1 HENSIKT

Styringssystemet for informasjonssikkerhet gjelder all informasjonsbehandling som skjer i Helse Nord[1]. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-verktøy er også inkludert.

Formålet med dokumentet er å beskrive sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet, og er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Styringssystemet skal sikre at administrerendedirektør (dataansvarlig) i alle helseforetak etablerer nødvendige krav, operative retningslinjer og prosedyrer. Dette innebærer å organisere virksomheten slik at lovpålagte plikter, pasienters og andre registrertes rettigheter etterleves. Styringssystemet skal også tydeliggjøre ansvars- og myndighetsforholdene mellom helseforetakene, Helse Nord IKT HF og Helse Nord RHF.

Lovkravene omfatter å

- Bestemme formålet med databehandlingen av helse- og personopplysningene
- Prioritere og gjennomføre nødvendige sikkerhetstiltak
- Ha kontroll på risiko, også ved endringer
- Normalisere sikkerhetshendelser koordinert og effektivt

Figur 1 Nivåene i Helse Nords styringssystem for informasjonssikkerhet

[1] Med Helse Nord menes hele foretaksgruppen med alle helseforetakene og det regionale helseforetaket.

2 SIKKERHETSMÅL

Helse Nord har som målsetning å bli ledende i landet på å ta i bruk informasjonsteknologi som verktøy for å bedre tilgjengelighet, arbeidsflyt, samarbeid og effektivitet[2]. Samtidig skal pasienter og helsepersonell ha trygghet for at informasjonssikkerheten og de registrertes rettigheter blir ivaretatt. For å nå målsetningen settes følgende sikkerhetsmål:

1. Helse Nord skal sørge for at helsepersonell og pasienter har enkel og sikker tilgang til pasient- og helseopplysninger for å sikre god og effektiv pasientbehandling.
2. Helse Nord skal legge til rette for sikker behandling av helse- og personopplysninger og annen data til forskning, utdanning, kvalitetsforbedring og opplæring.
3. Helse Nord skal ivareta den registrertes rettigheter (innsyn, informasjon om hvordan opplysningene behandles, sperring, retting og sletting).
4. Infrastruktur, IKT-systemer og utstyr skal beskyttes på en slik måte at tjenestene er tilgjengelige, informasjon ikke går tapt, blir feilaktig endret eller eksponert for uvedkommende. Nivået på beskyttelsestiltakene skal være tilpasset viktigheten av informasjonen som behandles.

3 SIKKERHETSSTRATEGI

For å nå sikkerhetsmålene skal følgende strategi legges til grunn:

1. Gjeldende regelverk og Norm for informasjonssikkerhet i helse- og omsorgstjenesten skal følges.
2. Helse Nord skal følge regionale sikkerhetsmål, sikkerhetsstrategi, retningslinjer, prosedyrer og prosesser for å oppnå tilfredsstillende informasjonssikkerhet
3. Ansvar og myndighet for informasjonssikkerhet skal følge det ordinære linjeansvaret.
4. Alle systemer, enheter og applikasjoner som tilknyttes Helse Nord sin infrastruktur skal følge sikkerhetskravene som er beskrevet i regionalt styringssystem for informasjonssikkerhet.
5. Ledelsens gjennomgang skal gjennomføres årlig og gi nødvendige sikkerhetstiltak tilstrekkelig prioritet.
6. Risikostyring gjennom identifisering, vurdering og håndtering av sikkerhetsrisiko skal ivaretas gjennom kontinuerlig og planlagt arbeid (årshjul).
7. Informasjonssikkerhet og personvern skal være innebygd og innarbeidet i virksomhetsstyring, prosesser og IKT-løsningers livssyklus (etablering, endring og utfasing).
8. Alle tilganger som gis i Helse Nord skal bygge på prinsippet om tjenstlig behov
9. Før endringer som kan medføre økt risiko for tap av, feil i eller uønsket eksponering av data gjennomføres, skal endringen risikovurderes. Håndteringen av avdekkede risikoer skal være koordinert og planlagt.
10. Sikkerhetshendelser skal avdekkes og raskt normaliseres, og konsekvenser av hendelsene skal reduseres.
11. Individuelle kompetanseplaner skal omfatte kontinuerlig kompetansebygging innen informasjonssikkerhet tilpasset den enkeltes roller, ansvar og arbeidsoppgaver.

