsbelagt informasjon** eller informasjon som er klassifisert som «fortrolig» eller «strengt fortrolig» (nivå 3 og 4 i «Krav og retningslinjer for klassifisering av informasjon i Helse Midt-Norge» i åpne kilder. Deling i strid med dette er et brudd på din taushetsplikt.
- Du skal aldri dele påloggingsinformasjon
- Dersom du ønsker å opprette bruker på KI-tjenester som er tilgjengelig via åpne kilder, skal du ikke benytte din Helse Midt-Norge e-postadresse med mindre dette på forhånd er avklart med nærmeste leder.
- Har du behov for å laste ned KI-løsninger som ikke er tilgjengelig i arbeidsflaten, skal du avklare dette med nærmeste leder. Ved tvil skal nærmeste leder søke veiledning hos Hemit.

KI-løsninger som ikke skal brukes

Av sikkerhetsmessige årsaker er det noen KI-løsninger som ikke skal brukes. Disse vil bli sperret slik at de ikke er tilgjengelig via arbeidsflaten. Ansatte skal ikke legge opplysninger knyttet til Helse Midt-Norge eller Helse Midt-Norge inn i slike KI-løsninger, selv om de bruker private enheter.

Et eksempel på en KI-løsning som ikke skal brukes er Deepseek, som også er sperret for bruk på arbeidsflaten. Årsaken til dette er at den personlige informasjon samles inn og lagres på servere i Kina og kinesiske virksomheter plikter å samarbeide med og utlevere informasjon til kinesiske etterretningstjenester og myndigheter.

Av sikkerhetsmessige årsaker frarådes ansatte å bruke slike KI-løsninger også privat.

Spesifikt om retningslinjer for bruk av KI til klinisk bruk

KI vil kunne kategoriseres som medisinsk utstyr dersom det er ment å skulle brukes på mennesker i den hensikt å bidra til diagnostisering, forebygging, overvåking, prediksjon, prognostisering, behandling eller lindring av sykdom.

Helsedirektoratet har i sitt Regelverk for bruk av KI-systemer presisert at hvis det tiltenkte formålet er medisinsk, gjelder følgende:

- KI-systemet betraktes som medisinsk utstyr og virksomheten må bruke et CE-merket utstyr. Utstyret må oppfylle dokumentasjonskravene i Lov om medisinsk utstyr.
- KI-systemet vil i utgangspunktet betraktes som høyrisikosystem i henhold til KI-forordningen og må oppfylle kravene som stilles til disse systemene når den trer i kraft.

Denne type KI-systemer må dermed oppfylle to regulativer, både MDR og KI-forordningen for å kunne bli CE-merket og godkjent for bruk. Begge disse stiller tydelige krav til hele livsløpet til et KI-system. KI til pasientbehandling må dokumenteres som effektiv og trygg gjennom kliniske studier, følgeforskning eller prosesskontroll under utprøving og implementering.

Risikoanalyser skal gjøres i det enkelte implementeringsløp i tråd med regionalt rammeverk for risikovurderinger.

Alle anskaffelser av denne type KI må følge samme rutiner som øvrig anskaffelse av medisinsk teknisk utstyr.

Personvern

Bruk av KI kan, om det ikke brukes riktig, utfordre personvernet. Ved bruk av KI må alle ansatte være ekstra varsomme med å overholde kravene til personvern. Det er særlig stor risiko for såkalt formålsutglidning. Med det menes at personopplysninger blir brukt til flere formål enn det som Helse Midt-Norge tidligere har bestemt at de skal brukes til. Ved bruk av personopplysninger i KI-løsninger, er det derfor svært viktig å være bevisste på at personopplysningene kun brukes i tråd med opprinnelig formål. Ved tvil, kan personvernombudet kontaktes for rådgivning. All bruk av KI må skje i tråd med gjeldende krav og retningslinjer i Helse Midt-Norge for personvern.

Bruk av data

Utvikling av KI forutsetter ofte store mengder data. Det generelle utgangspunktet er at data som ikke er underlagt begrensninger fritt kan benyttes. Mange typer data er imidlertid regulert på en slik måte at bruken av dem er begrenset. I noen sammenhenger kan dette bety at det ikke er lov å bruke dataene. I andre sammenhenger kan dette bety at dataene kan brukes, men at flere vilkår må være oppfylt.

Du bør ære oppmerksom på følgende rammer for bruk av data:

- Immaterielle begrensninger: Data har en verdi. Derfor kan det være ulike rettigheter som gjør at bruk av dataene er begrenset, eksempelvis opphavsrett.
- Taushetsbelagt informasjon: Informasjon som gis til en person som har taushetsplikt vil være taushetsbelagt. Denne typen informasjon kan ikke deles eller brukes på en måte som er uforenelig med taushetsplikten.
- Personopplysninger: Behandling av personopplysninger er grundig regulert, og personopplysningsbegrepet er nokså vidt. Med mindre du er sikker på at KI-systemet ikke behandler personopplysninger, bør du vurdere se nærmere på hva som ligger i personopplysningsbegrepet og hvilke krav du eventuelt må etterleve.
- Gradert informasjon: Visse typer informasjon er begrenset av sikkerhetsmessige hensyn. Det er strenge krav til hvordan slik informasjon skal håndteres. Digitaliseringsdirektoratet anbefaler at du ikke benytter gradert informasjon til utvikling eller bruk av KI-løsninger med mindre du er sikker på at alle krav er ivaretatt.

