NORDLANDSSYKEHUSET
NORDLÁNDA SKIPPIJVIESSO

Direktøren

Styresak 048-2019
Orienteringssak - Informasjonssikkerhet pr mai 2019

Saksbehandler:	Alisa Larsen
Dato dok:	06.05.2019
Møtedato:	21.05.2019
Vår ref:	2019/3236

Vedlegg (t): Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet
Styring av informasjonssikkerhet

Innstilling til vedtak:
Styret tar saken til orientering

Bakgrunn:

- Oppdragsdokument for 2019 stiller krav om at foretakene skal styrebehandle status på risiko- og sårbarhetsanalyser om informasjonssikkerhet innen 1. juni 2019, jf punkt 4.2.2.
- Brev fra Helse Nord datert 05.11.2018 «Regionalt styringssystem for informasjonssikkerhet, revisjon», punkt 8 «Helse Nord RHF anbefaler at styringssystemet legges frem for styrene i helseforetakene»
- Styresak 037-2018 – Styret ber om å bli presentert en redegjørelse for fjernlagerløsningen jf. 107-2017 ved neste statusrapportering til styret om informasjonssikkerhet.

Beskrivelse:
Som rapportert i styresak juni 2018, ble det gjennomført ROS-analyser av alle de store kliniske systemene og medisinsk utstyr i perioden 2016-2018.

Personvernlovgivningen stiller krav om at risiko vurderes før en løsning som behandler personopplysninger tas i bruk. Samme krav gjelder dersom bruken av personopplysninger endres. På den bakgrunn gjennomføres det nå risikovurderinger løpende ved innføring av nye løsninger eller ved endringer.

Det er utviklet et elektronisk verktøy for innmelding av nye løsninger eller prosjekter når dette behandler personopplysninger. Det elektroniske meldeskjemaet har blant annet forenklet prosessen for prosjektledere som skal igangsette arbeid som involverer personopplysninger. I tillegg bidrar det elektroniske meldeskjemaet til at Nordlandssykehuset ivaretar andre krav i personvernregelverket, herunder å påse at bruken av personopplysningene er lovlig og å holde oversikt over måten vi bruker personopplysninger på. Dette elektroniske verktøyet bidrar til å holde oversikt over alle løsninger vi har samt tilknyttede risikovurderinger. Verktøyet er utarbeidet slik at selve risikovurderingen da kan gjøres på hver løsning, og gi indikasjon på risikobildet.

Resultater fra risikovurderingene som er gjennomført viser at Nordlandssykehuset har god kontroll på informasjonssikkerhet og personvern.

Styringssystem for informasjonssikkerhet

Det foreligger et felles regionalt styringssystem for informasjonssikkerhet i Helse Nord. Styringssystemet beskriver aktiviteter for å veilede og styre Helse Nord innenfor informasjonssikkerhet, herunder sikkerhetskrav som til enhver tid skal gjelde. Styringssystemet skal sikra at administrerende direktør (datasansvarlig) 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 tydeliggjør ansvars- og myndighetsforholdene mellom helseforetakene, Helse Nord IKT HF og Helse Nord RHF.

1. *Figur 1 Nivåene i Helse Nords styringssystem for informasjonssikkerhet.*

Det regionale fagråd for informasjonssikkerhet vedtok i 2017 å revidere styringssystemet. For å sikre nødvendig dokumentasjon ble det vedtatt å følge ISO-standard (NS-ISO/IEC 27001), men uten mål om å bruke tid/ressurser på en sertifisering. Nordlandssykehuset HF er en viktig bidragsyter til dette arbeidet. Figuren ovenfor viser hvordan styringssystemet er bygd opp på de ulike nivå. Dokumentene i styringssystemet er strukturert etter 4 nivåer.

Høsten 2018 ble nivå 1 (vedlegg 1) og nivå 2 (vedlegg 2) vedtatt og godkjent av alle dataansvarlige i Helse Nord. Nivå 2 i styringssystemet består av 24 ulike sikkerhetsområder, som beskriver hva som skal sikres. Disse tar utgangspunkt i ISO 27001/27002: annex A (internasjonal standard for informasjonssikkerhet), og er tilpasset Helse Nords sikkerhetsmål og sikkerhetsstrategi.

Nivå 3 består av operative regionale retningslinjer og prosedyrer. De regionale retningslinjer og prosedyrer som inngår i dagens styringssystem blir automatisk videreført og inngår i revidert styringssystem. Arbeidet med å videreutvikle og forbedre regionale rutiner og prosedyrer vil på områdene det er nødvendig fortsette utover i 2019.

Parallelt vurderes nivå 4 prosedyrer på hvert enkelt foretak, der ikke øvrige prosedyrer er tilstrekkelig.

Fjernlagerløsning – etablering av ny disaster og recovery løsning for Helse Nord

Høsten 2018 ble det etablert et prosjekt hos Helse Nord IKT med en målsetning om å få etablert en ny løsning for disaster og recovery i Helse Nord. Gjennom konseptfasen i prosjektet er det utarbeidet et overordnet løsningsforslag for etablering av infrastruktur som muliggjør en tilfredsstillende løsning for virksomhetskritiske, kliniske systemer. For å avklare krav og behov, samt utarbeide detaljerte løsningsdesign og planer for realisering av løsning er det igangsatt planfase for prosjektet. Planfasen er planlagt ferdigstilt 24. april 2019 og det er utarbeidet styringsdokumentasjon og plan for gjennomføringsfasen.

Nordlandssykehuset deltar i prosjektstyret og vil følge opp prosjektet i den videre gjennomføringsfasen. Prosjektet er planlagt ferdigstilt med ny løsning 30.04.2020.

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	

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6907
Versjon: 1.1

1 Styring av informasjonssikkerhet

Dette dokumentet er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Dokumentet beskriver hvordan Helse Nord ivaretar og etterlever sikkerhetsmål og sikkerhetsstrategi, som er beskrevet i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Nivå 2 i styringssystemet består av ulike sikkerhetsområder der hvert område beskriver krav innenfor samme tema. Se oversikt over sikkerhetsområdene i punkt 4.1.2. Sikkerhetsområdene tar utgangspunkt i ISO 27001/27002 (internasjonal standard for informasjonssikkerhet), og er tilpasset Helse Nords sikkerhetsmål og sikkerhetsstrategi.

Prosedyrene og retningslinjene på nivå 3 i styringssystemet presiserer aktiviteter som må gjennomføres, og hvem som er ansvarlig for å gjennomføre. For utdypende retningslinjer og/ eller sjekklister vil det henvises til egne dokumenter.

Lokale tilpasninger beskrives i egne prosedyrer, på nivå 4 i styringssystemet. Det enkelte foretaket er ansvarlig for å utarbeide og dokumentere disse.

2 Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle i Helse Nord. Eksterne parter som er tilkoblet Helse Nords infrastruktur eller som leverer tjenester til Helse Nord, skal følge krav og retningslinjer som er aktuelle for tilkoblingen eller tjenesten.

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

Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen) gjelder utfyllende for kravene som ikke er dekket av styringssystemet. Det skal henvises til Normen der det er naturlig. Ved motstrid skal Normen ha forrang.

3 Formål

Styringssystemet for informasjonssikkerhet skal gi en beskrivelse av hvordan Helse Nords aktiviteter planlegges, gjennomføres, evalueres og korrigeres.

Grunnlaget for styring av informasjonssikkerhet er styringssignal fra ledelsen, informasjonsidentifisering, fastsettelse av akseptabelt risikonivå, beskrivelse av sikkerhetsorganisasjon og valg av sikkerhetstiltak.

4 Krav til styring av informasjonssikkerhet

Informasjonssikkerhet skal ivaretas etter planlagte, systematiske og dokumenterte tiltak. For å sikre tilstrekkelig kontroll skal systematiske tiltak for å undersøke om sikkerhetstiltakene blir etterlevd, om de fungerer som forutsatt og om de er dekkende for risikobildet slik det foreligger på nåværende tidspunkt gjennomføres. Det skal også utføres undersøkelser om hvorvidt omfang og kvalitet av det arbeidet som Helse Nord gjør for styring og kontroll er tilfredsstillende, effektivt og tilpasset det

samlede risikobildet. Resultater fra disse undersøkelsene skal benyttes til å korrigere arbeidet som gjøres, og oppdaterer aktivitetene som gjennomføres.

Disse prosessene omtales samlet sett som Helse Nord sitt styringssystem for informasjonssikkerhet. For å oppnå tilfredsstillende styring av informasjonssikkerheten forutsetter dette sammenheng mellom aktivitetene beskrevet over.

4.1 Felles regionalt styringssystem for informasjonssikkerhet

Helse Nords regionale styringssystem for informasjonssikkerhet består av:

a) Regionale strategiske krav for informasjonssikkerhet i Helse Nord (nivå 1) «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».
b) Regionale områdekrav (nivå 2)
c) De regionale områdekravene konkretiseres i regionale prosedyrer og retningslinjer (nivå 3)
d) Lokale prosedyrer (nivå 4), som gir en beskrivelse av lokale forhold

4.1.1 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord (nivå 1)

a) Definerer overordnet sikkerhetsmål, sikkerhetsstrategi og ansvarsforhold.
b) Skal være i tråd med gjeldene regelverk og trusselbilde.
c) Skal behandles i foretaksgruppens Direktørmøte.
d) Administrerende direktør i Helse Nord RHF skal godkjenne dokumentet «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord», under forutsetning av at hver enkelt foretaksdirektør har godkjent dette dokumentet.
e) Administrerende direktør er dataansvarlig for all behandling av helse- og personopplysninger i eget foretak. Ansvaret innebærer en plikt til å etablere tilstrekkelig informasjonssikkerhet og etterleve regionale sikkerhetsmål og sikkerhetsstrategi.

4.1.2 Regionale sikkerhetsområder (nivå 2)

Regionale områdekrav beskriver de overordnede sikkerhetskravene som gjelder for Helse Nord innenfor det enkelte område, og beskriver hva som skal sikres. Kravene er delt inn i ulike sikkerhetsområder, med beskrivelse av mål og nødvendige sikkerhetskrav. Det er tatt utgangspunkt i ISO 27001:2013, annex A. Sikkerhetsområdene er tilpasset Helse Nord sine behov.

a) Et sett regionale områder for informasjonssikkerhet i Helse Nord defineres og sikkerhetsmål og hva som skal sikres beskrives.
b) Sikkerhetsområdene skal være tilpasset Helse Nords sikkerhetsmål og sikkerhetsstrategi.
c) Sikkerhetsområdene skal godkjennes av administrerende direktør RHF under forutsetning av at hver enkelt foretaksdirektør i helseforetakene har godkjent alle sikkerhetsområdene med innhold.
d) Endringer i krav som kan redusere dataansvarliges og regionens informasjonssikkerhet skal risikovurderes og godkjennes av dataansvarlige, jf punkt 4.4 krav til endring av sikkerhetsområder og innhold i krav.
e) Ved endringer i krav som kan påvirke Helse Nord IKT sitt ansvarsområde, skal det innhentes en anbefaling og tilråding fra Helse Nord IKT.
f) Alle sikkerhetsområder har en dokumentgodkjenner, og ansvaret følger strukturen beskrevet i «Regionale strategiske krav for informasjonssikkerhet i Helse Nord» (nivå 1).
g) For sikkerhetsområder som omhandler regional infrastruktur, og regionale krav til systemer, enheter og applikasjoner som tilknyttes denne, er administrerende direktør i Helse Nord IKT

dokumentgodkjenner, under forutsetning av at hver enkelt foretaksdirektør har godkjent sikkerhetsområdene med innhold.[1]
Sett inn lenke til «avtaledokumentet», der administrerende direktør har signert. Brevet skal også arkiveres i Sak/Arkiv, og referanse til dette nummert bør fremgå i fotnote i dette dokumentet.

h) For øvrige sikkerhetsområder er Administrerende direktør i Helse Nord RHF[2] dokumentgodkjenner, under forutsetning av at hver enkelt foretaksdirektør har godkjent sikkerhetsområdene med innhold.
Sett inn lenke til «avtaledokumentet», der administrerende direktør har signert. Brevet skal også arkiveres i Sak/Arkiv, og referanse til dette nummert bør fremgå i fotnote i dette dokumentet.

i) Dokumentgodkjenner, er ansvarlig for å etablere og forvalte kravene innenfor sitt ansvarsområde.

j) Sikkerhetsområdene skal publiseres og kommuniseres til alle medarbeidere i Helse Nord, og til relevante eksterne parter. Det enkelte helseforetak er selv ansvarlig for å informere internt/eksternt.

k) Dataansvarlig og databehandler er ansvarlig for å implementere og etterleve alle områdekrav.

l) Dataansvarlig og databehandler skal sørge for at etterlevelse av krav kontrolleres og dokumenteres. Se også sikkerhetsområde «06 Etterlevelse».

Sikkerhetskrav inndelt i områder

Dokument ID[3]	Sikkerhetsområde	Dokument-godkjenner[4]	ISO 27002-referanse
HN-ISMS-01	Styring av informasjonssikkerhet	HN RHF	A.5: Information security policies
HN-ISMS-02	Organisering av informasjons-sikkerhetsarbeidet i Helse Nord	HN RHF	A.6: Organization of information security
HN-ISMS-03	Risikovurdering og risikostyring	HN RHF	A.5: Information security policies A.8: Asset management
HN-ISMS-04	Personvern og pasientrettigheter	HN RHF	N/A
HN-ISMS-05	Ansatte, kompetanse og holdningsskapende arbeid	HN RHF	A.7: Human resource security
HN-ISMS-06	Etterlevelse	HN RHF	A.18: Compliance
HN-ISMS-07	Avvikshåndtering	HN RHF	A.16: Information security incident management
HN-ISMS-08	Fysisk sikkerhet og sikring av utstyr	HN RHF	A.11: Physical and environmental security
HN-ISMS-09	Identitetshåndtering	HN RHF	A.9: Access control
HN-ISMS-10	Tilgangsstyring	HN RHF	A.9: Access control
HN-ISMS-11	Beredskapsplanlegging helseforetak	HN RHF	A.17: Information security aspects of business continuity management
HN-ISMS-12	E-post, sms og sosiale medier	HN RHF	A.13: Communications security
HN-ISMS-13	Overføring av personopplysninger til utlandet	HN RHF	N/A
HN-ISMS-14	Innebygd personvern	HN RHF	N/A
HN-ISMS-15	Leverandørhåndtering	HN IKT	A.15: Supplier relationships
HN-ISMS-16	Kontroll på utstyr og verdier i Helse Nords	HN IKT	A.8: Asset management

[1] Jamfør Styresak 70-2002, og Styresak 005-2017
[2] Myndighet er delegert til Eierdirektør, og til Fagdirektør for forhold som omfatter klinikk/fagenhet.
[3] Dokument ID vil erstattes med DS samling i DocMap, når dokumentene blir lagt inn i DocMap.
[4] Under forutsetning at administrerende direktør i alle helseforetakene har godkjent innholdet i dokumentene.

	nettverk (Forvaltning av utstyr og verdier (asset))		
HN-ISMS-17	Kryptografi	HN IKT	A.10: Cryptography A.11: Physical and environmental security
HN-ISMS-18	Sikring av kommunikasjonsrom	HN IKT	A.11: Physical and environmental security
HN-ISMS-19	Sikkerhet i IKT-produksjonsmiljø	HN IKT	A.12: Operations security
HN-ISMS-20	Sikkerhetssoner	HN IKT	A.14: System acquisition, development and maintenance
HN-ISMS-21	Informasjonssikkerhet i IKT-anskaffelser	HN IKT	A.14: System acquisition, development and maintenance
HN-ISMS-22	Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare	HN IKT	A.14: System acquisition, development and maintenance
HN-ISMS-23	Informasjonssikkerhet i test	HN IKT	A.14: System acquisition, development and maintenance
HN-ISMS -24	Administratortilganger	HN IKT	A.6.1 Internal organization, A.9.2.3 Management of privileged access rights

4.1.3 Regionale retningslinjer og/eller prosedyrer (nivå 3)

a) Regionale retningslinjer og/eller prosedyrer gir detaljerte beskrivelser av hvordan kravene skal etterleves.
b) Helseforetakene skal bidra med å utarbeide, vedlikeholde og revidere regionale retningslinjer og prosedyrer.

4.1.4 Lokale rutiner (nivå 4)

a) Lokale rutiner og tilpasninger skal dokumenteres i egne prosedyrer.
b) Det enkelte helseforetaket er ansvarlig for å utarbeide slike.

4.2 Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen)

Normen er en bransjenorm, som forvaltes av en styringsgruppe, hvor Helse Nord er representert. Alle som er tilknyttet Norsk Helsenett er forpliktet til å følge den.

a) Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten (Normen) gjelder utfyllende.
b) Det skal henvises til Normen og Normens støttedokumenter der det er naturlig.
c) Normen har forrang ved eventuell motstrid med dette styringssystemet.

4.3 Ledelsens gjennomgang av området informasjonssikkerhet

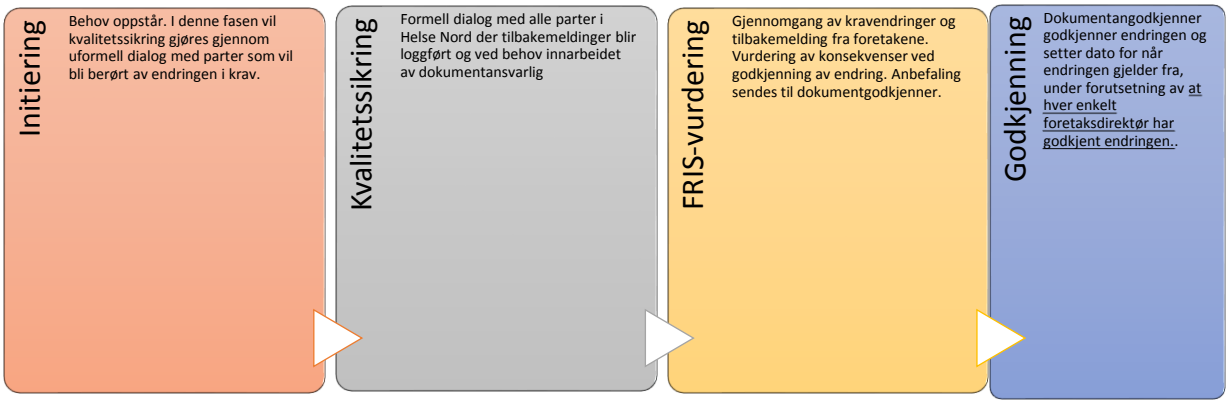
a) Ledelsens gjennomgang skal, minimum årlig, gi ledelsen status på informasjonssikkerhetsområdet. Ledelsens gjennomgang skal som minimum omfatte:
    1. Utvikling i trusselbildet for helseforetakene
    2. Trender fra gjennomførte risikovurderinger, inntrengingstester, sikkerhetstester og sikkerhetsrevisjoner

3. Oppsummering fra avviksrapportering
4. Behov for endringer i styringssystem for informasjonssikkerhet

b) Helseforetakene skal utarbeide ledelsens gjennomgang, og denne skal rapporteres til styrene.
c) Den enkelte helseforetaket skal ha egne retningslinjer for hvordan dette skal gjennomføres, herunder beskrive hvem som er ansvarlig for denne aktiviteten.

4.4 Endring av sikkerhetskrav

a) Ved behov for endring av eller innhold i sikkerhetskrav, skal dette følge en fastsatt prosess.
b) Behov for endringer kan blant annet oppstå ved årlig revisjon, resultat av ledelsens gjennomgang eller ved endringer i risikobildet som tilser at det er behov for å oppdatere regionale krav.
c) Alle endringer skal godkjennes formelt i Helse Nord før de blir gjeldende.
d) Den formelle godkjenningen skal gjennomføres i henhold til følgende prosedyre:



e) Informasjonssikkerhetsansvarlig/ sikkerhetssjef i helseforetaket skal ivareta kvalitetssikringsprosessen internt i eget helseforetak.
f) Fagråd for informasjonssikkerhet (FRIS) gir sin anbefaling.
g) Beslutning til endringen må foretas av de enkelte foretaksdirektører før dokumentgodkjenner publiserer og godkjenner sikkerhetskravet i DocMap.
h) Helseforetakenes Informasjonssikkerhetsansvarlig/sikkerhetssjef er ansvarlig for at endring i sikkerhetskrav blir kommunisert til relevante parter og medarbeidere i eget helseforetak.