[2] Kilde: Helse Nord strategi, under informasjonsteknologi og telemedisin

4 ANSVAR OG MYNDIGHET FOR INFORMASJONSSIKKERHET I HELSE NORD

Administrerende direktører har ansvar og myndighet for informasjonssikkerhet. Arbeidsoppgaver kan delegeres.

Administrerende direktør Helse Nord RHF
Administrerende direktør for Helse Nord RHF skal sørge for tilfredsstillende informasjonssikkerhet i Helse Nord, og sikre etterlevelse av sikkerhetsmål og sikkerhetsstrategi. Administrerende direktør skal etablere og forvalte regionale sikkerhetskrav beskrevet i regionalt styringssystem for informasjonssikkerhet, hvor Helse Nord RHF er dokumentgodkjenner.
For enkelte løsninger eller tjenester er Helse Nord RHF databehandler for helseforetakene. Dette er beskrevet i egne databehandleravtaler.

Administrerende direktør helseforetak
Administrerende direktør for helseforetakene er dataansvarlig for all databehandling av helse- og personopplysninger i egen virksomhet, herunder for felles kliniske systemer med delt dataansvar.

Administrerende direktør skal sikre etterlevelse av sikkerhetsmål og sikkerhetsstrategi gjennom:

- organisering av informasjonssikkerhetsarbeidet
- tildeling av tilstrekkelige ressurser for å ivareta informasjonssikkerhetsansvaret
- å gjennomføre ledelsens årlige gjennomgang av informasjonssikkerheten i virksomheten
- prioritering og iverksetting av nødvendige sikkerhetstiltak
- revisjoner og kontrollhandlinger
- fastsette akseptabelt risikonivå for informasjonssikkerhet

Noen av helseforetakene er i enkelte tilfeller databehandler for helseforetakene, eller det regionale helseforetaket. Dette er beskrevet i egne databehandleravtaler.

Administrerende direktør Helse Nord IKT HF
Helse Nord IKT leverer teknologiske løsninger og tjenester til sykehusene i Nordland, Troms og Finnmark. Administrerende direktør for Helse Nord IKT er databehandler for disse løsningene og tjenestene, og skal oppfylle krav i lov og forskrift, regionalt styringssystem for informasjonssikkerhet og databehandleravtaler.
I tillegg til å sikre etterlevelse av sikkerhetsmål og sikkerhetsstrategi i egen virksomhet, har administrerende direktør i Helse Nord IKT HF et særskilt ansvar for å:

- etablere og forvalte regionale sikkerhetskrav til regional infrastruktur, og krav til systemer, enheter og applikasjoner som tilknyttes denne. Sikkerhetskravene er beskrevet i regionalt styringssystem for informasjonssikkerhet, hvor Helse Nord IKT er dokumentgodkjenner.

Styret
Styret har ansvar for at foretakets samlede virksomhet er tilfredsstillende organisert. Styret skal holde seg orientert om foretakets virksomhet og økonomiske stilling. Det skal føre tilsyn med at virksomheten drives i samsvar med fastsatte mål. For øvrig vises det til helseforetaksloven kapittel 7.

Medarbeider

Den enkelte medarbeider har et selvstendig ansvar for informasjonssikkerheten i Helse Nord, ut fra de særskilte oppgaver og myndighet som tillegger stillingen.

Endringslogg

Versjon	*Dato*	*Endringer*	*Utført av*	*Godkjent av*
1.0	4.10.2017	Dokumentet behandlet i Direktørmøtet	Ida Martinussen	
1.1	29.9.2018	Oppdatert i henhold til ny terminologi etter personvernforordningen Tydeliggjort Helse Nord RHF ansvar Tydeliggjort styrenes ansvar Tydeliggjort hvem som kan være databehandler	Ida Martinussen	
1.2	27.11.2018	Presisert begrepet sikkerhetskrav, i sikkerhetsstrategi og under Helse Nord IKT HF sitt ansvar. Presisering av Helse Nord RHF sitt ansvar vedrørende etablere og forvalte regionale sikkerhetskrav.	Ida Martinussen	