Risikovurderinger av KI-løsninger

Alle initiativ i Helse Midt-Norge som har til hensikt å anskaffe, etablere, utvikle, eller integrere mot KI-løsninger skal gjennomføre risikovurderinger før tjenesten tas i bruk. Ved usikkerhet, eller spørsmål rundt dette ta kontakt med informasjonssikkerhetsansvarlig eller informasjonssikkerhetsrådgiver ved ditt foretak. Dette gjelder også dersom en eksisterende KI-løsning skal benyttes til et annet formål enn det opprinnelige.

Vedlegg – utdypende informasjon

Definisjoner

Kunstig intelligens (KI):
Refererer til datasystemers evne til å utføre oppgaver som vanligvis krever menneskelig intelligens. Dette kan inkludere problemløsning, mønstergjenkjenning, språkforståelse, beslutningstaking og læring. KI kan deles inn i flere underområder:

Generativ KI:

Er en gren av KI som bruker generative modeller for å produsere tekst, bilder, videoer og andre former for data. Disse modellene lærer de underliggende mønstrene og strukturene i treningsdataene sine og bruker denne kunnskapen til å generere nytt innhold basert på input, ofte i form av naturlige språkspørsmål. Eksempler på dette er Copilot og DALL-E.

Generativ KI bruker avanserte teknikker innen maskinlæring, spesielt dype nevrale nettverk som transformatorer og store språkmodeller (LLMs). Disse modellene trenes på store mengder data for å forstå og etterligne de komplekse mønstrene i dataene.

Bruksområder

Generativ KI kan benyttes av flere fagområder:

- **Helsevesen:** Generere medisinske bilder og hjelpe til med diagnose.
- **Økonomi:** Lage økonomiske modeller og forutsi markedsbevegelser.
- **Kommunikasjon:** Skape medieinnhold

Maskinlæring (ML):
Er en underkategori av KI som fokuserer på å utvikle algoritmer og modeller som gjør at datamaskiner kan lære fra og gjøre forutsigelser eller beslutninger basert på data. I stedet for å bli eksplisitt programmert for hver oppgave (regelbasert automatisering), bruker maskinlæring mønstre og innsikt fra data for å forbedre ytelsen over tid.

Dype læringsmodeller og nevrale nettverk
Er inspirert av den menneskelige hjernen, og består av lag med noder (nevroner) som kan lære komplekse mønstre i data. Dyp læring bruker nevrale nettverk med mange lag for å modellere komplekse data som bilder, lyd og tekst.
Eksempler på bruk:

- Medisinsk bildediagnostikk: Analyserer medisinske bilder for å identifisere sykdommer som kreft og hjerneslag.
- Genomikk og personlig medisin: Analyserer genetiske data for å identifisere mutasjoner og forstå deres sammenheng med sykdommer.
- Elektroniske pasientjournaler (EPJ): Analyserer data for å forutsi sykdomsforløp og hjelpe leger med behandlingsbeslutninger.

Åpne kilder:
Med åpne kilder menes tjenester for KI som er åpent tilgjengelig på internett. Disse er ofte gratis og lett tilgjengelig i nettleser, da dataen som legges inn i tjenesten brukes for å videreutvikle produktet. Det er viktig å være klar over at verken brukeren eller Helse Midt-Norge har kontroll over informasjon som er lagt inn i åpne kilder. Bruk må da skje med stor varsomhet.

Regelverk

KI som fagområde utvikler seg raskt og det regulatoriske landskapet er også i bevegelse. AI Act (forordning (EU) nr. 2024/1689 ("KI-forordningen") trådte i kraft i EU 1. august. De fleste av de betydeligste kravene i regelverket gjelder fra august 2026 og det ventes at forordningen trer i kraft i Norge samme år. Ved anskaffelser av KI-løsninger i Helse Midt-Norge kravstiller vi allerede i henhold til krav i KI-forordningen. Det er god praksis å se til forordningen både ved bruk og utvikling av KI-løsninger. KI-forordningen deler risikoprofilene for KI-løsninger. Risikoprofilen har stor betydning for hvordan en KI-løsning kan utvikles, brukes og overvåkes.

Blant annet personvernlovgivningen, likestillings- og diskrimineringsloven, regler om opphavsrett, og sektorspesifikk lovgivning tilknyttet helserett gjør seg gjeldende ved bruk og utvikling av KI-løsninger.

Kilder

Helse Midt-Norge har hentet god inspirasjon fra Sykehuspartners veileder for ansvarlig bruk av KI, Helse Nords retningslinjer for bruk og utvikling av kunstig intelligens (KI) i Helse Nord, Kunstig intelligens ved St. Olavs hospital, Strategi for utvikling og bruk, samt Om bruk av generativ KI Helse Vest.

Referanser

Referanse til et bredt spekter av retningslinjer og forskrifter sørger for at utviklingen og bruken av KI i Helse Midt-Norge skjer i tråd med beste praksis og gjeldende regelverk. Dette omfatter blant annet:

- KI-forordning
- Datatilsynet retningslinje til personvern
- Krav og retningslinjer for klassifisering av informasjon i Helse Midt-Norge
- Dokument «Etiske retningslinjer Helse Midt-Norge», ID 874 - EQS
- Artikkel 2 i MDR