5 Feilkilder

Ingen kjente feilkilder.

6 Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.5: Information security policies

Bransjenorm for informasjonssikkerhet og personvern i Helse- og omsorgstjenesten

1. Organisering av informasjonssikkerhet

Dokumentsamlingen «Organisering av informasjonssikkerheter» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av Informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Organisering av informasjonssikkerheter», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Organisering av informasjonssikkerheter» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle i Helse Nord. Eksterne parter som er tilkoblet Helse Nords infrastruktur eller som leverer tjenester til Helse Nord, skal følge krav og retningslinjer som er aktuelle for tilkoblingen eller tjenesten.

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

3. Formål

Helseforetakene skal ha tilfredsstillende informasjonssikkerhet basert på vurdering av risiko og sårbarhet, og oppfølging gjennom styringssystemet for ledelse og kvalitetsforbedring (internkontroll).

Det enkelte helseforetak, har et selvstendig og overordet ansvar for at informasjonssikkerheten blir ivaretatt i henhold til gjelden krav. Formålet med dette dokumentet er å beskrive hvilke krav som gjelder for sikkerhetsorganisering i helseforetakene.

4. Krav til sikkerhetsorganisering

Helseforetakene skal beskrive sikkerhetsorganiseringen i eget dokument. Ansvar, roller og rapporteringsrutiner skal være tydeliggjort. Det overordnede ansvaret ligger hos administrerende direktør i helseforetaket. Direktøren kan delegere myndighet og oppgaver til egne ansatte innen gitte rammer. Oppgaver kan også overføres til eksterne, f.eks. til *leverandører*, på grunnlag av skriftlige avtaler. Uansett om oppgaver er delegert eller ikke, ligger det juridiske ansvaret hos *dataansvarlig,* som er administrerende direktør i helseforetaket.

4.1 Organisering og ansvar i foretakene

Oppgavefordelingen av informasjonssikkerhetsarbeidet i det enkelte helseforetaket skal være klart definert, dokumentert og kjent for alle medarbeidere.

a) Sett inn lenke til Regionale retningslinjer for organisering av informasjonssikkerhet i helseforetakene (under utarbeidelse)

4.1.1 Administrerende direktør (AD)

a) Er dataansvarlig for all behandling av personopplysninger, og skal ha en dokumentert oversikt over databehandlingen i samsvar med art 30 i personvernforordningen. Se sikkerhetsområde «03 Risikovurdering og risikostyring».
b) Har det overordnede ansvar for informasjonssikkerheten i eget foretak, og for felles kliniske systemer hvor det er inngått en samarbeid om en felles journal.

4.1.2 Ledere som for eksempel klinikksjef, enhetsleder, avdelingsledere m.m

a) Enhver leder er ansvarlig for informasjonssikkerhet innen egen organisasjonsenhet.
b) Leders ansvar er utfyllende beskrevet i en egen retningslinje: se «Regionale retningslinjer for organisering av informasjonssikkerhet i helseforetakene» (under utarbeidelse)

4.1.3 Informasjonssikkerhetsansvarlig

a) Har det utøvende ansvar for foretakets sikkerhetsarbeid.
b) Sikkerhetssjef IKT / Informasjonssikkerhetsansvarlig skal rapportere til administrerende direktør.
c) Sikkerhetssjef/ infossikkerhetsansvarliges ansvar er utfyllende beskrevet i en egen retningslinje: se «Regionale retningslinjer for organisering av informasjonssikkerhet i helseforetakene» (under utarbeidelse)

4.1.4 Personvernombud(PVO)

a) Alle helseforetak i Helse Nord skal utpeke personvernombud.
b) Personvernombudet skal være uavhengig.
c) Personvernombudet skal ikke instrueres eller straffes for å utføre oppgaver i kraft av sin rolle som personvernombud.
d) Personvernombudet skal involveres og rapportere til høyeste ledelsesnivå
e) Personvernombudets oppgaver må ikke være i interessekonflikt med andre oppgaver eller roller.
f) Reglene om personvernombudets rolle følger av forordningens artikkel 38.
g) Personvernombudets rolle og arbeidsoppgaver er utfyllende beskrevet i en egen retningslinje: se «Regionale retningslinjer for organisering av informasjonssikkerhet i helseforetakene» (under utarbeidelse)

4.1.5 Drift og eiendomssjef

a) Har ansvaret for planlegging, koordinering, saksbehandling, gjennomføring av sentrale fysiske sikkerhetstiltak og øvelser, samt årlig rapportering av status til sikkerhetsledelsen (ledelsens gjennomgang).
b) Drift og eiendomssjefs roller og arbeidsoppgaver er utfyllende beskrevet i en egen retningslinje: se «Regionale retningslinjer for organisering av informasjonssikkerhet i helseforetakene» (under utarbeidelse)

4.1.6 Medarbeidere

a) Alle medarbeider har et selvstendig ansvar for å ivareta krav til informasjonssikkerhet i den daglige oppgaveløsningen. For mer utfyllende informasjon se: sikkerhetsområde «05 Ansatte, kompetanse og holdningsskapende arbeid».

Relevante regionale retningslinjer og prosedyrer:

- Taushets- og egenerklæring se SJ1473 «Taushets- og egenerklæring i Helse Nord»
- Sikkerhetsinstruksen se RL0259 «Sikkerhetsinstruks»

4.1.7 Systemeier

PLACEHOLDER: *Denne skal oppdateres, men må ses i sammenheng med arbeidet som gjøres i forbindelse med roller og ansvar funksjonell forvalting. FRIS foreslår at dette punktet oppdateres når arbeidsgruppen sin vurdering er ferdigstilt.*

4.2 Samarbeid og informasjonsutveksling mellom foretakene vedrørende informasjonssikkerhet

Helse Nord RHF skal sørge for at det etableres samarbeid mellom de ulike helseforetak, herunder Helse Nord IKT om forhold som angår informasjonssikkerheten. Informasjon om sikkerhetssituasjonen av betydning skal utveksles raskt mellom foretakene.

a) Fagråd for informasjonssikkerhet (FRIS) er et rådgivende organ som skal sikre en mest mulig enhetlig tilnærming til området informasjonssikkerhet.
b) Hvert enkelt helseforetak i regionen skal ha en representant i FRIS, for å sikre aktiv involvering i det regionale sikkerhetsarbeidet.
c) Helse Nord IKT skal informere helseforetakene og det regionale helseforetaket om trusselbilde, hendelser og avvik som er relevante for informasjonssikkerheten.
d) Helseforetakene skal informere Helse Nord IKT om hendelser, endringer og avvik som kan påvirke sikkerheten i Helse Nord.
e) Alvorlige og kritiske forhold skal varsles uten ugrunnet opphold. Se sikkerhetsområde «07 Avvikshåndtering» og sikkerhetsområde «11 Beredskapsplanlegging».

4.3 Samarbeid med myndigheter og fagressurser innen informasjonssikkerhet

a) Helse Nord RHF skal sørge for å koordinere samarbeid med nasjonale myndigheter og leverandører om spørsmål og problemstillinger vedrørende informasjonssikkerhet.
b) Dataansvarlig skal sammen med databehandler ha god forståelse av risiko- og trusselbildet.
c) Helse Nord IKT skal koordinere kontakt med relevante operative samarbeidsorganer som for eksempel HelseCERT for å sikre en best mulig forståelse av trusselbildet.

4.3.1 Helse Nord IKT

Helse Nord IKT er databehandler for helseforetakene i Helse Nord og skal oppfylle kravene i lov og forskrift, i regionalt styringssystem for informasjonssikkerhet og databehandleravtaler.

a) Helse Nord IKT skal sørge for tilstrekkelig sikkerhet ved drift og forvaltning av Helse Nords IKT-løsninger.

b) Helse Nord IKT skal etablere og forvalte IKT-sikkerhetskrav til regional infrastruktur, og krav til systemer, enheter og applikasjoner som tilknyttes denne. Se sikkerhetsområde «01 Styring av informasjonssikkerhet».

4.3.2 Andre leverandører

a) Helseforetakenes bruk av private tjenesteytere eller leverandører skal reguleres i kontrakter/avtaler. Informasjonssikkerhet skal inngå som et eget punkt.
Se også sikkerhetsområde «15 Leverandørhåndtering».

4.4 Personvern og informasjonssikkerhet i prosjekter

Sikkerhetskravene og retningslinjene som er beskrevet i Helse Nord sitt styringssystem for informasjonssikkerhet gjelder for alle prosjekter.

a) Prosjektleder er ansvarlig for å etterleve alle krav til personvern og informasjonssikkerhet.
b) Personvern og informasjonssikkerhet skal være en del av prosjektmetodikken.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.9: Access control.

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

1. Risikovurdering og risikostyring

Dokumentsamlingen «Risikovurdering og risikostyring» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Risikovurdering og risikostyring», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Risikovurdering og risikostyring» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene og retningslinjene som er beskrevet i dette dokumentet gjelder for alle helse-foretak og alle medarbeidere i foretaksgruppen.

Med medarbeider menes enhver som utfører oppdrag på vegne av helseforetakene i Helse Nord og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller til adgangsregulerte områder.

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»).[1]

Helseopplysninger er personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand.[2]

Med **behandling** av helse- og personopplysninger menes enhver operasjon eller rekke av operasjoner som gjøres med slike opplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, tilgjengeliggjøring ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.[3]

[1] GDPR artikkel 4 nr. 1)
[2] GDPR artikkel 4 nr. 15), Pasientjournalloven § 2, Helseregisterloven § 2
[3] GDPR artikkel 4 nr. 2)

3. Formål

Risikostyring med hensyn til informasjonssikkerhet innebærer å etablere oversikt over informasjon som behandles i virksomheten, hvilken risiko databehandlingen medfører for både virksomheten og de registrerte og hvilke tiltak som skal gjennomføres for å ivareta informasjonssikkerheten.

Dokumentet er inndelt i tre hovedkapitler:

- Oversikt over behandling av helse og personopplysninger (kapittel 4)
- Risikovurdering og risikostyring (kapittel 5)
- Personvernkonsekvensvurdering – DPIA (kapittel 6)

4. Oversikt over behandling av helse- og personopplysninger

Helseforetakene, som er dataansvarlig, skal ha en oversikt over de behandlinger av helse- og personopplysninger som til enhver tid gjennomføres i foretaket.

a) Oversikten skal som minimum inneholde[4]:
    1. Navnet på og kontaktopplysningene til den behandlingsansvarlige, og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet.
    2. Formålene med behandlingen.
    3. En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger
    4. Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner.
    5. Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, med identifikasjon av nevnte tredjestat eller internasjonale organisasjon
    6. Dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger.
    7. Dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

b) Dataansvarlig skal ha rutiner for å sikre oppdatering ved eventuelle endringer i oversikten.
c) Oversikten skal være enkelt tilgjengelig elektronisk, og legges fram for tilsynsmyndigheten på forespørsel.

5. Risikostyring og risikovurdering

Risiko er det at en hendelse kan inntreffe og påvirke måloppnåelsen negativt.

Risikovurdering innebærer å ta stilling til *sannsynligheten* for at en hendelse med negativ effekt på måloppnåelsen vil inntreffe, og den forventede *konsekvensen* av hendelsen. Resultatet av vurderingen indikerer hvor høy den enkelte risiko er, og danner grunnlag for å prioritere hvilke risikoer som må følges opp (håndteres), og hvordan oppfølgingen skal skje.

[4] Jf. GDPR artikkel 30 og Datatilsynets veileder https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

Konsekvensen av at risikoen inntreffer vil ofte være tap i forhold til noe en har, eller noe en planlegger å oppnå. Hvor alvorlig konsekvensen er, vil blant annet avhenge av det mulige tapets art og omfang, sett opp mot virksomhetens målsettinger. Det kan for eksempel dreie seg om konsekvenser som:

1. tap av liv og helse
2. tap av materielle verdier
3. tap av informasjon
4. tap av kompetanse
5. tap av tid
6. tap av omdømme

Risikostyring er en prosess som skal gi rimelig grad av sikkerhet for virksomhetens måloppnåelse. Prosessen gjennomføres av virksomhetens styre, ledelse og ansatte, anvendes i fastsettelse av strategi og på tvers av virksomheten, og er utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og håndtere risiko slik at den er i samsvar med virksomhetens risikotoleranse. Risikostyring skal være en integrert del av den øvrige styringen foretakene har etablert.

Risikostyring vil på ledelsesnivå i foretaket dreie seg om å realisere styringskrav og overordnede mål. Ute i organisasjonen vil risikostyring i tillegg være rettet mot å sikre at vanlige aktiviteter og daglig produksjon gjennomføres innenfor et akseptabelt risikonivå. Det vil innebære fokus på uønskede hendelser som uhell, ulykker, svikt i viktige funksjoner m.m.

5.1 Krav om risikostyring

a) Foretakene skal ha et system for risikostyring for å forebygge, hindre og avdekke avvik.
b) Risikofaktorer som kan medvirke til at målene for helseforetakene ikke blir nådd, skal identifiseres, og korrigerende tiltak som kan redusere faren for manglende måloppnåelse, skal iverksettes.
c) De dataansvarlige (foretakene i Helse Nord) skal sikre at det gjennomføres risikovurdering
    1. før en ny behandling av helse- og personopplysninger påbegynnes,
    2. ved endringer som har betydning for informasjonssikkerheten, herunder organisatoriske eller tekniske endringer i et system,
    3. når det gis ny tilgang til helse- og personopplysninger mellom virksomheter,
    4. når trusselbildet endres.
d) Risikovurderingen skal dokumenteres.

5.2 Ledelsens ansvar

Kunnskap fra risikovurderinger og risikohåndtering ute i organisasjonen utgjør et viktig grunnlag for risikostyringen på ledelsesnivå, samtidig som signalene fra ledelsens risikostyring skal tas hensyn til i drift og prioriteringer ute i organisasjonen.

Risikovurderingene av de definerte behandlingene, og tiltakene som er iverksatt for å håndtere de avdekkede risikoene, skal følges opp regelmessig i foretakenes ledelse, minimum en gang i året, som en integrert del av mål- og resultatstyringen i foretaket.

a) Resultatet av risikovurderingen skal gjennomgås av virksomhetens ledelse
b) Helseforetakets ledelse skal prioritere tiltak for å oppnå et akseptabelt risikonivå
c) Helseforetakets ledelse skal minimum årlig behandle informasjonssikkerhet (ledelsens gjennomgang). Om organisering av informasjonssikkerhet, se sikkerhetsområdet 02 Organisering av informasjonssikkerhetsarbeidet i Helse Nord

d) Helseforetakets ledelse er ansvarlig for å sikre at databehandlingen ikke medfører økt regional sikkerhetsrisiko

5.3 Akseptabel risiko

Helseforetaket ved administrerende direktør er dataansvarlig, og er ansvarlig for å definere akseptabelt risikonivå. Sikkerhetsbrudd aksepteres ikke, men det er en viss risiko for at sikkerhetsbrudd kan forekomme. Det er nivået for denne risikoen som skal aksepteres, ikke selve sikkerhetsbruddet.

Det må tas stilling til hva som er et akseptabelt nivå for risikoen for ikke å nå den aktuelle målsettingen, altså hvilken risikotoleranse vi har på området. Risikotoleransen tar utgangspunkt i den risiko foretaket kan akseptere i arbeidet med å realisere sitt formål/sin visjon, sine strategier og målsettinger. En risiko man vil akseptere fordi den opptrer på et område hvor man har høy risikotoleranse, må man trolig iverksette tiltak for å redusere hvis det dreier seg om et område eller en målsetting hvor risikotoleransen er lav.

Det er ledelsens oppgave å avklare foretakets holdning til risikoer og definere dets risikotoleranse (toleransegrenser).

5.4 Sikkerhetstiltak

a) Hvis den avdekkede risikoen er høyere enn akseptabelt risikonivå, skal det iverksettes tiltak.
b) Sikkerhetstiltak skal etableres slik at
    1. tiltakene omfatter både rutiner medarbeiderne forutsettes å følge, og tiltak som ikke kan påvirkes eller omgås av medarbeiderne med uaktsomhet.
    2. tiltakene ikke kan omgås av eksterne, selv om disse opptrer med forsett.
    3. det er liten sannsynlighet for at sensitive personopplysninger/helseopplysninger kompromitteres.
    4. øvrige personopplysninger minimum sikres med tiltak som gir moderat grad av sannsynlighet for kompromittering, forutsatt at dette ikke øker sannsynligheten for kompromittering av sensitive personopplysninger.
    5. det går flere måneder mellom hendelser med moderat konsekvens for helsehjelpen, forholdet til pasienten, foretaket/personellet og for øvrige medarbeidere.
    6. hendelser med alvorlig konsekvens er enda vanskeligere å forårsake og inntreffer enda sjeldnere enn hendelser med moderat konsekvens

6. Personvernkonsekvensvurdering (DPIA)

Dersom det er sannsynlig at en type databehandling vil medføre høy risiko for fysiske personers rettigheter og friheter, skal den dataansvarlige før databehandlingen foreta en vurdering av hvilke konsekvenser databehandlingen kan ha for personvernet.[5]
Dette innebærer at den dataansvarlige må:

1. Vurdere *om* det må gjøres en personvernkonsekvensvurdering
2. I så fall *gjennomføre* personvernkonsekvensvurderingen

[5] GDPR artikkel 35

3. Basert på resultatet av personvernkonsekvensvurderingen, vurdere om det er behov for å iverksette *tiltak*

6.1 Når skal personvernkonsekvensvurderinger gjennomføres

a) Det skal gjøres en vurdering av om personvernkonsekvensvurdering skal gjennomføres før nye produkter, tjenester og systemer skal tas i bruk.
b) Også før behandling av personopplysninger i forsknings- og kvalitetsprosjekter skal det vurderes om det er nødvendig å gjennomføre en personvernkonsekvensutredning.

c) Vurdering av personvernkonsekvenser skal alltid gjennomføres dersom databehandlingen sannsynligvis vil medføre en *høy risiko* for fysiske personers rettigheter og friheter.
Høy risiko vil sannsynligvis være til stede når databehandlingen omfatter to eller flere av følgende kriterier:[6]
    1. Evaluering eller poengsetting, inkludert profilering og forutsigelse.
    2. Automatiske beslutninger med betydelig virkning.
    3. Systematisk monitorering.
    4. Særlige kategorier av personopplysninger (tidligere kalt sensitive personopplysninger)
    5. Personopplysninger behandles i stor skala.
    6. Matching eller sammenstilling av datasett.
    7. Personopplysninger om sårbare registrerte.
    8. Innovativ bruk/anvendelse av ny teknologisk eller organisatorisk løsning.
    9. Når databehandlingen hindrer de registrerte i å utøve en rettighet eller gjøre bruk av en tjeneste eller en avtale.

d) Dersom databehandlingen *ikke* medfører høy risiko kan den dataansvarlige beslutte at det ikke skal gjennomføres personvernkonsekvensvurdering. Denne beslutningen skal dokumenteres.
Eksempler på behandlinger som kan være unntatt fra kravet om personvernkonsekvensvurdering er:[7]
    1. Dersom databehandlingen sannsynligvis ikke vil medføre en høy risiko.
    2. Dersom databehandlingens art, omfang, sammenheng og formål er veldig lik en databehandling det allerede er gjennomført en vurdering av personvernkonsekvenser for.
    3. Dersom databehandlingen er kontrollert av en tilsynsmyndighet før mai 2018 på særskilte betingelser, og at disse ikke har endret seg (f.eks. konsesjon fra Datatilsynet).
    4. Dersom en databehandling er nødvendig for å oppfylle en rettslig forpliktelse eller utføres i allmennhetens interesse (artikkel 6 nr. 1 c eller e) **og** har et hjemmelsgrunnlag i annen lovgiving (f.eks. helsepersonelloven) **og** en vurdering av personvernkonsekvenser allerede er gjennomført som ledd i utarbeidelse av rettsgrunnlaget, unntatt hvis lovgiver har bestemt at det er nødvendig å gjennomføre en vurdering av personvernkonsekvenser forut for databehandlingen.

[6] Datatilsynets veileder: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/?id=10362 se spesielt kapittel 5
[7] Datatilsynets veileder, se spesielt kapittel 3

6.2 Gjennomføring av personvernkonsekvensvurdering

a) Den behandlingsansvarlige skal rådføre seg med personvernombudet, dersom et personvernombud er utpekt, i forbindelse med utførelsen av en vurdering av personvernkonsekvenser.[8]
b) Dokumentasjon fra vurderingen skal som et minimum inneholde:[9]
    1. En systematisk beskrivelse av de planlagte behandlingsaktivitetene, formålene med behandlingen, og eventuelt hvilken berettiget interesse den ivaretar[10].
    2. En vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene.
    3. En vurdering av risikoen behandlingen har for de registrertes rettigheter og friheter.
    4. Beskrivelse av planlagte tiltak for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre at personopplysningene vernes og å påvise at forordningen overholdes[11].

c) Dersom det er relevant, skal den dataansvarlige innhente de registrertes synspunkter på den planlagte behandlingen[12].

7. Forhåndsdrøftelser

a) Hvis høy risiko ikke kan reduseres gjennom tiltak, skal Datatilsynet kontaktes for forhåndsdrøftelse.[13]

8. Feilkilder

Datatilsynet sier at de skal lage en liste over databehandlinger som krever DPIA: *«Noen behandlingsaktiviteter krever **alltid** at det utføres en vurdering av personvernkonsekvenser. En liste over disse vil komme her i løpet av høsten 2018, etter gjennomgang i personvernrådet i Brussel (EDPB).»*

9. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002

ISO/IEC 27005:2018 Information technology -- Security techniques -- Information security risk management

[8] GDPR artikkel 35 punkt 2
[9] GDPR artikkel 35 punkt 7
[10] Beskrivelse i protokoll over behandlingsaktiviteter iht. artikkel 30, se kapittel 4
[11] GDPR artikkel 32
[12] GDPR artikkel 35 punkt 9
[13] GDPR artikkel 36 punkt 1. Se også Datatilsynets veiledning for slike forhåndsdrøftelser: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/forhandsdroftelser/

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten («Normen»)
RL1602 Retningslinjer for risikostyring i Helse Nord

Andre maler, f.eks.:

- Datatilsynets veiledning for protokoll over behandlingsaktiviteter: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/
- Direktoratet for e-helse sin mal for DPIA: https://ehelse.no/Documents/Personvern%20og%20informasjonssikkerhet/Mal%20DPIA%20Personvernkonsekvensutredning%20etter%20GDPR%20%28word%29.docx
- Datatilsynets veileder for DPIA: https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/
- Datatilsynets veiledning for Forhåndsdrøftelser: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/forhandsdroftelser/

1. Personvern og pasientrettigheter

Dokumentsamlingen «Personvern og pasientrettigheter» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Personvern og pasientrettigheter», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Personvern og pasientrettigheter» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene og retningslinjene som er beskrevet i dette dokumentet gjelder for alle helse-foretak og alle medarbeidere i foretaksgruppen.

Med medarbeider menes enhver som utfører oppdrag på vegne av helseforetakene i Helse Nord og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller til adgangsregulerte områder.

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Etter personvernforordningen (GDPR[1]) er det den dataansvarlige som har plikter. For pasient-opplysninger vil f.eks. hvert helseforetak være dataansvarlig for opplysninger om egne pasienter.[2]

Personopplysninger er enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»).[3]

Helseopplysninger er personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand.[4]

[1] GDPR (General Data Protection Regulation) EUs personvernforordning
[2] Med dataansvarlig menes fysisk eller juridisk person, offentlig myndighet, institusjon eller organ som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes i databehandlingen GDPR artikkel 4 pkt. 7)
[3] GDPR artikkel 4 nr. 1)
[4] GDPR artikkel 4 nr. 15), Pasientjournalloven § 2, Helseregisterloven § 2

Med **behandling** av helse- og personopplysninger menes enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, tilgjengeliggjøring ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

3. Formål

Dette dokumentet omhandler krav til personvern og informasjonssikkerhet ved behandling av helse- og personopplysninger i Helse Nords virksomheter/helseforetak og pasientenes rettigheter knyttet til denne databehandlingen. Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger.

Dokumentet beskriver rettighetene til pasienter, pårørende og ansatte, heretter kalt de registrerte. I dette dokumentet betyr det «den registrertes» rettigheter mht. behandling av de opplysninger som er registrert om vedkommende, så som rett til innsyn, rett til retting av feilaktige opplysninger, rett til å begrense innsyn (sperring), sletting av informasjon mv.

Dokumentet inneholder derfor følgende hovedkapitler:

- Dataansvarliges plikter, inkl. taushetsplikt
- De registrertes rettigheter
- Utlevering av helse- og personopplysninger

4. Dataansvarliges plikter

Den dataansvarlige er ansvarlig for at kravene til behandling av helse- og personopplysninger etterleves, og skal kunne påvise at disse overholdes («ansvarsprinsippet»)[5].

4.1 Lovlighet, rettferdighet og åpenhet

Helselovgivningen danner grunnlaget for behandling av helseopplysninger. I tillegg vil person-opplysningsloven danne grunnlag for behandling av andre personopplysninger (f.eks. opplysninger om ansatte).

a) Hjemmelsgrunnlag for behandling av personopplysninger er at:
    1. Den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål.[6]
    2. Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.[7]
    3. Behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt.[8]

b) Hjemmelsgrunnlag for behandling av helseopplysninger er at:
    1. Den registrerte har gitt uttrykkelig samtykke til behandling av slike personopplysninger for ett eller flere spesifikke formål, unntatt de tilfellende der den registrerte ikke kan nekte slik behandling.[9]
    2. Behandlingen er nødvendig av hensyn til viktige allmenne interesser.[10]

[5] GDPR artikkel 5
[6] GDPR artikkel 6 pkt. a
[7] GDPR artikkel 6 pkt. c
[8] GDPR artikkel 6 pkt. e
[9] GDPR artikkel 9 nr. 2 pkt. a

3. Behandlingen er nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin for å vurdere en arbeidstakers arbeidskapasitet, i forbindelse med medisinsk diagnostikk, yting av helse- eller sosialtjenester, behandling eller forvaltning av helse- eller sosialtjenester og -systemer på grunnlag av … nasjonal rett eller i henhold til en avtale med helsepersonell.[11]

c) All behandling av helse- og personopplysninger skal gjøres med respekt for den registrertes interesser og rettigheter.
d) Hvert helseforetak skal ha en lett tilgjengelig personvernerklæring, som overordnet beskriver hvordan helseforetaket behandler helse- og personopplysninger. Her skal det også fremgå hvem den registrerte kan kontakte for å få oppfylt sine rettigheter, se også punkt 5.1

4.2 Formålsbegrensning

a) Dataansvarlig skal sørge for at alle helse- og personopplysninger som samles inn har et spesifikt og dokumentert formål, for eksempel helsehjelp, diagnostiske opplysninger, forskning, kvalitetskontroll, ansattopplysninger, mv. Formål dokumenteres bl.a. i protokoll over behandlingsaktiviteter.
b) Helse- og personopplysningene kan ikke viderebehandles på en måte som er uforenelig med det opprinnelige formålet.

4.3 Dataminimering

a) Behandling av helse- og personopplysninger skal være adekvat, relevant og begrenset til det som er nødvendig for formålene de behandles for, for eksempel dokumentasjon av gitt helsehjelp, dokumentasjon av diagnostiske undersøkelser mv.

4.4 Riktighet (integritet)

a) Helse- og personopplysninger skal være korrekte og oppdaterte
b) Det skal treffes tiltak for å sikre at helse- og personopplysninger som er faktisk uriktige, slettes eller rettes (f.eks. demografiske opplysninger om pasient, tidspunkt for hendelser …). For helseopplysninger må dette gjøres i tråd med helsepersonelloven §§ 42 og 44.

4.5 Lagringsbegrensning

a) Helse- og personopplysninger skal ikke lagres lenger enn det som er nødvendig for de formålene de behandles for, med unntak som følger av lov (f.eks. arkivloven, pasientjournalloven, helseforskningsloven).
    1. For helse- og personopplysninger til forskning er det krav om sletting etter gitt tid.[12]
    2. Helseopplysninger i pasientjournal skal oppbevares minst 10 år etter pasientens død, hvis ikke annet er avtalt, for deretter å overføres til Norsk helsearkiv[13].

4.6 Integritet og konfidensialitet[14]

a) Den behandlingsansvarlige og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet:
    1. Pseudonymisering og kryptering av personopplysninger.
    2. Evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene.
    3. Evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse.

[10] GDPR artikkel 9 nr. 2 pkt. g
[11] GDPR artikkel 9 nr. 2 pkt. h
[12] GDPR artikkel 89
[13] Helsearkivforskriften §§ 17 - 18
[14] GDPR artikkel 32

4. En prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

b) Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

4.7 Taushetsplikt

a) Enhver medarbeider i Helse Nord har et aktivt ansvar for å hindre at helse- og personopplysninger kommer på avveier.
b) Enhver medarbeider i Helse Nord har en (passiv) plikt til å tie.

Taushetsplikt er hjemlet i helsepersonelloven § 21; se også pasient- og brukerrettighetsloven § 3-6. Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker[15], samt unntakene gitt i helsepersonellovens §§ 23 - 29.

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helse- og personopplysninger uten at det er begrunnet i helsehjelp til pasienten eller administrasjon av slik hjelp, eller at det har særskilt hjemmel i lov eller forskrift («Snokeparagrafen» - helsepersonelloven § 21a). Jf. kapittel 11 i dokumentet Instruks pasientjournalen om krav til signering av taushetsplikt og straffereaksjon. Se PR04663 «Instruks pasientjournal».

5. De registrertes rettigheter

Det skal legges til rette for at den registrerte skal kunne få oppfylt sine rettigheter. Dette betyr bl.a. at den registrerte skal få innsyn i hvilke opplysninger som behandles og hvordan dette skjer. Rettighetene til pasienter ivaretas gjennom helselovgivningen[16]. Den registrertes rettigheter i forbindelse med behandling av personopplysninger (f.eks. om ansatte) reguleres av personopplysningslovgivningen.

5.1 Informasjon[17]

Noe informasjon må stå i en generell personvernerklæring for foretaket, noe informasjon gis direkte til den registrerte.

a) Den registrerte har rett til å få informasjon om behandlingen av sine helse- og personopplysninger. Informasjonen skal framlegges på en kortfattet, åpen, forståelig og lett tilgjengelig måte.
b) Når det samles inn helse- og personopplysninger fra den registrerte skal det gis informasjon om:
    1. Kontaktopplysninger til den dataansvarlige
    2. Kontaktopplysninger til personvernombudet
    3. Formålet med behandlingen av personopplysningene
    4. Rettslig grunnlag for databehandlingen
    5. Eventuelle mottakere av personopplysningene
    6. Overføring av personopplysninger til tredjeland
    7. Tidsrom for lagring
    8. Retten til å anmode om innsyn, retting, sletting og begrensning i databehandlingen
c) Denne typen informasjon skal gis gratis.

[15] Pasient- og brukerrettighetsloven § 3-6
[16] Eksempelvis Pasient- og brukerrettighetsloven
[17] GDPR artikkel 12-14

5.2 Krav til samtykke[18]

Samtykke skal være frivillig, informert og uttrykkelig.
Samtykke kan gis uttrykkelig eller stilltiende. Stilltiende samtykke anses å foreligge dersom det ut fra pasientens handlemåte og omstendighetene for øvrig er sannsynlig at hun eller han godtar at helsehjelp ytes og derigjennom behandlingen av helseopplysninger i tilknytning til helsehjelpen[19].
Forordningen gir unntak fra kravet om eksplisitt (uttrykkelig) samtykke med hjemmel i nasjonal lovgivning.[20] Det kan for eksempel være helsepersonelloven § 39 (helsepersonells plikt til å føre journal) og helseforskningsloven § 28 (humant biologisk materiale innsamlet i helse- og omsorgstjenesten som ledd i diagnostisering og behandling, kan under visse vilkår brukes til forskning uten innhenting av pasientens samtykke).

a) Dersom behandlingen av helse- og personopplysninger bygger på samtykke, skal den dataansvarlige dokumentere at den registrerte har samtykket.
b) Dersom den dataansvarlige skal viderebehandle personopplysningene for et annet/nytt formål som er uforenlig med det opprinnelige, skal den dataansvarlige gi den registrerte informasjon om dette[21]. Det skal da innhentes nytt samtykke.
c) Den registrerte skal ha rett til å trekke tilbake sitt samtykke til enhver tid. Det skal være like enkelt å trekke tilbake et samtykke som å gi samtykke.
d) For barn under 16 år er behandling av barnets personopplysninger lovlig bare dersom og i den grad samtykke er gitt eller godkjent av den som har foreldreansvar for barnet. Medlemsstatene kan ved lov fastsette en lavere aldersgrense, forutsatt at den ikke er lavere enn 13 år.[22] I Norge er aldersgrensen satt til 13 år.[23]

5.3 Innsyn[24]

a) Den registrerte har rett til å få bekreftelse på *om* det behandles personopplysninger om vedkommende og, dersom dette er tilfelle, innsyn i personopplysningene.
b) Den registrerte har rett til på en enkel og sikker måte å se *hvem* som har hatt tilgang til helseopplysningene.

5.4 Korrigering[25]

Den registrerte har rett til å få uriktige helse- og personopplysninger om seg selv rettet uten ugrunnet opphold. Det kan være feilaktige, mangelfulle eller utilbørlige opplysninger eller utsagn i en journal[26] eller faktiske feil som demografiske opplysninger, tidspunkt, dokumentasjon registrert på feil person.

5.5 Sletting[27]

Den registrerte har rett til å få helse- og personopplysninger om seg selv slettet uten ugrunnet opphold. For helseopplysninger må dette gjøres i tråd med helsepersonelloven § 43, dvs. dersom opplysningene er feilaktige eller misvisende og føles belastende for den de gjelder eller dersom opplysningene åpenbart ikke er nødvendige for å gi pasienten helsehjelp.

[18] GDPR artikkel 7-8 og helsepersonelloven § 22
[19] Pasient- og brukerrettighetsloven § 4-2
[20] GDPR artikkel 9 pkt. 2a
[21] GDPR artikkel 13 pkt. 3
[22] GDPR artikkel 8
[23] Personopplysningsloven § 5
[24] GDPR artikkel 15, pasientjournalloven §18, helsepersonelloven § 41
[25] GDPR artikkel 16
[26] Helsepersonelloven § 42
[27] GDPR artikkel 17

5.6 Begrensning[28]

Den registrerte kan motsette seg at helseopplysninger i et behandlingsrettet helseregister gjøres tilgjengelige for helsepersonell (sperring), jf. helsepersonelloven §§ 25 og 45, pasient- og brukerrettighetsloven § 5-3.

5.7 Dataportabilitet [29]

Den registrerte har rett til å motta opplysninger om seg selv i et strukturert, alminnelig anvendt og maskinlesbart format og skal ha rett til å overføre disse opplysningene til en annen dataansvarlig. Behandling av helseopplysninger basert på pasientjournalloven og helseregister-loven vil imidlertid ikke være omfattet av retten til dataportabilitet. Informasjon eller analyse den dataansvarlige har generert på bakgrunn av opplysningene omfattes heller ikke.[30]

5.8 Innsigelse[31]

Det er ikke grunnlag for å motsette seg behandling av personopplysninger som er nødvendig for å oppfylle rettslige forpliktelser, for eksempel dokumentasjon av gitt helsehjelp i pasientjournalen, nødvendig tilgang til journal for å sikre forsvarlig helsehjelp mv.[32]

5.9 Rett til individuelle avgjørelser[33]

Automatiserte avgjørelser basert på helseopplysninger er kun lovlig når annen nasjonal lovgivning gir grunnlag for det[34].

6. Utlevering av helse- og personopplysninger

Dersom helsepersonell utleverer opplysninger som er undergitt lovbestemt opplysningsplikt, skal den opplysningene gjelder, så langt forholdene tilsier det, informeres om at opplysningene er gitt og hvilke opplysninger det dreier seg om[35].

6.1 Til helseforetakets ledelse for kvalitetsforbedring[36]

Opplysninger kan gis til virksomhetens ledelse for internkontroll og kvalitetssikring av tjenesten. Opplysningene skal så langt det er mulig, gis uten individualiserende kjennetegn. Slike opplysninger kan også gis til ledelsen i samarbeidende virksomhet ved samarbeid om behandlingsrettede helseregistre etter pasientjournalloven § 9.

[28] GDPR artikkel 18 og pasientjournalloven §17
[29] GDPR artikkel 20
[30] Direktoratet for e-helse: https://ehelse.no/rettigheter-ved-behandling-av-helse-og-personopplysninger-etter-gdpr
[31] GDPR artikkel 21
[32] GDPR artikkel 6 pkt. 1c
[33] GDPR artikkel 22
[34] GRPR artikkel 22 pkt. 4
[35] Helsepersonelloven kapittel 5 og 6 og Pasient- og brukerrettighetsloven § 3-6
[36] Helsepersonelloven § 26

Opplysninger om pasientens personnummer, diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data kan gis til vedkommende virksomhets pasientadministrasjon. Reglene om taushetsplikt gjelder tilsvarende for personell i pasientadministrasjonen.

6.2 Til helseforetaket for læring og kvalitetssikring[37]

Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger etter særskilt anmodning gis til annet helsepersonell som tidligere har ytt helsehjelp til pasienten i et konkret behandlingsforløp, for kvalitetssikring av helsehjelpen eller egen læring. Bare de opplysninger som er nødvendige og relevante for formålet kan gis ut. Utleveringen skal dokumenteres i pasientens journal.

6.3 Til forskning[38]

Opplysninger kan gis til bruk i forskning, uten hinder av taushetsplikt. Til slikt vedtak kan knyttes vilkår. Myndighet til å tillate at opplysninger brukes i forskning er delegert til den regionale komiteen for medisinsk og helsefaglig forskningsetikk (REK). Opplysninger til forskning som ikke faller inn under helseforskningsloven, eksempelvis tjenesteforskning, nytt utstyr mv., må ha særskilt hjemmel og databehandlingen må godkjennes av virksomheten.

6.4 Tilgang til helse- og personopplysninger mellom virksomheter[39]

Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.

Den dataansvarlige skal sørge for at relevante og nødvendige helseopplysninger er tilgjengelige for helsepersonell og annet samarbeidende personell når dette er nødvendig for å yte, administrere eller kvalitetssikre helsehjelp til den enkelte. Den dataansvarlige bestemmer på hvilken måte opplysningene skal gjøres tilgjengelige. Opplysningene skal gjøres tilgjengelige på en måte som ivaretar informasjonssikkerheten.

6.5 Til andre instanser[40]

Helse- og personopplysninger kan også utleveres til ulike tilsynsmyndigheter, til den kommunale helse- og omsorgstjenesten, til barnevern og til politi og brannvesen. I tillegg kommer meldeplikt til en rekke nasjonale registre.

a) Tilsynsmyndigheter skal gis alle de opplysninger som ansees påkrevd for utøvelsen av tilsyn med helsepersonells virksomhet. Dokumenter, lyd- og bildeopptak og lignende som kreves, skal utleveres uten hinder av taushetsplikten.
b) Den som yter helsehjelp, skal gi den kommunale helse- og omsorgstjenesten opplysninger om forhold som bør føre til tiltak etter å ha innhentet samtykke fra pasienten, eller så langt opplysningene ellers kan gis uten hinder av taushetsplikt.

[37] Helsepersonelloven § 29c
[38] Helsepersonelloven 29
[39] Helsepersonelloven §§ 25 og 45; Pasientjournalloven §19
[40] Helsepersonelloven §§ 30 - 34

c) Opplysninger skal gis til barneverntjenesten når det er grunn til å tro at et barn blir mishandlet i hjemmet eller det foreligger andre former for alvorlig omsorgssvikt. Det samme gjelder når et barn har vist vedvarende og alvorlige atferdsvansker.
d) Helsepersonell skal varsle politi og brannvesen dersom dette er nødvendig for å avverge alvorlig skade på person eller eiendom.

6.6 Meldeplikt til ulike registre[41]

a) Helsepersonell skal gi opplysninger om fødsler og dødsfall, samt opplysninger til ulike nasjonale helseregistre (se helseregisterloven § 11).

7. Feilkilder

Ingen kjente feilkilder.

8. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten («Normen»)

PR04663 i DocMap: Instruks pasientjournal

[41] Helsepersonelloven §§ 35 - 37

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6910
Versjon: 1

1. Ansatte, kompetanse og holdningsskapende arbeid

Dokumentsamlingen «Ansatte, kompetanse og holdningsskapende arbeid» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Ansatte, kompetanse og holdningsskapende arbeid» består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «05 Ansatte, kompetanse og holdningsskapende arbeid» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord og skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller til adgangsregulerte områder. Det vil si at kravene også gjelder for eksterne konsulenter, studenter og hospitanter.

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

Kravene i dette dokumentet gjelder ikke ansatte hos leverandører som får tilgang til Helse Nords systemer og infrastruktur via leverandørkontoer. Se sikkerhetsområde «15 Leverandørhåndtering».

3. Formål

Helse Nord skal ha tiltak og aktiviteter som skaper en god sikkerhetskultur. Alle medarbeidere skal få opplæring i informasjonssikkerhet, og opplæringen skal i størst mulig grad tilpasses den enkeltes arbeidsoppgaver. Alle medarbeidere skal forstår sitt ansvar og være egnet for den rollen de skal inneha i Helse Nord.

4. Krav ved ansettelse

4.1 Før ansettelse

4.1.1 Det skal gjennomføres en bakgrunnssjekk av alle kandidater før tilbud om tilsetting sendes til medarbeider

a) Bakgrunnssjekken skal være i samsvar med relevante lover, forskrifter og etikk, og skal tilpasses behovet for den konkrete stillingen.
b) Det skal utføres referansesjekk i samsvar var med stillingsbeskrivelse, og i henhold til prosedyre for ansettelse beskrevet i personalhåndboka.
c) For helsepersonell skal det utføres sjekk av helsepersonellregistret (HPR), i samsvar med retningslinje beskrevet i Personalportalen.
d) I de tilfeller det er krav til politiattest, skal dette gjøres i samsvar med beskrivelse i Personalhåndboka.
e) Kontakt personal/HR i ditt helseforetak for utfyllende beskrivelse og/eller der du har behov for bistand om hva som gjelder i konkrete tilsettingssaker.

4.1.2 Alle medarbeidere skal underskrive taushetshets- og egenerklæring

a) Taushetshets- og egenerklæring skal arkiveres i foretakets sak- og arkivsystem
b) Se SJ1473 «Taushets- og egenerklæring i Helse Nord»
c) Se SJ2256 Taushets- og egenerklæring, engelsk versjon»

4.1.3 Alle medarbeidere skal gjøre seg kjent med og ha forstått innholdet i sikkerhetsinstruksen

Relevante regionale retningslinjer:

a) Se RL0259 «Sikkerhetsinstruks»
b) Sikkerhetsinstruks engelsk versjon er under arbeid

4.1.4 Alle medarbeidere skal ha en gyldig avtale før det opprettes en brukerkonto for pålogging til datasystemene

a) Medarbeider skal ha underskrevet en avtale før det gis elektronisk tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller tilgang til adgangsregulerte områder.
b) Med avtale menes ansattkontrakt/ eller annen avtale, se krav 4.1 i sikkerhetsområde «10 Tilgangsstyring».

4.2 Under ansettelsesforholdet – daglig sikkerhetsledelse

Helse Nord skal sikre at alle medarbeidere er bevisst sitt ansvar for informasjonssikkerhet. Informasjonssikkerhet skal være en integrert del av arbeidsprosessene.

4.2.1 Leder er ansvarlig for at medarbeider har forstått sitt ansvar for informasjonssikkerhet

4.2.2 Alle medarbeidere skal gis nødvendig opplæring i informasjonssikkerhet

a) Alle medarbeidere blir tildelt obligatorisk e-læringskurs i informasjonssikkerhet i kompetanseplanen.
b) Leder skal sørge for at alle medarbeidere får nødvendig opplæring i informasjonssikkerhet.
c) Det skal gis opplæring innen informasjonssikkerhet tilpasset den enkeltes arbeidsoppgaver og ansvarsområde.
d) Opplæringen skal som hovedregel foregå i det enkelte helseforetaket. Eksempler på opplæring som bør gjennomføres, i tillegg til det obligatoriske e-læringskurset:
    1. Repeterende og løpende opplæringstiltak for vedlikehold av kompetanse
    2. Tilpasset opplæring til personell med spesielle oppgaver (for eksempel tildeling av autorisasjon, brukerstøtte, riktig bruk av utstyr som inneholder helse- og personopplysninger, driftsrelaterte sikkerhetsaspekter m.m.)

4.2.3 Helseforetakene skal ha oversikt over utstyr som gis til medarbeidere

a) Nærmeste leder skal ha en løpende oversikt over hvilke utstyr den enkelte medarbeider har fått tildelt.
b) Nærmeste leder skal ha en løpende oversikt over hvilke utstyr eksternt personell har fått tildelt.

4.2.4 Sanksjoner ved sikkerhetsbrudd

a) Sikkerhetsbrudd kan få konsekvenser for arbeidsforholdet i henhold til arbeidsreglement.
b) Nærmeste leder skal i samarbeide med HR/ personalavdeling beslutte og iverksette tiltak.

4.3 Ved opphør eller endring i ansettelsesforhold

4.3.1 Leder skal iverksette nødvendige tiltak ved opphør eller endring av ansettelsesforhold

a) Tiltak som minimum skal iverksettes:
    1. Fjerne eller endre tilgangene til en person som slutter, eller endrer rolle
    2. Tilbakelevering av nøkler/adgangskort dersom medarbeideren ikke har behov for disse etter endringen i ansettelsesforholdet
    3. Tilbakelevering av utstyr dersom medarbeideren ikke har behov for disse etter endringen i ansettelsesforholdet

4.3.2 Medarbeider er ansvarlig for å overføre pågående arbeidsoppgaver til relevant personell ved opphør eller endring av ansettelsesforhold

a) Medarbeider har ansvar for å avslutte/overføre arbeidsoppgaver tilstrekkelig, slik at oppgaven kan ferdigstilles.
b) Taushetsplikten gjelder også etter at avtalen med Helse Nord er avsluttet.
c) Med avtale menes ansattkontrakt/ eller annen avtale, se krav 4.1 i sikkerhetsområde «10 Tilgangsstyring».

d) E-post og privat filområde skal ryddes. Virksomhetsrelevant informasjon skal arkiveres, i henhold til helseforetakets arkivreglement.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.7: Human resource security

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

1. Etterlevelse

Dokumentsamlingen «Etterlevelse» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Etterlevelse» består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Etterlevelse» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

3. Formål

Helse Nord skal ha tiltak og aktiviteter for å unngå brudd på juridiske, lovfestede, regulatoriske eller kontraktsmessige forpliktelser knyttet til informasjonssikkerhet, og sikre etterlevelse av sikkerhetskravene i det regionale styringssystemet. Dette betyr at forskjellige kontrollerende tiltak må utføres.

Datatilsynet beskriver kontrollerende dokumentasjon slik:
«Kontrollerende dokumentasjon er dokumenter som har til formål å verifisere at aktivitetene har foregått i samsvar med fastsatte rutiner og instrukser. Eksempler er rapporter, sjekklister og logg. Kontrollerende dokumentasjon kan betraktes som et «sikkerhetsnett» som bidrar til at

styringsdokumentene følges og at eventuelle avvik lettere oppdages. Dokumentene skal ikke være statiske, men endre seg i tråd med virksomhetens utvikling og den rettslige utvikling.»

4. Krav til etterlevelse innen informasjonssikkerhet

4.1 Beskrivelse av sikkerhetskrav

4.1.1 Helse Nord skal identifisere gjeldende lovgivning og kontraktsmessige krav

a) Alle relevante lovfestede, regulatoriske og kontraktsmessige krav skal gjenspeiles i sikkerhetskravene/områdene i dette styringssystemet («01 Styring av informasjonssikkerhet»).
b) Helse Nord skal følge gjeldende lovverk og forskrifter som er relevant for personvern og informasjonssikkerhet.

4.2 Kontroll av etterlevelse

4.2.1 Etterlevelse/kontroll av sikkerhetskrav

For å sikre etterlevelse av sikkerhetskravene i styringssystemet skal §8 Evaluer og §9 Korriger fra forskrift om ledelse og kvalitetsforbedring følges:

Helseforetakene har ansvar for å:

a) §8a: Kontrollere at sikkerhetskravenes mål, oppgaver, tiltak og planer gjennomføres (se MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet)
b) §8b: Vurdere om gjennomføringen av oppgavene, tiltakene og planene er egnet til å etterleve sikkerhetskrav, og om det har ønsket effekt.
c) §8e: Gjennomgå sikkerhetsavvik, slik at lignende forhold kan forebygges (se sikkerhetsområde «07 Avvikshåndtering»)
d) §8f: Minst en gang årlig systematisk gjennomgå og vurdere hele styringssystemet for å sikre at det fungerer som forutsatt (se sikkerhetsområde «01 Styring av informasjonssikkerhet», kap. 4.3 a. 5.)
e) §9a: Rette opp uforsvarlige og lovstridige forhold – lukke avvik (se sikkerhetsområde «07 Avvikshåndtering»)
f) §9b: Sørge for korrigerende tiltak som bidrar til at sikkerhetskravene etterleves. Det er ikke tilstrekkelig å iverksette tiltak uten å sikre at tiltakene faktisk virker.
g) Helseforetakene skal utarbeide dokumentasjon på gjennomført kontroll av etterlevelse, f.eks. i form av sjekklister, rapporter på gjennomført sikkerhetsrevisjon, avviksrapporter, logger etc.

4.2.2 Etterlevelse/kontroll av identiteter

a) Helseforetakene har ansvar for å kontrollere at den registrerte identiteten til medarbeidere er kontrollert i tråd med kravene i sikkerhetsområde «09 Identitetshåndtering»

4.2.3 Etterlevelse/kontroll av tilganger

a) Helseforetakene har ansvar for å kontrollere at tilganger til enhver tid er i tråd med tjenstlig behov, jf. sikkerhetsområde «10 Tilgangsstyring», kap. 4.3 Oppfølging og kontroll av tilganger

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.18 Compliance

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Faktaark nr 6b sjekkliste sikkerhetsrevisjoner, Støttedokument til Norm for informasjonssikkerhet

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6902
Versjon: 1

1. Avvikshåndtering og avviksrapportering

Dokumentsamlingen «Avvikshåndtering og avviksrapportering» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Avvikshåndtering og avviksrapportering» består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Avvikshåndtering og avviksrapportering» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene vil være aktuelle både for informasjonssikkerhetsavvik og forbedringsforslag for informasjonssikkerhet.

3. Formål

Formålet med kravene i dette dokumentet er å gi et grunnlag for å sikre ivaretakelse og etterlevelse av sikkerhetsmål og sikkerhetsstrategi.

Informasjonssikkerhetsavvik er brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet. For å sikre at regelverket følges skal det etableres avviksbehandling slik at årsak til avviket, korrigerende tiltak og rapportering blir dokumentert.

4. Krav til avvikshåndtering og avviksrapportering

4.1 Informasjonssikkerhetsavvik skal rapporteres

a) Den som observerer informasjonssikkerhetsavviket eller eventuelt avdekker avviket, skal melde avviket eller forbedringsforslaget i Helse Nords kvalitetssystem umiddelbart.
b) Helse Nord IKT skal i tillegg følge intern rutine for rapportering til helseforetakene som berører informasjonssikkerhetsavvik.
c) Hvert helseforetak skal følge egne rutiner for håndtering av informasjonssikkerhetsavvik.
d) For hvert rapportert informasjonssikkerhetsavvik skal det foretas en innsamling av fakta om hendelsesforløpet og foretas en vurdering som grunnlag for iverksettelse av korrigerende tiltak.
e) Det skal foreslås tiltak og eventuelle alternative tiltak med beskrivelse av plan for gjennomføring for å gjenopprette normal tilstand og forhindre gjentagelse.
f) Hvert foretak skal sikre at personvernombud varsles om informasjonssikkerhetsavvik.

Eksempler på informasjonssikkerhetsavvik kan være:

1. Utskrift kommer på feil skriver
2. Bærbart utstyr blir stjålet eller tapt på annen måte
3. Personopplysninger ligger åpent tilgjengelig for uvedkommende
4. Bruker går fra arbeidsstasjonen usikret
5. Bruker låner ut brukernavn og passord til andre
6. Autorisert bruker får ikke tilgang
7. Urettmessig tilegnelse av taushetsbelagte opplysninger (snoking)
8. Helse- og/eller personopplysninger blir utlevert til uvedkommende

4.2 Den dataansvarlige skal melde informasjonssikkerhetsavvik til Datatilsynet

Informasjonssikkerhetsavvik som skyldes brudd på personopplysningssikkerheten og det er sannsynlig at bruddet vil medføre en risiko for de registrere sine rettigheter og friheter skal meldes til Datatilsynet. Den dataansvarlige skal vurdere om avviket skal meldes til Datatilsynet. Vurderingen skal dokumenteres.

Informasjonssikkerhetsavvik skal meldes til tilsynsmyndighet uten ugrunnet opphold og innen 72 timer fra det tidspunkt man blir kjent med avviket. Dersom behandlingsansvarlig setter behandling av personopplysninger til databehandler skal partene sees under ett. Det vil si at dersom informasjonssikkerhetsavviket først oppdages hos databehandleren, begynner fristen å løpe når databehandleren ble klar over bruddet. Den behandlingsansvarlige anses altså å være klar over avviket så snart databehandleren er klar over avviket. Dersom melding ikke kan gis innen 72 timer, bør årsaken til forsinkelsen oppgis i meldingen. Avviksmeldingen kan sendes trinnvis.

4.2.1 Innholdet i avviksmeldingen skal som minimum inneholde:

a) En beskrivelse av avviket, hva slags personer og personopplysninger som er berørt
b) Et anslag på hvor mange personer og oppføringer av personopplysninger som er berørt av avviket

c) Kontaktinformasjon til personvernombudet eller et annet kontaktpunkt i virksomheten
d) En beskrivelse av hvilke konsekvenser avviket trolig vil ha
e) En beskrivelse av de tiltak som er (planlagt) iverksatt for å lukke avviket og begrense konsekvensene av det.

4.2.2 Avviket skal rapporteres i henhold til fastsattskjema

a) Skjema er tilgjengelig på https://www.datatilsynet.no/regelverk-og-skjema/avviksbehandling/melde-avvik-til-datatilsynet/
b) Det enkelte helseforetaket skal ha rutiner for hvordan avvik skal rapporteres til Datatilsynet.

4.3 Den dataansvarlige skal varsle de registrerte

a) Varsling til de berørte skal skje når det er sannsynlig at informasjonssikkerhetsavviket vil medføre en høy risiko for personvernet til de som er berørt.
b) Det er imidlertid noen unntak:
   1. Dersom det er iverksatt beskyttelsestiltak for personopplysningene som er omfattet av informasjonssikkerhetsavviket.
   2. Det er truffet tiltak i etterkant som gjør at det er lite trolig at avviket har ført til utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert tilgjengeliggjøring av eller tilgang til personopplysninger
   3. Hvis det er uforholdsmessig vanskelig å varsle hver enkelt av de berørte. I slike tilfeller skal informasjonen i stedet offentliggjøres eller deles på en annen måte, slik at de berørte likevel underrettes på en effektiv måte.

4.3.3 Det skal gis varsel uten ugrunnet opphold, og skal inneholde minimum:

a) En beskrivelse av informasjonssikkerhetsavvikets natur
b) Kontaktinformasjon til personvernombudet eller annet kontaktpunkt
c) En beskrivelse av mulige konsekvenser av informasjonssikkerhetsavviket
d) En beskrivelse av tiltak som er (planlagt) iverksatt for å lukke informasjonssikkerhetsavviket og begrense konsekvensene.

5. Feilkilder

Er det kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen") art. 4, 33 og 34

ISO Internasjonal standard for informasjonssikkerhet 27001/27002, kapittel 10, tillegg A.16

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten, faktaark 41

1. Fysisk sikkerhet og sikring av utstyr

Kravdokumentet «Fysisk sikkerhet og sikring av utstyr» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Fysisk sikkerhet og sikring av utstyr», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Fysisk sikkerhet og sikring av utstyr» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene i dette dokumentet omhandler ikke områder som er regulert gjennom sikkerhetsloven. For dette området gjelder helseforetakenes egne prosedyrer og retningslinjer.

3. Formål

Helseforetakene i Helse Nord skal forhindre at uvedkommende får adgang til informasjon og informasjonssystemer.

4. Fysisk sikkerhet

Fysisk sikkerhet omhandler kun fysisk sikring av utstyr lokalisert i en virksomhet. Elektronisk sikring er ikke inkludert. Mobilt utstyr og hjemmekontor er heller ikke inkludert.

4.1 Adgang til Helse Nords lokaler

Lokalene som Helse Nord disponerer skal deles inn ulike fysiske områder, og sikres utfra hvilke verdier som plasseres i disse områdene.

a) Helse Nord skal sikre konfidensialitet, integritet og tilgjengelighet gjennom å hindre uvedkommende adgang til informasjonssystemene i Helse Nord.
b) Områder som inneholder helse- og personopplysninger aller annen taushetsbelagt informasjon (papirer og elektronisk) skal kartlegges og risikovurderes.
c) Det er helseforetakets ledelse som har det overordnede ansvaret for at risikoen vurderes, men hver klinikk/avdeling er ansvarlig for egne områder.

4.1.1 Åpent område

Åpent område omfatter arealer hvor alle har fri adgang, og som i hovedsak ikke er låst. Eks. korridorer, venterom, pasientrom, fellesarealer, områder med alminnelig ferdsel.

a) Utstyr, inkludert printere, som inneholder helse- og personopplysninger eller annen taushetsbelagt informasjon skal som hovedregel ikke stå i åpne områder.
b) Hvis slikt utstyr må stå i åpne områder skal det gjennomføres en risikovurdering og nødvendige sikkerhetstiltak iverksettes basert på risikovurderingen.
c) Områder for varelevering og -lasting samt andre steder hvor uvedkommende kan komme inn i lokalene, skal kontrolleres for å forhindre uautorisert adgang.

4.1.2 Internt område

Internt område omfatter åpne arbeidsplasser (områder med begrenset ferdsel), arealer beregnet kun for medarbeidere i virksomheten, evt. publikum i følge med medarbeidere - resepsjon, kontorer, vaktrom, behandlingsrom.

a) Prosedyre for fysisk sikring av kontorer, rom og fasiliteter skal utformes og benyttes.
b) Det skal etableres prosedyrer for administrasjon av nøkler/adgangskort.
c) I hvert helseforetak skal det finnes en oversikt over hvem som har adgang til internt og eventuelle sikre områder (se beskrivelse av sikkert område under).

4.1.3 Sikkert område

Med sikkert område menes adgangsregulerte områder hvor kun spesielt godkjente medarbeidere og leverandører har adgang. Eks. medisinrom, operasjonssaler og tekniske styringsrom. Sikkerhetskrav for kommunikasjonsrom er beskrevet i se sikkerhetsområde «18 Sikring av kommunikasjonsrom».

a) Sikre områder skal beskyttes med hensiktsmessige adgangskontroller for å sikre at bare autorisert personell har adgang. Eksempel på hensiktsmessig adgangskontroll er kort + kode.
b) Det skal etableres prosedyrer for administrasjon av nøkler/adgangskort, herunder oversikt over hvem som har tilgang, og til hvilke områder.
c) Prosedyrer for arbeid i sikkert område skal utformes og benyttes.
d) Sikkert område skal beskyttes mot naturkatastrofer, ondsinnede angrep og ulykker.

4.2 Sikring av utstyr

Helse Nord skal forhindre tap, skade, tyveri eller kompromittering av utstyr, samt avbrudd i organisasjonens drift. Se sikkerhetsområde 16 Kontroll på utstyr og verdier i Helse Nords nettverk. Kabling for strøm og telekommunikasjon som fører data eller understøtter informasjonstjenester, skal beskyttes mot avlytting, forstyrrelser eller skade. Det er eier av utstyret som er ansvarlig for at kravene er oppfylt.

4.2.1 Plassering og beskyttelse av utstyr

a) Utstyr skal plasseres og beskyttes på en slik måte at risikoene for uautorisert adgang reduseres.
b) Viktig utstyr med krav til oppe tid skal beskyttes mot strømbrudd og andre avbrudd forårsaket av svikt i understøttende utstyr.
c) Utstyr skal vedlikeholdes i henhold til leverandørens spesifikasjon for å sikre fortsatt tilgjengelighet og integritet.

4.2.2 Fjerning av utstyr

a) Utstyr, informasjon eller programvare skal ikke tas ut av organisasjonen uten forhåndsgodkjennelse.
b) Det skal iverksettes sikringstiltak for utstyr som skal brukes eksternt, der det tas hensyn til de ulike risikoene ved å arbeide utenfor organisasjonens lokaler.
c) Før avhending eller gjenbruk skal alt utstyr som inneholder lagringsmedier kontrolleres for å sikre at alle sensitive data og lisensiert programvare har blitt fjernet eller overskrevet på en sikker måte.

4.2.3 Utstyr uten tilsyn[3]

a) Medarbeidere skal låse eller logge av utstyret når de forlater det, for å hindre at uvedkommende får tilgang til informasjon og/eller misbruk av utstyret.
b) Det skal innføres en retningslinje for rydding av papirer og flyttbare lagringsmedier, samt en låst-skjerm-retningslinje for systemer for informasjonsbehandling.

4.2.4 Hjemmekontor og mobilt utstyr

a) Det skal gjennomføres risikovurdering av de løsninger som skal brukes av medarbeidere i Helse Nord for tilgang via eksternt nett.
b) Helse Nord skal ha utarbeidet prosedyrer for bruk av hjemmekontor og mobilt utstyr. Se RL0260 Hjemmekontor/bærbar PC.
c) Det skal iverksettes egnede sikkerhetstiltak som hindrer at personer som ikke er autorisert får tilgang til helse- og personopplysninger, jf. sikkerhetsområde «10 Tilgangsstyring».
d) Helse Nord skal ha en autentiseringsmetode som kan kontrollere fjernbrukers tilgang.
e) Autentiseringsløsningen som brukes skal ha tilstrekkelig sikkerhet, og skal dokumenteres i en risikovurdering.
f) Helse- og personopplysninger skal i utgangspunktet ikke lagres på mobile/eksterne enheter inkludert minnepinner, og skal i tilfellet alltid krypteres.

g) Helse Nord skal ha teknisk støtte og administrative rutiner som sikrer at helse- og personopplysninger som lagres på mobile og/eller eksterne enheter, inkludert minnepinner alltid lagres kryptert.

5. Feilkilder

Ingen kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven).

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen")

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 tillegg A: A.11 Fysisk og miljømessig sikkerhet.

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet.

Faktaark 17- Fysisk sikring av områder og utstyr.

1. Identitetshåndtering

Dokumentsamlingen «Identitetshåndtering» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Identitetshåndtering», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Identitetshåndtering» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

3. Formål

Helseforetakene skal ha kontroll på identiteten til alle brukere som har tilgang til informasjon, helse- og personopplysninger, systemer og infrastruktur i Helse Nord. Det skal til enhver tid være korrekt identifisert person som er registrert og er gitt tilganger. Dette er nødvendig for å gi tilganger kun i henhold til tjenstlig behov og at riktig person er ansvarlig for handlinger som utføres.

Med identitet menes i dette dokumentet fullstendig navn slik det er registrert i det sentrale folkeregisteret (DSF) og fødselsnummer eller D-nummer (11 siffer).

4. Krav til håndtering av identiteter

4.1 Før tilgang til infrastruktur eller adgangsregulerte områder gis

4.1.1 Personers identitet skal kontrolleres før det gis tilgang til Helse Nords infrastruktur, systemer eller til adgangsregulerte områder

a) Fullstendig navn og fødselsnummer/D-nummer skal kontrolleres ved første gangs registrering av personalia i det regionale lønns- og personalsystemet.
b) For personer som ikke har fødsels- eller D-nummer skal fødselsdato og internasjonal ID registreres i det regionale lønns- og personalsystemet. Kopi av pass, førerkort eller annet ID-kort med bilde skal lagres i sak- og arkivsystemet og være tilgjengelig for inspeksjon.
c) For helsepersonellgrupper som skal tildeles helseperonellnummer, skal helsepersonellnummeret kontrolleres mot helsepersonellregisteret ved første gangs registrering av personens identitet i det regionale lønns- og personalsystemet.
d) Gyldig legitimasjon skal fremvises før påloggingsinformasjon og/eller adgangskort utleveres til bruker. Gyldig legitimasjon er førerkort, bankkort med bilde, nasjonale identitetskort og pass. Det skal sjekkes at identietsbeviset er ekte, gyldig og representerer søker.
e) Gyldig legitimasjon skal fremvises ved endring av ansattforhold der leder ikke kjenner identiteten til den ansatte fra før.
f) Tilgang som **ikke** kan gis i henhold til punktene over skal kun benyttes unntaksvis. De skal alltid dokumenteres, og godkjennes av nærmeste leder. Tilgang som gis på denne måten skal følge dokumterte lokale prosedyrer.
g) Tilgang for leverandører skal følge krav som er beskrevet i sikkerhetsområde «15 Leverandørhåndtering»

4.2 Krav ved bruk av digitale identiteter

4.2.1 En personlig brukerkonto og andre personlige tilganger skal knyttes til én person.

a) Alle medarbeidere med behov for å logge seg på systemene i Helse Nord skal tildeles en personlig brukerkonto.
b) En personlig brukerkonto skal kun benyttes av personen den er tildelt.

4.2.2 Det regionale lønns- og personalsystemet skal være intern kilde til medarbeidernes navn, fødselsnummer/D-nummer, brukernavn og stillingstitler.

a) Det skal utarbeides en regional retningslinje som skal beskrive hvordan informasjon fra den interne kilden skal fødereres til andre systemer.

4.2.3 Personalia og helsepersonellautorisasjon skal kontrolleres regelmessig og ved endring av ansettelsesforhold.

a) Helsepersonells autorisasjon skal kontrolleres mot helsepersonellregisteret (HPR) ved endring i ansettelsesforhold.
b) Helsepersonells autorisasjon skal regelmessig kontrolleres av leder.

c) Ansatte som endrer navn, skal sende forespørsel og gyldig dokumentasjon fra Det sentrale folkeregistret, til leder som videreformidler til lønn og personal.
d) Ansatte som endrer adresse er selv ansvarlig for å registrer dette inn i personalportalen.

4.2.4 Pasienter og andre som har rettigheter på vegne av pasienten, som gis innsyn i helse- og personopplysninger, skal entydig identifiseres.

a) Pasienter og andre som har rettigheter på vegne av pasienten, skal benytte den nasjonale felleskomponenten helsenorge.no for elektronisk tilgang til pasientens helseopplysninger i Helse Nord.
b) Dataansvarlige skal ha egne prosedyrer for identifisering av pasienter ved ikke-elektronisk tilgang til egne helseopplysninger.

5. Feilkilder

Ingen kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL).

Bransjenorm for personvern og informasjonssikkerhet i Helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.9.2.1: Identity management.

Nasjonal sikkerhetsmyndighet (NSM) grunnprinsipper kap 1.1 og 1.2. https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

1. Tilgangsstyring

Dokumentsamlingen «Tilgangsstyring» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Denne retningslinjen, «Tilgangsstyring», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen ««Tilgangsstyring» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere i Helse Nord. Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord og skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller til adgangsregulerte områder.

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

Sikkerhetskravene omfatter ikke leverandørers tilgang til Helse Nords systemer og infrastruktur eller til adgangsregulerte områder. Dette er regulert i HN-ISMS-15 Leverandørhåndtering og HN-ISMS-24 Administratortilganger.

3. Formål

Helse Nord skal sikre at autorisert personell har tilgang til riktig informasjon når de trenger det, og hindre uautorisert tilgang til informasjon. En autorisert person i denne sammenheng er en som har blitt tildelt tilgang basert på tjenstlig behov.

4. Krav til tilgangsstyring

4.1 Autorisering

Med autorisering menes her tildeling av rettigheter og tilganger til informasjon, helse- og personopplysninger, systemer og infrastruktur i Helse Nord.

4.1.1 Tilgang kan bare tildeles personer som har en gyldig avtale med et av foretakene i Helse Nord

a) Fast ansatte og vikarer skal ha signert ansattkontrakt og taushetserklæring før påloggingsinformasjon og/eller adgangskort utleveres.
b) Innleide fra vikarbyrå eller andre virksomheter som Helse Nord har avtale med skal oppfylle kravene i denne avtalen. Dette inkludert signering av taushetserklæring som tilfredsstiller Helse Nords krav til taushetsplikten, før påloggingsinformasjon og/eller adgangskort utleveres.
c) Alle medarbeider som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur eller til adgangsregulerte områder skal gjennomføre obligatorisk opplæring i informasjonssikkerhet. Nærmeste leder er ansvarlig for at slik opplæring blir gitt. Se også sikkerhetsområde «05 Ansatte, kompetanse og holdningsskapende arbeid».
d) Personer som ikke omfattes av et ansettelses- eller innleieforhold (f.eks. studenter og hospitanter), men som skal ha midlertidig tilgang til informasjon, helse- og personopplysninger, systemer og infrastruktur i Helse Nord, og/eller adgangsregulerte områder, skal registreres med et forenklet arbeidsforhold i personalsystemet. Vedkommende skal ha undertegnet taushetserklæring og gis nødvendig opplæring i informasjonssikkerhet før påloggingsinformasjon og/eller adgangskort utleveres.
   Nærmeste leder, eller den som koordinerer oppdraget, er ansvarlig for at slik opplæring blir gitt. Se også sikkerhetsområde «05 Ansatte, kompetanse og holdningsskapende arbeid».
e) For administratortilganger, se sikkerhetsområde «24 Administratortilganger».
f) Kravene gjelder ikke for Helse Nord sine systemer og tjenester som er åpent tilgjengelig på Internett for innbyggere eks pasienter og pårørende. Det er ikke krav at disse skal ha en gyldig avtalte med Helse Nord før de kan ta i bruk disse tjenestene for eksempel på Helsekompetanse.no eller Campus.

4.1.2 Forvaltning av brukertilganger (tildeling, endring eller inndragelse av tilgangsrettigheter) for alle typer brukere skal skje i henhold til dokumentert prosedyre

a) Dataansvarlig er ansvarlig for at det foreligger en dokumentert prosedyre for hvordan tildeling, endring og inndragelse av tilganger skal foregå.
b) Nærmeste leder er ansvarlig for at tilganger tildeles i henhold til dokumentert prosedyre.
c) Nærmeste leder er ansvarlig for at tilgang til informasjon og datasystemer fjernes ved opphør av ansettelsesforholdet, kontrakten eller avtalen, og korrigeres ved endringer.
d) Alle tilganger skal være basert på tjenstlig behov, og i tråd med krav i EPJ standarden der det er relevant.
e) Alle brukere skal ha tilgang til systemer og tjenester som bare inneholder informasjon i informasjonsklassene 1 (åpen) og 2 (intern) (Sett inn lenke til «Regional retningslinje for sikring av informasjon»[1]).
f) Tilganger skal være tidsbegrenset for vikarer og annet innleid personell, og skal ikke overskride avtaleforholdets varighet.
g) Tildeling og endringer i tilganger og hvem som beslutter endringer i tilganger, skal loggføres.

4.1.3 Studenters brukertilganger skal forvaltes i tråd med dokumenterte prosedyrer og rutiner

Målsetningen er å gi studenter nødvendig tilgang til datasystemer og helseopplysninger i tråd med gjeldende regelverk.

a) Foretak som gir studenter tilgang til datasystemer og tjenester skal ha dokumenterte prosedyrer og rutiner for tildeling og forvaltning av tilgangene.

[1] http://boo-hndcm-01.hn.helsenord.no/DocMapProd/page/doc/dmDocIndex.html?DOCKEYID=597228

4.1.4 Brukernes tilgangsrettigheter skal gjennomgås regelmessig (minimum årlig), og tilganger som ikke lenger oppfyller kravet om tjenstlig behov skal inndras

a) Nærmeste leder skal sørge for regelmessig kontroll av tilganger. Dette gjelder også for tilgang til helse- og personopplysninger på utstyr som ikke er tilkoblet Helse Nord sin infrastruktur. Se også Sikkerhetsområde «05 Ansatte, kompetanse og holdningsskapende arbeid», og sikkerhetsområde «06 Etterlevelse».

4.2 Pålogging (autentisering)

Formålet med autentisering er å sikre at det er rett person som gis tilgang, og at det er mulig å spore i ettertid hvem som har hatt tilgang eller har gjort endringer.

4.2.1 Det skal være en felles sentral autentiseringsløsning for pålogging til arbeidsflate i Helse Nord

Med arbeidsflate menes brukergrensesnittet brukeren får tilgang til ved pålogging på PC eller annen enhet i Helse Nord, eller ved tilgang via eksternt nett.

a) Pålogging på stasjonær PC, eller annen enhet som står i Helse Nords infrastruktur skal gjøres med brukernavn og passord, eller to-faktorautentisering, som sjekkes mot regionens sentrale autentiseringstjeneste. For krav til passord se egen prosedyre, se også PR04628 Prosedyre for tilgangsstyring og passord policy i Helse Nord.
b) Pålogging til Helse Nords infrastruktur via eksternt nett, f.eks. fra internett eller et av Helse Nords gjestenett, skal gjøres ved bruk av minimum to-faktorautentisering, og denne skal sjekkes mot regionens sentrale autentiseringstjeneste.
c) Ved bruk av smartkort for to-faktorautentisering skal ansattkortet benyttes som bærer for autentiseringsnøkkelen/-sertifikatet.

4.2.2 Tilgang til Helse Nord sin regionale infrastruktur/datasystemer skal som hovedregel baseres på to-faktorautentisering

a) Tilgang til helse- og personopplysninger skal som hovedregel baseres på to-faktorautentisering.
b) Tilgang til datasystemer i Helse Nord uten bruk av to-faktorautentisering skal som minimum være basert på personlig brukernavn og passord, som er registrert i AD, med unntak av fellesbrukerkontoer (se 4.2.5).
c) For systemer der to-faktorautentisering ikke iverksettes, skal det gjennomføres risikovurdering for å fastslå hvilke andre tiltak, som for eksempel utstyr plasseres i låst rom, kun mulig å logge på ved å sitte fysisk ved en gitt arbeidsstasjon, nettverksmessig isolasjon m.m., som må gjennomføres for å redusere risikoen til et akseptabelt nivå. Dataansvarlig skal fastsette akseptabelt risikonivå.
d) Tilgang til helse- og personopplysninger via portalløsninger og skyløsninger for pasienter og innbyggere skal skje ved med minimum to-faktorautentisering.

4.2.3 Passord som benyttes i Helse Nord skal tilfredsstille definerte krav

a) Helse Nord skal ha felles krav til utforming av passord. Se PR04628 Prosedyre for tilgangsstyring og passord policy i Helse Nord.

4.2.4 Nytt passord skal utleveres i henhold til Helse Nords fastsatte rutine

a) Helse Nord skal ha felles krav for utlevering av passord. Se

PR04628 Prosedyre for tilgangsstyring og passord policy i Helse Nord - Rutine for utlevering av nytt passord (kap 6.9).

4.2.5 Fellesbrukerkontoer skal kun opprettes for formål som krever slik konto, og kun benyttes i tråd med etablerte retningslinjer

En fellesbrukerkonto er en brukerkonto som ikke er personlig men som flere medarbeidere kan benytte (med samme brukernavn og passord). Fellesbrukerkontoer skal normalt ikke benyttes.

a) En fellesbrukerkonto kan bare benyttes på *en* (1) forhåndsdefinert PC.
b) Passord til fellesbrukerkontoer skal ikke deles med andre enn de som er autorisert for tilgang til den aktuelle fellesbrukerkontoen.
c) Fellesbrukerkonto skal ikke være autorisert for tilgang til internett eller e-post.

4.3 Oppfølging og kontroll av tilganger

Det skal foreligge både tekniske og organisatoriske tiltak for å oppdage uautorisert bruk eller forsøk på uautorisert bruk av helse- og personopplysninger.

4.3.1 Helseforetakene skal ha dokumenterte prosesser for å oppdage uautorisert bruk og forsøk på uautorisert bruk av helse- og personopplysninger

a) Helseforetakene skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt tilgang til helse- og personopplysninger.
b) Dataansvarlig er ansvarlig for at det foreligger en dokumentert og oppdatert prosedyre for loggføring og kontroll av innsyn i pasientens journal (behandlingsrettede helseregister). For DIPS se PR 1573.
c) Dataansvarlig er ansvarlig for at punktene i prosedyren følges, og at det utarbeides lokale rutiner ved behov for ytterligere presisering.
d) Dersom kontrollen av det uforklarlige innsynet viser at det har skjedd en urettmessig tilgang, skal dette håndteres som et avvik. Se sikkerhetsområde «07 Avvikshåndtering».

4.3.2 I Helse Nord skal det legges til rette for at pasient/innbygger kan få digitalt innsyn i hvem som har hatt tilgang til deres helse- og personopplysninger

a) Pasientene i Helse Nord skal, i størst mulig grad, ha elektronisk tilgang til egne helseopplysninger, herunder innsynslogger i spesialisthelsetjenesten, via helseportalen www.helsenorge.no.
b) Innsynsloggen skal vise en oversikt over hvem som har gjort oppslag i pasientens journal.

4.3.3 Det skal legges til rette for etablering av maskinelle analyser for identifisering av unormal bruk av pasientjournaler (mønstergjenkjenning)

a) Helse Nord skal følge nasjonale prosesser for anskaffelse av maskinelle analyser for identifisering av unormal bruk av pasientjournaler

5. Feilkilder

Det er ingen kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen")

Norm for personvern og informasjonssikkerhet Helse- og omsorgstjenesten

Veileder for tilgangsstyring, Veilederen er et støttedokument til Norm for informasjonssikkerhet
Faktaark nr 14 tilgangsstyring, Støttedokument til Norm for informasjonssikkerhet

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.9: Access control

EPJ standarden HIS 800505:2015

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6903
Versjon: 1

1 Beredskapsplanlegging helseforetak

Dokumentsamlingen «Beredskapsplanlegging helseforetak» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».
Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318».
Dette kravdokumentet, «Beredskapsplanlegging helseforetak», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.
Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Beredskapsplanlegging helseforetak» henger nøye sammen, og må derfor ses på under ett.

2 Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.
Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.
Med Helse Nord menes hele foretaksgruppen med alle helseforetakene og det regionale helseforetaket.
Kravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

3 Formål

Beredskapsplanlegging som omfatter informasjonssikkerhet skal være naturlig del av helseforetakenes beredskapsplaner.

4 Krav til beredskapsplanlegging helseforetak

4.1 Beredskap – og kontinuitetsplanlegging helseforetak

Helse nord skal ha fastsatte krav til informasjonssikkerhet og kontinuitet i uforutsette situasjoner som for eksempel ved krise eller katastrofe.

a) Hvert helseforetak skal ha egne beredskapsplaner, hvor krav til informasjonssikkerhet og kontinuitetsplanlegging for IKT skal inngå.
b) Helseforetakene skal ha dokumentert hvor lang tid det vil gå for reetablering av tjenester og plattform ved tekniske brudd, eller bortfall.
c) Krav til kontinuitet i normal drift ivaretas i sikkerhetsområde (Ida setter inn navn).
d) Helseforetaket eier og forvalter egne beredskapsplaner.

e) Helseforetaket er ansvarlig for at lokale beredskapsplaner er koordinert med regional beredskapsplan, beredskapsplanene til Helse Nord IKT, og andre relevante samarbeidspartnere.

4.2 Implementering av beredskapsplanlegging helseforetak

Det skal være innarbeidede, dokumenterte og oppdaterte prosesser, og kontroller for å sikre at fastsatt kontinuitetsnivå for informasjonssikkerhet også opprettholdes under en eventuell uforutsett situasjon.

a) Beredskapsplanene skal være kjent i egen organisasjon.
b) Alle som har en rolle i helseforetakets beredskapsorganisasjon skal være kjent med hva rollen faktisk innebærer.
c) Helseforetakene er ansvarlig for opplæring i forbindelse med beredskapsarbeidet i egen organisasjon.

4.3 Verifikasjon av beredskapstiltak

Helseforetakene skal gjennomføre rutinemessige kontroller av informasjonssikkerhet i beredskapsplanene for å sikre at de har en effektiv krisehåndtering.

a) Beredskapsplaner skal øves jevnlig.
b) Beredskapsplaner skal oppdateres etter hver øvelse og fortløpende ved endringer.

4.4 Nødprosedyrer

a) Helseforetakene skal ha prosedyrer for å sikre at vitale kliniske funksjoner opprettholdes ved bortfall av IKT-tjenester, herunder å sikre at pasientjournaler og annen nødvendig informasjon er tilgjengelig.
b) Nødprosedyrene skal være en del av helseforetakets beredskapsplan.
c) Helseforetakene skal kontrollere at Helse Nord IKT eller annen driftsleverandør, har tiltak som kan stenge risikoutsatte tilganger, slik at de ikke er tilgjengelig for uautoriserte i en eventuell hendelse.

5 Feilkilder

Ingen kjente feilkilder

6 Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.17: Information security aspects of business continuity management

Bransjenorm for informasjonssikkerhet og personvern i Helse – og omsorgstjenesten

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6904
Versjon: 1

1 E-post, sms, skype og sosiale medier

Dokumentsamlingen «E-post, sms, skype og sosiale medier» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «E-post, sms, skype og sosiale medier» består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «E-post, sms, skype og sosiale medier» henger nøye sammen, og må derfor ses på samlet.

2 Omfang

Sikkerhetskravene og retningslinjene som er beskrevet i dette dokumentet gjelder for alle medarbeidere i Helse Nord.

Med medarbeidere menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse – og personopplysninger, systemer og infrastruktur eller adgangsregulerte områder.

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

3 Formål

I Helse Nord skal det legges til rette for at administrative verktøy brukes riktig. Den enkelte medarbeider er ansvarlig for å etterleve de krav som til enhver tid er gjeldene.

Kravene i «E-post, sms, skype og sosiale medier» skal sikre at opplysningene til Helse Nord behandles korrekt, og i samsvar med relevant regelverk.

4 Krav til bruk av e-post, sms, skype og sosiale medier

4.1 Krav til bruk av e-post

4.1.1 Helseforetaket er ansvarlig for å beskrive og informere egne medarbeidere om hva e-post kan, og ikke kan benyttes til

a) Din e-postadresse hos Helse Nord er personlig, og skal ikke benyttes av andre.
b) Begrens bruk av din e-postadresse hos Helse Nord til private formål.
c) Private e-post legges i en egen mappe merket Privat.
d) Alle som har tilgang til Helse Nord sitt e-postsystem skal stå oppført i adresselisten
e) Ved lengre fravær skal automatiske fraværsmeldinger benyttes, med henvisning til hvem som kan kontaktes i ditt fravær.
f) Automatisk videresending til e-postkonto utenfor Helse Nord er ikke tillat.
g) E-post adressert til rolle eller funksjon bør rettes til felles e-postbokser
h) For arbeidsgivers innsyn i medarbeiders e-post vises det til egen retningslinje. Se PR31593 Innsyn i e-post og personlig område
i) Etter endt ansettelsesforhold slettes innholdet i e-postkonto. Se sikkerhetsområde «05 Ansatte, kompetanse og holdningsskapende arbeid».
j) Det skal vises varsomhet ved mottak av e-post. Vedlegg kan inneholde virus. Ved tvil skal avsender eller Helse Nord IKT kontaktes. Slike e-postmeldingene skal slettes.
k) Ved mistanke om svindelforsøk (spam, whaling, phishing etc) kan Helse Nord IKT slette e-post uten å involvere brukeren.
l) Dersom du venter en e-post, som avsender har sendt, men som ikke er kommet frem til deg bør du først sjekke mappen «Useriøs e-post/Søppelpost». Dersom e-posten ikke ligger i denne mappen må du kontakte Helse Nord IKT brukerstøtte via «Gohjelp».
m) Dobbeltsjekk mottakeradressen. Gjør det til en god vane å kontrollere adresser og vedlegg før du trykker på send.

4.1.2 Standard e-post skal ikke benyttes til kommunikasjon av sensitive personopplysninger

Bruk av e-post kan sammenlignes med å sende et postkort. Standard e-post er ikke kryptert. Dette gjelder også om det sendes e-post intern i Helse Nord sitt nettverk.

a) Opplysninger som omfattes av lovbestemt taushetsplikt, som f.eks. helseopplysninger skal ikke sendes i åpen e-post[1]. Dette gjelder både standard e-post som sendes internt og ekstern.
b) Det er heller ikke lov å sende fødselsnummer (11 siffer) på denne måten.
c) Dersom du som medarbeider mottar en e-post som inneholder taushetsbelagt informasjon, for eksempel helseopplysninger og/eller sensitive personopplysninger, skal ikke denne e-posten besvares eller videresendes før disse opplysningene er fjernet.

4.1.3 Helseforetaket skal iverksette egnede tiltak for å forhindre at sensitive personopplysninger formidles ved hjelp av standard e-post

a) Helseforetakenes nettsted skal gjøre pasienten oppmerksom på risikoen ved å sende sensitive personopplysninger eller helseopplysninger via standard e-post.

[1] Lovbestemt taushetsplikt helsepersonelloven §21 og forvaltingsloven § 13

1. Det skal henvises til en sikker kommunikasjonsløsning. For eksempel telefon eller Min helse på helsenorge.no.
2. Det skal også opplyses om at henvendelser som inneholder sensitive personopplysninger eller helseopplysninger vil ikke bli besvart, men at det må benyttes telefon, sikre kommunikasjonskanaler eller at kontakt må tas ved personlig fremmøte.

b) Klargjøre internt i virksomheten at dersom helseforetaket likevel mottar e-post som inneholder helse - og personopplysninger fra pasient / bruker, skal ikke slike henvendelser besvares. Foretakene skal ha egne rutiner for håndtering av dette.
c) For kommunikasjon til pasienter, og ved kommunikasjon som inneholder sensitive personopplysninger skal det benyttes løsninger som sørger for sikker kommunikasjon, for eksempel via en egnet løsning som sørger for at sensitive personopplysninger ikke overføres ukryptert.
d) Ved behov for å sende sensitive personopplysninger via e-post, skal det benyttes godkjente krypteringsløsninger.
e) Før nye kommunikasjonsløsninger tas i bruk skal disse risikovurderes og godkjennes av sikkerhetsansvarlig i helseforetaket.
f) Ved kommunikasjon til pasienter, og ved kommunikasjon som inneholder sensitive personopplysninger skal det iverksettes egnede tiltak slik at sensitive personopplysninger ikke automatisk blir liggende på brukerens lokale PC.

4.2 SMS i kontakt med pasienten/brukeren

4.2.1 SMS kan benyttes i kommunikasjon med pasienten/brukeren

a) Helseforetakene som tar i bruk slike tjenester skal ha egne rutiner for håndtering av dette.
b) Før SMS-varsling benyttes skal det være innhentes samtykke fra pasienten.[2]
c) Enkel timebestilling kan kommuniseres på SMS.
d) Opplysninger som omfattes av lovbestemt taushetsplikt, som f.eks. helseopplysninger og/eller sensitive personopplysninger, skal ikke sendes i SMS.
e) Angivelse av poliklinikk eller sted på sykehuset for oppmøte kan avsløre en diagnose og må derfor ikke sendes på SMS.
f) Nærmere beskrivelse se «Regionale retningslinjer for bruk av SMS i pasientkontakt PR11703»

Se for øvrig Normens veileder «personvern og informasjonssikkerhet i kontakt med pasient/bruker»

4.3 Skype for Business til kliniske formål

[2] Dersom pasient/bruker har oppgitt digital kontaktinformasjon kan dette anses som et stilltiende samtykke til at virksomheten kan sende timepåminnelser per SMS. Pasienten skal i innkallingsbrev informeres om hvilket mobilnummer som er registrert, samt hvordan man går frem om man f.eks ikke ønsker å motta påminnelse om timer

For å oppnå tilfredsstillende informasjonssikkerhet ved bruk av Skype 4B for kliniske formål, er det noen absolutte sikkerhetskrav som alltid skal følges.

a) Det skal alltid innhentes samtykke fra bruker/ pasient
b) Entydig identifisering av helsepersonell og bruker/pasienten
c) Tekniske tiltak for å sikre at kommunikasjonen alltid er ende- til ende- kryptert.
d) Adskille pasientene – Det skal ikke kunne kommuniseres samtidig med andre parter enn den angitte brukeren/ pasienten.
e) Nærmere beskrivelse se RL5765 «Regionale retningslinjen for bruk av Skype 4B til klinisk bruk.»
f) Dersom Skype 4B til klinisk bruk skal brukes på annen måte enn det som er beskrevet i denne retningslinjen, skal det gjennomføres en risikovurdering. Hvordan løsningen brukes og til hva vil påvirke hvilke scenarioer som kan oppstå.

4.4 Internett og sosiale medier

Internett skal benyttes i samsvar med etiske retningslinjer for Helse Nord[2]. Virksomhetsrelaterte oppgaver og funksjoner, samt opplysninger virksomheten behandler, skal ikke bli skadelidende. Aktiviteter på Internett kan spores tilbake til virksomheten og den PC/brukerkonto oppslaget er utført fra.

Ved bruk av sosiale media er den enkelte ansvarlig for at taushetsplikten blir overholdt og at pasienters og ansattes integritet blir ivaretatt. Taushetsplikten gjelder også informasjon om at noen *er* eller *har vært* pasient hos oss. Vi kan derfor ikke legge ut informasjon av typen: «Traff Kari Nordmann på venterommet i dag.

Dersom den enkelte vil kunne oppfattes som representant for virksomheten, skal det alltid presiseres at uttalelsen står for egen regning hvis personlige synspunkter fremmes. Helse Nord har utarbeidet en veileder for ansatte vedrørende bruk av sosiale medier (RL3934).

5 Feilkilder

Ingen kjente feilkilder

6 Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.18 Compliance

Informasjonssikkerhet ved bruk av private leverandører EL- 1012

Norm for personvern og informasjonssikkerhet i helse- og omsorgstjenesten

Faktaark: Personvern og informasjonssikkerhet i kontakten med pasient/bruker - En veileder i bruk av portalløsninger, SMS og e-post Støttedokument til Norm for informasjonssikkerhet

Dokumentansvarlig: Ida-Kristin Martinussen
Godkjent av: Hilde Rolandsen
Gyldig for: Helse Nord
Dokumentnummer: RL6917
Versjon: 1

1. Overføring av personopplysninger til utlandet

Dokumentsamlingen «Overføring av personopplysninger til utlandet» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Overføring av personopplysninger til utlandet», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Overføring av personopplysninger til utlandet» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

For overføring av forsknings- og kvalitetsprosjekter gjelder egne prosedyrer og retningslinjer. Personvernombud ved ditt foretak kan kontaktes for nærmere informasjon.

3. Formål

Formålet med dokumentet er å sikre at informasjonssikkerhet og personvern ivaretas ved overføring av opplysninger til utlandet.

4. Krav for bruk av private leverandører

4.1 Før Helse Nord kan ta i bruk private leverandører må følgende punkter gjennomføres:

a) Leverandøren skal dokumentere eget internkontroll- og styringssystem, organisering og løsninger for ivareta informasjonssikkerheten
b) Informasjonssikkerhetsrisiko ved bruk av aktuell leverandør skal vurderes.
Se sikkerhetsområde «03 Risikovurdering og risikostyring»
Personvernkonsekvenser skal vurderes når leverandør skal behandle personopplysninger. Dersom det ikke er behov må det dokumenteres særskilt. Se sikkerhetsområde «03 Risikovurdering og risikostyring»
c) Dataansvarlig skal beslutte at leverandøren kan brukes.
d) Se sikkerhetsområde «15 Leverandørhåndtering»

4.2 Før Helse Nord kan overføre personopplysninger til utlandet gjelder i tillegg:

4.2.1 Dersom landet er en del av EU/EØS

Landene innenfor EU/EØS-området er anerkjent som stater som sikrer at personopplysninger behandles forsvarlig.

a) Det er kun tillatt å overføre personopplysninger til land som er en del av EU/EØS forutsatt at personopplysningslovens vilkår er oppfylt og punktene i 4.1 er gjennomført.

4.2.2 Dersom landet er utenfor EU/EØS og er forhåndsgodkjent av Europakommisjonen

Overføring av personopplysninger kan bare skje til stater som sikrer en forsvarlig behandling av opplysningene. Enkelte land utenfor EU/EØS har blitt forhåndsgodkjent av Europakommisjonen.

a) Det er kun tillat å overføre opplysninger til land som er godkjent på lik linje med land innenfor EU/EØS, og at punkt 4.1 er gjennomført.

4.2.3 Overføring av opplysninger til USA

Personopplysninger kan overføres til USA dersom mottakervirksomheten har sertifisert seg etter Privacy Shield-avtalen. Virksomhetene som deltar i programmet har underlagt seg særlige regler for beskyttelse av personopplysninger.

a) Overføring av personopplysninger til amerikanske selskaper som ikke har sluttet seg til Privacy Shield, må basere seg på vilkårene som gjelder for øvrige tredjeland (se nedenfor).
b) Før personopplysninger kan overføres til virksomheten må det kontrolleres om virksomheten står oppført på listen[1] over Privacy-Shield sertifiserte virksomheter.
c) Listen oppdateres årlig. Dataansvarlig skal årlig kontrollere listen for å sjekke om leverandøren som det overføres personopplysninger til fortsatt er en del av Privacy Shield.

4.2.4 Land utenfor EU/EØS som ikke er forhåndsgodkjent av Europakommisjonen (tredjeland)

Overføring til land som ikke er godkjent av Europakommisjonen kan kun skje på visse vilkår.

[1] https://www.privacyshield.gov/welcome

a) Det skal søkes tillatelse til Datatilsynet. Man må kunne gi tilstrekkelige garantier for vern av den registrertes rettigheter.
b) EUs standardkontrakter skal brukes. Dersom man bruker EUs standardkontrakt[2] for overføring til databehandler, trenger man ikke søke Datatilsynet om tillatelse. Da er det tilstrekkelig å varsle Datatilsynet før overføringen finner sted. For at standardkontrakten skal kunne danne et grunnlag for overføring til land utenfor EU/EØS kan det ikke gjøres noen endringer i kontraktsvilkårene.
c) Datatilsynet skal godkjenne den endrede kontrakten dersom avtalepartene gjør endringer i standardvilkårene før data overføres til databehandler i tredjeland.

I alle tilfeller må personopplysningslovens krav til behandling av personopplysninger være oppfylt. Reglene om behandling til utlandet kommer ikke i stedet for, men i tillegg til de øvrige kravene som personopplysningsloven stiller.

5. Feilkilder

Er det kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

ISO Internasjonal standard for informasjonssikkerhet 27001/27002

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten https://ehelse.no/Documents/E-helsekunnskap/Informasjonssikkerhet%20ved%20bruk%20av%20private%20leverand%C3%B8rer%20i%20helse%20og%20omsorgstjenesten.pdf

Veileder i bruk av skytjenester ved behandling av helse og personopplysninger Støttedokument til Norm for informasjonssikkerhet

[2] https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/overfore/

1. Innebygd personvern og personvern som standardinnstilling

Dokumentsamlingen «Innebygd personvern og personvern som standardinnstilling» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Innebygd personvern og personvern som standardinnstilling», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Innebygd personvern og personvern som standardinnstilling» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Kravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Det er spesielt viktig at alle utviklere, arkitekter, prosjektledere, testere, rådgivere innen personvern og informasjonssikkerhet som utvikler, og bidrar til utvikling av og tester programvare som inneholder personopplysninger kjenner til disse personvernprinsippene. Prinsippene skal også være kjent og etterleves av helsepersonell og medarbeidere som utfører arbeidsoppgaver der det behandles helse- og personopplysninger.

3. Formål

For å ivareta gjeldende regelverk for informasjonssikkerhet og personvern, skal personvern og informasjonssikkerhet være en integrert del av alle løsninger i Helse Nord. Formålet med dokumentet er å gi en innføring i prinsipper som omfattes av begrepet «innebygd personvern.» Konkrete krav til innebygd personvern vil gjengis i andre dokumenter.

Helse Nord skal sikre at personvern og informasjonssikkerhet er en del av alle utviklingsfaser av et system eller en løsning, jf. sikkerhetsområde «22 Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare».

Informasjonssystemene som Helse Nord bruker skal oppfylle personvernprinsippene, og de skal ivareta de registrertes1 rettigheter, jf. sikkerhetsområde «04 Personvern og pasientrettigheter».

4. Prinsipper for innebygd personvern

Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning, slik at løsningen eller systemet på en naturlig måte legger til rette for at personvernet blir ivaretatt ved bruk.

4.1 Vær i forkant, forebygg fremfor å reparere

For å lage en personvernvennlig løsning, er det viktig å vurdere risikoene og konsekvenser for personvernet så tidlig som mulig i utviklingsprosessen. Dersom man tar hensyn til personvernet tidlig i utviklingen, kan man unngå unødvendige krenkelser av personvernet.

4.2 Gjør personvern til standardinnstilling

Standardinnstillinger er førende for hvordan et system blir brukt, og hvordan personopplysninger blir lagret. For at et system skal ha innebygd personvern, må standardinnstillingene settes opp slik at ikke flere personopplysninger enn nødvendig samles inn eller vises, at det finnes et lovlig formål med innsamlingen, at det er satt tekniske begrensninger for bruken av opplysningene, at opplysningene slettes når formålet er oppnådd, og at det legges til rette for at den registrerte får innsyn i de opplysninger som er registrert på seg selv. Et slikt system vil automatisk styre brukeren til en arbeidsmåte som gir bedre personvern.

4.3 Bygg personvern inn i designet

Personvern skal være innebygd i systemer og løsninger. Det skal ikke være en funksjon lagt til i etterkant. Dermed blir personvernet en viktig del av kjernefunksjonaliteten. Det vil si at personvern er en integrert del av løsningen uten at det går på bekostning av funksjonaliteten.

4.4 Skap full funksjonalitet

Gjennom innebygd personvern ivaretar man både brukerens personvern og virksomhetens behov. Det er viktig å ta hensyn til personvernet fra start for å unngå reparasjoner som går utover funksjonaliteten til løsningen.

[1] Med «registrert» menes den som personopplysninger kan knyttes til.

4.5 Ivareta informasjonssikkerheten fra start til slutt

Personvern **skal** være del av hele prosessen med å behandle helse- og personopplysninger. Det betyr at alt som skjer i et system på forhånd er risikovurdert og konsekvensene er utredet. Systemet skal være hensiktsmessig sikret, helt fra før personopplysningene samles inn, mens de behandles, og til de er slettet. Personopplysningene skal sikres mot uautorisert tilgang, endring, ødeleggelse og spredning.

4.6 Vis åpenhet

Det skal være åpenhet om hvordan systemet fungerer, og hvordan personvernet blir ivaretatt. Virksomheten skal sørge for at brukerne får god informasjon og at det legges til rette for innsyn i egne opplysninger. Det skal være mulig å kontrollere at systemet ivaretar personvernet slik leverandøren oppgir.

4.7 Respekter brukerens personvern

Innebygd personvern krever at alle gir den registrertes personvern høy prioritet. Dette vil si å sørge for at personvernet ivaretas gjennom standardinnstillinger, tydelige brukervilkår, og løsninger for at brukeren skal kunne kontrollere opplysningene sine selv.

5. Feilkilder

Er det kjente feilkilder

6. Eksterne referanser

Lov om behandling av personopplysninger (personopplysningsloven)

EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation) (heretter omtalt som "personvernforordningen").

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten

Datatilsynet
https://www.datatilsynet.no/regelverk-og-skjema/veiledere/grunnleggende-personvernprinsipper-etter-nytt-regelverk/?id=7770

https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/

Veileder om programvareutvikling med innebygd personvern
Sjekkliste for krav https://www.datatilsynet.no/globalassets/global/regelverk-skjema/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf

Sjekkliste for koding: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/?id=7735

Dokumentansvarlig: Jan Harald Solberg
Godkjent av: Frank Daniel Fredriksen
Gyldig for: Helse Nord
Dokumentnummer: RL6905
Versjon: 1

1. Leverandørhåndtering

Dokumentsamlingen «Leverandørhåndtering» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Leverandørhåndtering», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Leverandørhåndtering» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene i dette dokumentet gjelder leverandører eller tredjepart som skal få eller har tilgang til helse- og personopplysninger, systemer og enheter i Helse Nords infrastruktur. Kravene er utviklet for å beskytte IKT-infrastrukturen og opplysninger leverandører får tilgang til.

Kravene gjelder alle leverandører som skal ha tilgang til Helse Nord sin informasjonsverdier, infrastruktur, enheter, programvare, herunder helse- og personopplysninger. Kravene gjelder også leverandørkjeder (supply chain) og kommer i tillegg til krav som gjelder leverandører i de andre sikkerhetsområdene, herunder anskaffelser, utvikling og endring.

3. Formål

Helse Nord skal ha kontroll på alle leverandører og deres digitale tilganger i Helse Nords infrastruktur. Det skal være tilsvarende kontroll på administratortilganger for leverandører som for egne medarbeidere, se sikkerhetsområde «24 Administratortilganger».

For leverandørtilganger skal kravene sikre at leverandører utelukkende har tilgang til det som er avtalt gjennom databehandleravtaler eller sikkerhetsavtaler.

Ved fysisk tilgang til lokaler gjelder kravene i sikkerhetsområde «08 Fysisk sikkerhet og sikring av utstyr».

Kravene skal samlet forhindre uautorisert tilgang til systemer og opplysninger, samt uautorisert eller uaktsom utlevering, modifisering, fjerning eller ødeleggelse av informasjon.

4. Krav til leverandører

4.1 Leverandørtilganger

4.1.1 Leverandører skal vurderes og godkjennes før bruk

a) Leverandøren skal dokumentere eget internkontroll- og styringssystem, organisering og løsninger for ivareta informasjonssikkerheten
b) Informasjonssikkerhetsrisiko ved bruk av aktuell leverandør skal vurderes. Se sikkerhetsområde «03 Risikovurdering og risikostyring».
c) Personvernkonsekvenser skal vurderes når leverandør skal behandle personopplysninger. Dersom det ikke er behov må det dokumenteres særskilt. «03 Risikovurdering og risikostyring».
d) Dataansvarlig skal beslutte at leverandøren kan brukes.

4.1.2 Leverandører skal ha gyldig avtale før det gis tilgang til IKT-infrastrukturen og helse- og personopplysninger

a) Leverandører skal ha gyldig databehandleravtale eller sikkerhetsavtale[1] med Helse Nord IKT eller ansvarlig helseforetak før tilgang gis. Se AV0629mal databehandleravtale.
b) Dersom det er sannsynlig at leverandør kan få tilgang til helse- og personopplysninger skal det inngås en databehandleravtale (for eksempel ved feilsøking i en applikasjon/system som inneholder personopplysninger).
c) Helse Nords mal for databehandleravtale skal benyttes. Dersom leverandørens avtalemal skal brukes må det gjøres en særskilt vurdering og godkjenning av dataansvarlig.
d) For oppdrag der leverandør ikke får tilgang til helse- og personopplysninger, men til IKT-infrastrukturen skal det inngås en sikkerhetsavtale.
e) Leverandørtilganger skal være dokumenterte og Helse Nord IKTs kontrakts- og bestillingsskjema for leverandørkonto skal være utfylt.
f) Leverandørenes konsulenter skal signere Helse Nord IKTs eller helseforetakets taushetserklæring før tilgang gis. Unntak fra denne retningslinjen kan gjøres dersom det inngås en avtale der leverandøren forplikter seg til å håndtere taushetserklæringer, opplæring og tilgangsstyring i tråd med sikkerhetsområde «10 Tilgangsstyring».

4.1.3 Avtaler med leverandører skal følges opp

Kravet definerer ansvaret til den som inngår avtaler med leverandører. De faktiske oppgavene som følger av ansvaret kan delegeres til andre (f.eks. driftsleverandør) gjennom egne avtaler.

[1] En sikkerhetsavtale skal minimum inneholde krav om implementering av prosesser for tilgangsstyring, overvåking, hendelseshåndtering, rapportering og revisjoner, og regler for akseptabel bruk, krav til opplæring av

a) Den som er avtalepart med leverandør er ansvarlig for at avtalens innhold blir fulgt opp, og at tjenesteleveranser fra leverandører overvåkes og vurderes mot avtale.
b) Den som er avtalepart med leverandør skal vurdere leverandører for revisjon og skal følge opp avvik.
c) Sikkerhetshendelser, leveranseproblemer, feil, mangler og forstyrrelser skal meldes til den som er avtalepart eller den vedkommende bemyndiger i avtalen.
d) Den som er avtalepart med leverandør skal gjennomføre eller oppdatere risikovurderinger ved endringer i avtaler eller i tjenestene som leverandøren tilbyr.

4.1.4 Leverandører skal benytte Helse Nords fjernaksessløsninger for tilgang til IKT-infrastrukturen

a) Leverandørtilganger skal bare gis gjennom sikrede kanaler gjennom Helse Nord IKTs fjernaksessløsning med multi-faktor autentisering.
b) Bestilling og forvaltning av leverandørtilganger skal følge Helse Nord IKTs rutine for leverandørkonto (fjernaksess).
c) Kun autoriserte bestillere hos helseforetakene kan bestille leverandørtilganger.
d) Leverandørtilganger skal lukkes så tidlig som mulig etter bruk.
e) All bruk av fjernaksessløsninger skal logges.
f) Helse Nord IKT skal ha oversikt over leverandører som har tilgang gjennom deres fjernaksessløsning.
g) Andre tilganger som ikke kan løses gjennom punkt a) (f.eks. direktetilgang mellom leverandør og medisinskteknisk utstyr) må risikovurderes og godkjennes av berørte helseforetak og Helse Nord IKT. Dataansvarlige som har behov for en slik løsning er ansvarlig for at risikovurdering gjennomføres og for å ha oversikt over alle slike løsninger.

4.1.5 Leverandører som skal ha administratortilganger skal følge alle bestemmelser i sikkerhetsområde «24 Administratortilganger»

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO 27002-referanse: A.15 Supplier Relationships

Nasjonal sikkerhetsmyndighet (NSM) grunnprinsipper kap. 2.1
https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren
https://ehelse.no/Documents/Normen/Publisering/Normen%205.3.pdf

Informasjonssikkerhet ved bruk av private leverandører i helse- og omsorgstjenesten
https://ehelse.no/Documents/E-helsekunnskap/Informasjonssikkerhet%20ved%20bruk%20av%20private%20leverandører%20i%20helse%20og%20omsorgstjenesten.pdf

Dokumentansvarlig: Jan Harald Solberg
Godkjent av: Frank Daniel Fredriksen
Gyldig for: Helse Nord
Dokumentnummer: RL6919
Versjon: 1

1. Kontroll på utstyr og verdier i Helse Nords nettverk

Dokumentsamlingen «Kontroll på utstyr og verdier i Helse Nords nettverk» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Kontroll på utstyr og verdier i Helse Nords nettverk», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Kontroll på utstyr og verdier i Helse Nords nettverk» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene i dette styringsdokumentet gjelder registrering og forvaltning av enheter, programvare og informasjonsverdier som er eller skal bli tilkoblet Helse Nords infrastruktur.

3. Formål

Helse Nord skal identifisere og holde en oppdatert oversikt over enheter, programvare og informasjonsverdier som er tilkoblet Helse Nords infrastruktur.

Kravene skal sikre at:

- virksomhetens verdier er identifisert
- ansvar for tilstrekkelig beskyttelse av disse er definert

- enheter, programvare og informasjon har et beskyttelsesnivå i samsvar med deres betydning for virksomheten og skadepotensialet

Kravene skal også forhindre uautorisert utlevering, modifisering, fjerning eller ødeleggelse av informasjon lagret på medier.

4. Krav til kontroll på utstyr, programvare og informasjon

4.1 Registrering

4.1.1 Alt utstyr og all programvare skal være registrert gjennom hele sin livssyklus

a) Helse Nord skal ha et felles verktøy for registrering av utstyr og programvare som kobles til IKT-infrastrukturen. Registeret skal forvaltes av Helse Nord IKT.
b) Umiddelbart etter anskaffelses- eller opprettelsestidspunktet skal utstyret eller programvaren registreres for å holde oversikt over verdier.
c) Registreringen skal minimum inneholde:
    1. Dato for anskaffelse eller opprettelse
    2. Estimert levetid
    3. [Investeringskostnad/pris]
    4. Status (anskaffet, innfasing/test, i produksjon, utfaset)
    5. Type [klassifisering må utvikles eller hentes fra dagens CMDB, bør inneholde nettverk, server, programvare, klient, informasjonsmengde/element etc.]
    6. Funksjon (hva verdien benyttes til)
    7. Kritikalitet (iht konsekvensmatrise brukt ved risikovurderinger)
    8. Eier (funksjon eller virksomhet som har anskaffet enheten)
    9. Kontaktinformasjon (person eller rolle som skal ha varsling)
    10. Klassifisering i henhold til informasjonsklassifisering
    11. Om enheten eller programvaren inngår i en behandling av personopplysninger (ja/nei)
        i. Om enheten eller programvaren oppbevarer/lagrer identifiserbare helseopplysninger (Ja/Nei)
    12. Fysisk sted/lokasjon (hvis relevant) med adresse, etasje, rom nr. evt. GPS-koordinater
d) Systemeieren i helseforetaket skal sikre at verdier blir registrert, klassifisert, beskyttet og avhendet der dette er relevant.
e) Systemeieren i helseforetaket skal sikre at oppføringen til verdier blir oppdatert ved endringer i verdiens egenskaper listet under b).
f) Systemeieren i helseforetaket skal sikre at verdier blir deaktivert i det felles verktøyet for registrering nevnt i punkt a) ved avhending/utfasing.

4.2 Informasjonsklassifisering

4.2.1 Informasjonsverdier i Helse Nords infrastruktur skal klassifiseres [pt kun iht. konfidensialitet]

a) Informasjonsverdier skal klassifiseres i henhold til RL5860 «Regional retningslinje for sikring av informasjon».
b) For informasjonsverdier høyere enn klasse 2 skal det etableres tilstrekkelige løsninger for tilgangsstyring.

4.3 Lagringsmedia

4.3.1 Lagringsmedia som inneholder helse- og personopplysninger skal merkes

a) For lagringsmedium som inneholder helse- og personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking.
b) Merking skal gjøres på en hensiktsmessig måte. Enkeltmedia merkes dersom de oppbevares eller benyttes alene, større lagringsmedia (eks lagringskabinett) kan merkes som helhet.
c) For lagringsmedium som inneholder informasjon i klasse 5 (GRADERT) gjelder sikkerhetslovens bestemmelser. https://lovdata.no/dokument/NL/lov/1998-03-20-10?q=sikkerhetsloven
d) Prosedyre PR30596 «Håndtering av pasientopplysninger på medisinsk teknisk utstyr» gjelder der det er relevant.

4.3.2 Lagringsmedia som inneholder helse- og personopplysninger skal forvaltes i tråd med RL5860 «Regional retningslinje for sikring av informasjon» både under bruk, rekonstruksjon, transport og ved avhending

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO 27002-referanse: A.8: Asset management

Nasjonal sikkerhetsmyndighet (NSM) grunnprinsipper kap 1,1 og 1.2
https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgssektoren kap. 3.2
www.normen.no/

1. Kryptografi

Dokumentsamlingen «Kryptografi» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Kryptografi», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Kryptografi» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene omfatter ikke opplysninger gradert i henhold til Sikkerhetsloven

3. Formål

Formålet med kravene i dette dokumentet er å gi et grunnlag for å sikre ivaretakelse av sikkerhetsmål og sikkerhetsstrategi. Kryptografi/kryptering er et verktøy for å sikre at informasjon ivaretas på en tilstrekkelig sikker måte. Kravene skal også bidra til at man er i stand til å begrense omfanget og konsekvensene av en eventuell sikkerhetshendelse.

Disse kravene skal sørge for at bruk av kryptografiske teknikker gjøres på en god og effektiv måte, for å beskytte konfidensialitet, ekthet og integritet til informasjon og informasjonssystemer.

4. Krav til kryptografi

Nasjonal sikkerhetsmyndighet er i Sikkerhetsloven gitt det nasjonale ansvaret for kryptosikkerhetstjenesten og sentral forvaltning av kryptomateriell.

4.1 Generelt

4.1.1 Personopplysninger skal ved overføring krypteres i henhold til gjeldende lov- og regelverkskrav

4.1.2 Helse Nord skal ha kryptografiske løsninger basert på standarder og tilpasset behov

a) I den grad Nasjonal sikkerhetsmyndighet https://www.nsm.stat.no/ har gjort vurderinger eller laget retningslinjer på området skal disse følges.
b) All bruk av kryptografi skal være basert på internasjonale åpne og veldefinerte standarder.
c) Internasjonalt anerkjente implementasjoner av kryptofunksjonalitet skal benyttes så langt det er mulig.
d) Det skal velges krypteringsmotorer (ciphere) som er uten kjente svakheter og egnet for formålet for informasjonen de skal beskytte.

4.2 Nøkler og nøkkelhåndtering

4.2.1 Det skal finnes detaljerte retningslinjer med tekniske og prosessuelle krav for nøkkelhåndtering

a) De detaljerte retningslinjene skal være utviklet og forvaltes av Helse Nord IKT.
b) Retningslinjene skal dekke krav til oppretting, oppbevaring og utveksling av nøkler.
c) Retningslinjene skal beskrive ansvar i de ulike delene av prosessene.

4.3 Sertifikathåndtering

4.3.1 Det skal finnes detaljerte retningslinjer med tekniske og prosessuelle krav for søknad, utstedelse og utfasing eller tilbakekalling av sertifikater

a) For hver sertifikattype skal det defineres rutiner som minimum skal beskrive utfasing, tilbakekalling og fornyelse.
b) Det skal eksistere retningslinjer for hver sertifikattype som minimum skal beskrive krav som må være oppfylt før utstedelse, tekniske krav til krypteringsmotor (ciphere), sertifikatprofil og sertifikatpolicy.
c) Retningslinjene skal beskrive ansvar i de ulike delene av prosessene.
d) Retningslinjene skal være utviklet av og skal forvaltes av Helse Nord IKT.

4.4 Kryptering av kommunikasjonsdata

4.4.1 Det skal finnes detaljerte retningslinjer med tekniske og prosessuelle krav for kryptering av kommunikasjonsdata

a) De detaljerte retningslinjene skal være utviklet og forvaltes av Helse Nord IKT.
b) Retningslinjene skal dekke krav til meldingskryptering, linjekryptering og nøkkelbytte.
c) Retningslinjene skal beskrive ansvar i de ulike delene av prosessene.

4.5 Kryptering av data ved lagring

4.5.1 Beskyttelsesbehov skal vurderes

a) For hver anvendelse skal det vurderes og dokumenteres hvor store datamengder som skal krypteres med samme nøkkel for å oppnå riktig risikoprofil. Systemeier er ansvarlig for at vurderingen blir gjennomført.
b) For nøkler som benyttes i forbindelse med kryptering ved lagring skal det finnes sentral nøkkelbackup forvaltet av Helse Nord IKT.
c) Backup av krypterte volumer, databaser mv. skal være kryptert.

4.6 Kryptografisk/digital signering

4.6.1 Behov for signering skal vurderes

a) For hver anvendelse skal det vurderes og dokumenteres hvilke lovkrav som gjelder for digital signatur. Vurderingen skal som minimum omfatte nødvendig sikkerhetsnivå og ikke-benektbarhet.
b) For hver anvendelse må det vurderes hvor lenge signaturen må kunne verifiseres.

4.7 Lagring av passord i systemer

4.7.1 I systemer skal lagring av passord skje ved hjelp av en kryptografisk enveisfunksjon som gjør det svært vanskelig å gjette klartekstpassord basert på den krypterte utgaven

a) De detaljerte retningslinjene skal være utviklet og forvaltes av Helse Nord IKT.

4.8 Sikkerhetsgradert informasjon etter Sikkerhetsloven

4.8.1 For informasjon gradert etter Sikkerhetsloven gjelder egne regler fra Nasjonal sikkerhetsmyndighet for bruk av kryptering

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO27001: A.10: Cryptography

Nasjonal sikkerhetsmyndighet grunnprinsipper kap 2.4.6, 2.6.7, 2.8, 3.6.7 og 3.6.8 Sett inn lenke: https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/.

Dokumentansvarlig: Jan Harald Solberg
Godkjent av: Frank Daniel Fredriksen
Gyldig for: Helse Nord
Dokumentnummer: RL6921
Versjon: 1

1. Sikring av kommunikasjonsrom

Dokumentsamlingen «Sikring av kommunikasjonsrom» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Sikring av kommunikasjonsrom», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Sikring av kommunikasjonsrom» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Helse Nord IKT (HN IKT) har IKT-utstyr på alle helseforetakene i Helse Nord. Dette utstyret står på forskjellige typer kommunikasjonsrom:

- Noen av disse er sentralt plassert og det er kun ett eller to av disse på hvert sykehus. Disse kalles enten SHKR (sentralt hovedkommunikasjonsrom) eller HKR (hovedkommunikasjonsrom). Heretter vil overnevnte rom omtales som "Hoved-kommunikasjonsrom".
- Hoved-kommunikasjonsrom (HKR) kalles i dagligtale for "datarom" eller "lokalt datarom".
- Andre kommunikasjonsrom (KR) er spredt rundt om i bygget og kan være alt fra et skap i en korridor til et mindre rom. Det kan være mange slike rom/skap i en bygning. Disse rommene er i dagligtale omtalt som "underfordelere" og er en del av IKT infrastruktur/forgreningsnettverket fra HKR til avdelinger og brukere i et sykehus eller annen driftsbygning i Helse Nord.

Dette dokumentet inneholder krav til infrastrukturen for alle disse rommene.

Kravene i dette dokumentet omfatter ikke de sentrale datasentrene. Kravene til disse er regulert i driftsavtale med byggeier og avtaler med relevante aktører.

3. Formål

Formålet med kravene i dette kravdokumentet er å ivareta informasjonssikkerheten og sikre stabil drift av utstyr og systemer i helseforetakene (HF-ene). HF-ene er ansvarlig for at disse kravene etterleves og ivaretas.

4. Krav for hovedkommunikasjonsrom

4.1 Hovedkommunikasjonsrom skal ha stabil og tilstrekkelig strøm

4.1.1 Alle rack skal ha redundant strøm (fra to forskjellige kilder)

a) Rack skal enten være tilknyttet to forskjellige UPS-er (avbruddsfritt strømforsyningsanlegg med batteribank),
b) Eller være tilknyttet UPS og PRI (prioritert strøm, dvs. levert fra aggregat)
c) UPS-er skal være sentralt plassert (i annet rom enn hovedkommunikasjonsrom)
    - Dette gjelder på alle nye sykehus samt der det installeres ny UPS på eksisterende sykehus

4.1.2 Antall og type strømuttak ved hvert rack skal være avklart med HN IKT

a) Strømuttak skal enten være 400V 3-faset (helst 32A) kontakt over eller underrack for å koble til PDU (Power Distribution Unit)
    - Dette gjelder hovedkommunikasjonsrom på alle nye sykehus samt der det installeres ny sentral UPS på eksisterende sykehus
b) Eller vanlige 230V 16A strømuttak fordelt på flere kurser.
c) Det totale effektforbruket må defineres i samråd med HN IKT.

4.1.3 Alle kontakter skal være plassert slik at strømkabler ikke blir i veien for daglig drift

4.1.4 Det skal være redundant reservekraftanlegg med tilstrekkelig kapasitet

a) Hvert sykehus skal ha minst to aggregater for å ha reservekraft også ved feil og service.
b) Det totale effektforbruket må defineres i samråd med HN IKT.

4.2 Hovedkommunikasjonsrom skal ha stabil og tilstrekkelig kjøling samt stabil luftfuktighet

4.2.1 Temperaturen i HKR skal ligge innenfor anbefalte verdier

a) Anbefalt temperatur er mellom 20°C og 25°C.

4.2.2 Det skal være redundant kjøleanlegganlegg

a) Det skal være minst to kjøleenheter i hvert HKR for å holde temperaturen innenfor anbefalte verdier også ved feil og service.
b) Kjøleanlegget skal fungere selv om strøm fra kraftleverandør faller ut.

4.2.3 Luftfuktigheten skal ligge innenfor anbefalte verdier

a) Anbefalt luftfuktighet er mellom 20 % og 80 % RH.

4.3 Hovedkommunikasjonsrom skal ha redundans på fiber inn

4.3.1 Redundante fiber inn skal gå i forskjellige traséer slik at en enkelthendelse ikke kan påvirke begge

a) Hvis sykehuset har to hovedkommunikasjonsrom, skal det gå minst én fiberkabel til hvert av rommene.
b) Hvis det er grensesnittrom i tilknytning til hovedkommunikasjonsrom, så anses disse rommene som ett i forhold til krav og retningslinjer i dette dokumentet.

4.4 Hovedkommunikasjonsrom skal være beskyttet mot uautorisert tilgang

Se også sikkerhetsområde «08 Fysisk sikkerhet og sikring av utstyr» pkt. 4.1.3

4.4.1 Kun personer med tjenstlig behov skal kunne få adgang til hovedkommunikasjonsrom

a) Helseforetaket i samråd med utstyrseier skal avgjøre hvem som har tjenstlig behov.
b) Det skal være mulig å ta ut ei liste på alle som har eller har hatt tilgang til rommet.
c) Hvis person fra innleide firma skal inn, skal vedkommende enten autoriseres på forhånd (innebærer bl.a. gjennomgang av driftsrutiner og signering av taushetserklæring) eller følges av den som er ansvarlig for innleie av firmaet/personen, eller noen denne bemyndiger.
d) Helseforetaket skal i samråd med utstyrseier utarbeide driftsrutiner som skal signeres av alle som får tilgang til et hovedkommunikasjonsrom. Driftsrutinene skal omfatte regler for bruk av adgangskort, varslingsrutine ved tap av adgangskort, konsekvenser ved misbruk.

4.4.2 Kortleseren til hovedkommunikasjonsrom skal være overvåket

a) Det skal gå en alarm ved sabotasje.
b) Det skal gå alarm dersom dør blir stående åpen ut over et forhåndsdefinert tidsrom.
c) Det skal være mulig å hente ut logg på hvem som har åpnet døra.

4.4.3 Dør med kortleser skal være eneste adkomstvei til hovedkommunikasjonsrom

a) Det skal ikke være mulig å ta seg inn i rommet gjennom vindu eller via luftekanaler eller åpninger fra utsiden.

4.5 Hovedkommunikasjonsrom skal være tilstrekkelig brannsikret iht. myndighetskrav

4.5.1 Det skal være røykdetektorer tilknyttet byggets brannvarslingsanlegg

a) Varsling skal gå til brannvesen og teknisk personell på sykehuset.

4.5.2 Det skal være gasslokkeanlegg eller anlegg for inert luft

a) Utløsing av slokkegass skal skje automatisk, men være 2-sone avhengig.
b) Manuell utløsing av slokkegass skal også være mulig.

4.6 Alle kritiske komponenter i hovedkommunikasjonsrom skal være overvåket

4.6.1 Helseforetakene skal ha teknisk personell med døgnkontinuerlig vakt som kan ta imot og respondere på alarmer

a) Det skal være rutiner for når Helse Nord IKT skal varsles.

4.6.2 Alarm skal gå ved feil på eller avstengning av kritiske komponenter

4.6.3 Alarm skal gå ved for høy lufttemperatur, for høy eller for lav luftfuktighet eller ved vann på gulvet (ref. pkt. 4.2)

4.7 Hovedkommunikasjonsrom skal være ryddig og funksjonelt

4.7.1 Det skal være rutiner for renhold

a) Utstyrseier har ansvar for rydding av eget utstyr.
b) Helseforetaket har ansvar for renhold av selve rommet samt ansvar for å føre kontinuerlig tilsyn.

4.7.2 Det skal være tilgjengelig lagerplass for reservedeler, verktøy mm.

4.8 Krav for andre kommunikasjonsrom

4.8.1 Kommunikasjonsrom skal være beskyttet mot uautorisert tilgang

a) Kommunikasjonsrom skal til enhver tid være låst.
b) Kun personer med tjenstlig behov skal kunne få adgang til kommunikasjonsrom.
c) Utstyrseier skal avgjøre hvem som har tjenstlig behov.
d) Hvis innleide firma skal inn, skal disse følges av bestiller.

4.8.2 Kommunikasjonsrom skal ha redundant strøm

a) Strøm skal komme fra to forskjellige kilder.
b) Minst en av kildene skal være UPS.

4.8.3 Temperaturen skal ligge innenfor anbefalte verdier

a) Anbefalt temperatur er mellom 20°C og 25°C.

4.8.4 Luftfuktigheten skal ligge innenfor anbefalte verdier

a) Anbefalt luftfuktighet er mellom 20 % og 80 % RH.

4.8.5 Kommunikasjonsrom skal være ryddig og funksjonelt

a) Størrelse og utforming av rommet må være slik at drift og feilsøking ikke forsinkes unødvendig.
b) Patchekabler skal gå i dedikerte føringsveier (guider, kanaler).

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO 27002: A.11: Physical and environmental security

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten:
https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

1. Sikkerhet i IKT produksjonsmiljø

Dokumentsamlingen «Sikkerhet i IKT produksjonsmiljø» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Sikkerhet i IKT produksjonsmiljø», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Sikkerhet i IKT produksjonsmiljø» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Kravene i dette dokumentet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen.

Kravene gjelder alle helseforetak og andre virksomheter som har systemer tilkoblet infrastrukturen, samt driftsleverandører som kan være Helse Nord IKT eller andre som leverer tjeneste- og systemdrift til Helse Nord.

3. Formål

Formålet med kravene i dette dokumentet er å sikre ivaretakelse av sikkerhetsmål og sikkerhetsstrategi i produksjonsmiljøet for IKT-tjenester i Helse Nord. Etterlevelse av kravene i dette dokumentet skal hindre at uforutsette hendelser oppstår, og begrense omfanget av skadevirkninger av eventuelle hendelser i produksjonsmiljøet.

Kravene skal sikre at oppdatering eller endring av programvare eller IKT-infrastruktur styres iht. etablerte prosesser, og hindre at påvirkning av IKT-infrastruktur eller programvare er av utilsiktet eller uønsket art.

Ved unntak fra krav må det påses at det overordnede sikkerhetsnivået for det aktuelle systemet er ivaretatt, samt at sikkerheten til omkringliggende systemer ikke kompromitteres. Et slikt unntak skal dokumenteres, både med hensyn til hvorfor unntaket gjøres, men også hvilke tiltak som treffes for å ivareta overnevnte hensyn.

4. Sikkerhetskrav

4.1 Generelt

4.1.1 Alle tjenester, systemer og applikasjoner skal ha en systemeier

a) Alle systemer og applikasjoner skal ha en systemeier som er ansvarlig for at forvaltning og drift av systemet utføres i tråd med gjeldende sikkerhetskrav og retningslinjer.
b) Ivaretakelse av sikkerhetskravene utføres av personell fra eget helseforetak eller fra driftsleverandør med dedikert ansvar for tjenesten eller fagområdet. Eksempler på roller kan være fag-, tjeneste-, eller systemansvarlig. Heretter omtalt som fag-/tjenesteansvarlig.
c) Rolleavklaring og ansvarsforhold som beskrives i punkt a) og punkt b) skal dokumenteres i avtale mellom helseforetak/systemeier og driftsleverandør.

4.1.2 Alle systemer og applikasjoner skal minimum sikres i henhold til produsentens beste praksis

a) Dokumentert beste praksis for å sikre et system eller en komponent til et system skal implementeres når det er tilgjengelig.
b) Dersom produsenten ikke kan tilby en beste praksis skal det etableres en beste praksis iht anerkjente systemer for sikker forvaltning av IKT-systemer, før systemet kan tas i bruk.

4.1.3 Kritiske tjenester, komponenter og enheter skal overvåkes

a) Status som presenteres gjennom overvåkingsverktøy skal gjenspeile objektets reelle og oppdaterte driftsstatus.

4.1.4 Systemlogger skal samles og beskyttes

a) Logging skal settes til rett nivå slik at sporbarhet ivaretas.
b) Logg skal beskyttes mot uautorisert innsyn og endring.

4.1.5 All tilgang til helse- og personopplysninger skal logges

a) For systemer som behandler helse- og personopplysninger skal tilganger logges. Innholdet i loggene skal være i samsvar med krav i Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet.
b) Der logging ikke er mulig må dette dokumenteres og vurdering av risiko og eventuelle personvernkonsekvenser gjennomføres. Supplerende sikkerhetstiltak i henhold til risiko må vurderes.

4.1.6 Systemklokker må synkroniseres fra en sentral kilde

a) Helse Nords systemklokketjeneste (NTP) skal brukes til å synkronisere systemklokker.

4.2 Beskyttelse mot sårbarheter i programvare og systemer

I systemer innebærer dette at hele plattformen skal holdes oppdatert, inkludert BIOS/firmware og annen software som kan ha innvirkning på systemets sikkerhetsnivå.

4.2.1 Alle systemer skal sikkerhetsoppdateres

a) Sikkerhetsoppdateringer skal behandles så fort som mulig iht plan og senest innen tidsfrister som er oppgitt for det enkelte system.
b) Ved sikkerhetsmessig behov kan oppdateringene gjennomføres umiddelbart.
c) Det er fag-/tjenesteansvarliges oppgave å holde oversikt over aktuelle oppdateringer.
d) Sikkerhetsoppdateringer skal rulles ut automatisk. Der dette må gjøres manuelt skal det etableres rutiner som sikrer at oppdateringene hurtig kan rulles ut.
e) Produksjonssetting av endringer og oppdateringer gjennomføres iht rutiner og prosesser for endringshåndtering i Helse Nord.
f) Avgjørelse om unnlatelse av oppdatering skal gjøres etter en risikovurdering og dokumenteres.
g) Systemer som ikke oppdateres må sikres på en slik måte at sikkerheten til andre systemer ikke kompromitteres.
h) Systemer som ikke oppdateres skal ha en rutine for regelmessig omstart for å avdekke feiltilstander.

4.2.2 Det skal finnes en oversikt over hvilke systemer som har hvilke sikkerhetsoppdateringer

a) Det skal foreligge en oppdatert liste over sikkerhetsoppdateringer for hvert system.
b) Det skal foreligge en oversikt over systemer som ikke er sikkerhetsoppdatert, med redegjørelse for årsak til manglende sikkerhetsoppdatering iht. 4.2.1.

4.3 Operative prosesser

4.3.1 Alle operative prosesser skal være dokumentert. Rolle, ansvar og mandat skal gå tydelig fram av dokumentasjonen

a) Driftsleverandøren skal ha dokumentert oversikt over sine prosesser.

4.3.2 Det skal finnes nødvendig dokumentasjon for alle systemer, applikasjoner og tjenester

a) Fag-/tjenesteansvarlig skal sørge for at systemer, applikasjoner og tjenester under respektivt ansvarsområde er dokumentert.
b) Dokumentasjonen skal gjenspeile nåværende konfigurasjon av maskinvare, operativsystem, endringer og all informasjon som er nødvendig for å gjennomføre gjenoppbygging av system.
c) Dokumentasjon skal være tilgjengelig på forespørsel fra dataansvarlig og tilsynsmyndigheter.

4.3.3 Alle endringer av systemer i produksjon skal skje i henhold til gjeldende rutiner og prosesser for endringshåndtering

a) Fag-/tjenesteansvarlig har ansvar for endringer av systemer i produksjon.
b) Helse Nord IKTs endringsprosess skal involveres og brukes ved endringer som kan påvirke sikkerheten i IKT-produksjonsmiljøet i Helse Nord.

c) Endringsforslag skal forberedes og fremmes for godkjenning i etablerte rutiner/ prosesser for sikker endring i systemer.
d) Godkjente endringer skal implementeres iht plan.
e) Evaluering av konsekvenser av endringen og risiko skal vurderes helhetlig. Dette kan eksempelvis være nedetid på IKT-systemer og behov for opplæring eller håndtering av økt risiko ved at endringen ikke er gjennomført.

4.3.4 Kapasitetsstyring og planlegging må være ivaretatt

a) Ansvaret for kapasitetsstyring og planlegging ligger hos driftsleverandør.
b) Ressursbruken til det enkelte system skal overvåkes og optimaliseres.
c) Fremtidig kapasitetsbehov skal beregnes på bakgrunn av historisk kapasitetsbruk og trender.
d) Dersom det oppstår situasjoner hvor tilgjengelig kapasitet ikke strekker til, må det gjøres en prioritering iht. SLA.

4.3.5 Det skal være separate miljøer for produksjon, utvikling og test

a) Sikkerheten i produksjonsmiljøet skal ikke kunne påvirkes negativt av utviklingsmiljø eller testmiljø, inkludert QA-miljø.

4.4 Beskyttelse mot skadevare

4.4.1 Det skal være tekniske tiltak mot skadevare på plass både på servere og klienter

a) Det skal være antivirus installert på servere og klienter, og eventuelle avvik skal dokumenteres.
b) Lokal brannvegg eller tilsvarende funksjonalitet skal være aktivert og det skal etableres regler som sikrer akseptabel inngående trafikk.
c) Avvik skal dokumenteres og begrunnes.
d) Programvare og funksjoner som ikke er i bruk i produksjon skal avinstalleres eller skrus av / deaktiveres.

4.4.2 Installasjon av programvare skal være kontrollert og underlagt sentral administrasjon

a) På klienter og servere skal det opereres med en "hvitliste" som forteller hvilke programmer som tillates å kjøre på disse.
b) Installasjon skal skje fra en sikker kilde og følge en dokumentert prosess.

4.4.3 Alle systemer skal være underlagt konfigurasjonskontroll og under sentral administrasjon

a) Fag-/tjenesteansvarlig skal sikre konfigurasjonskontroll på systemer innenfor sitt ansvarsområde.

4.5 Sikkerhetskopi og gjenoppretting

4.5.1 Det skal tas sikkerhetskopier av systemer, data og konfigurasjon der det er avtalt, eller hvor tap av dette vil påvirke driften

a) Gjenopprettingsfunksjonalitet for kritiske IKT-systemer skal testes iht. etablert praksis, jf. sikkerhetsområde «23 Informasjonssikkerhet i test».

b) Det skal testes og dokumenteres hvor lang tid man vil bruke på en gjenoppretting av systemet eller tjenesten og dens enkelte komponenter.
c) Sikkerhetskopi skal behandles med samme krav til konfidensialitet, integritet og tilgjengelighet som kildesystemet.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten
https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.12: Operations security

1. Sikkerhetssoner

Dokumentsamlingen «Sikkerhetssoner» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Sikkerhetssoner», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Sikkerhetssoner» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i dette dokumentet gjelder den regionale IKT-infrastrukturen i Helse Nord, og alle enheter og programvare som er tilkoblet den.

3. Formål

Formålet med kravene i dette dokumentet er å gi et grunnlag for å sikre ivaretakelse av sikkerhetsmål og sikkerhetsstrategi. Sikkerhetssoner er et verktøy for å enkelt finne ut hvor helseopplysningene skal behandles, og sikre at de ivaretas på en tilstrekkelig sikker måte. Kravene som stilles til sikkerhetssonene skal sikre at de rettslige krav som er pålagt databehandler og dataansvarlige blir ivaretatt, samt at man kan agere både raskt og på riktig måte ved eventuelle sikkerhetshendelser. Kravene skal også gjøre at man er i stand til å begrense omfanget og konsekvensene av en eventuell sikkerhetshendelse.

4. Krav til sikkerhetssoner

Sikkerhetssoner skal sørge for enkel oversikt over hvor helseopplysningene håndteres, og sikre at de ivaretas på en tilstrekkelig sikker måte. Helse Nord IKT forvalter den tekniske implementeringen av sikkerhetssoner gjennom egne utdypende retningslinjer.

4.1 Alle enheter og brukere i en sikkerhetssone skal identifiseres

4.1.1 Enheter og brukere skal være identifisert

a) Alle personer (inkludert gjester) som gis tilgang til Helse Nords infrastruktur skal identifiseres og alle enheter skal være registrert med ansvarlig og lokasjon. Den som tilbyr tjenesten[1] til personer i sikkerhetssonen er ansvarlig for at registrering blir gjennomført.
b) Gjester kan tilbys tilgang til internett mot at de beviser hvem de er, men skal ikke ha tilgang til andre soner i IKT-infrastrukturen/.
c) Det skal være mulig å spore alle enheter som befinner seg i IKT-infrastrukturen.
d) Tilganger eller tilkoblinger som må gis i strid med punktene over skal være regulert i særskilt avtale med Helse Nord IKT.

4.2 Utstyr med ulikt sikkerhetsnivå skal skilles fra hverandre

Det skal være egne tiltak tilpasset hver sikkerhetssone. Alt utstyr skal plasseres i den sikkerhetssonen bruken eller opplysningene krever iht kritikalitet for pasientbehandling og/eller informasjonsklassifisering, jf «RL5860 Regional retningslinje for sikring av informasjon»

Dersom utstyret plasseres i en sikkerhetssone med lavere sikkerhetsnivå enn det bruken eller opplysningene som behandles på utstyret tilsier, skal det iverksettes tilpassede tiltak for dette utstyret basert på en vurdering av risiko. Det samme gjelder der informasjon skal transporteres mellom sikkerhetssoner.

4.2.1 Brukerenheter/utstyr skal skilles fra hverandre

a) Brukerenheter/utstyr med internettilgang skal isoleres fra andre brukerenheter/utstyr.
b) Brukerenheter/utstyr som ikke kan sikkerhetsoppdateres eller har kritiske sårbarheter skal plasseres i en høysikkerhetssone som eliminerer trusler fra egen sikkerhetssone, andre sikkerhetssoner og internett.

4.2.2 Utstyr i ett helseforetak skal kunne skilles fra andre helseforetak

Hvert helseforetak har ansvar for tilstrekkelig sikring av egne data, og har kontroll over lokale deler av infrastrukturen i Helse Nord.

a) Enheter/utstyr i hvert helseforetak skal kunne skjermes eller isoleres fra de andre helseforetakene.

4.2.3 Byggteknisk utstyr skal skilles fra annet utstyr

Byggteknisk utstyr (FDV/HVAC/SD/tilsvarende) er ofte spesialtilpasset og administrert/vedlikeholdt iht. helseforetakenes lokale vedlikeholdsrutiner. Utstyr av denne typen som er tilkoblet IKT-infrastrukturen må derfor skilles fra annet utstyr.

[1] I praksis vil dette si den som har besluttet at tjenesten skal være tilgjengelig. For gjestenett vil dette for eksempel normalt være et sykehus eller helseforetak.

a) Byggteknisk utstyr skal isoleres fra andre typer enheter/annet utstyr.
b) Byggteknisk utstyr som ikke kan sikkerhetsoppdateres eller har kritiske sårbarheter skal plasseres i en høysikkerhetssone som minimerer trusler fra egen sikkerhetssone, andre sikkerhetssoner og internett.

4.2.4 Medisinteknisk utstyr skal skilles fra annen type utstyr

Medisinteknisk utstyr (MTU) er ofte spesialtilpasset og administrert/vedlikeholdt iht. helseforetakenes lokale vedlikeholdsrutiner. Utstyr av denne typen som er tilkoblet IKT-infrastrukturen må derfor skilles fra annet utstyr.

a) Medisinteknisk utstyr skal isoleres fra andre typer enheter/annet utstyr.
b) Medisinteknisk utstyr som ikke kan sikkerhetsoppdateres eller har kritiske sårbarheter skal plasseres i en høysikkerhetssone som minimerer trusler fra egen sikkerhetssone, andre sikkerhetssoner og internett.

4.2.5 Enheter/utstyr som er kritisk for pasientbehandlingen skal kunne skjermes eller isoleres ut fra situasjon

Håndtering av en beredskapssituasjon skjer iht. beslutninger gjort av beredskapsorganisasjonene og de til enhver tid foreliggende beredskapsplaner.

a) Det skal være mulig å skjerme kritiske enheter/utstyr ved endring i trusselbildet.
b) Det skal være mulig å isolere kritiske enheter/utstyr ved en alvorlig hendelse (eks. virusangrep).

4.3 Utstyr og systemer som oppbevarer/lagrer informasjon med ulike informasjonsklasser skal skilles fra hverandre

Informasjonsklassene er definert i Se «RL5860 Regional retningslinje for sikring av informasjon»

4.3.1 Utstyr som oppbevarer/lagrer helseopplysninger eller som er vesentlige for pasientbehandlingen skal skilles fra annet utstyr

a) Utstyr som behandler/oppbevarer/lagrer helseopplysninger, eller som er vesentlig for pasientbehandlingen skal isoleres fra annet utstyr (se 4.2.4).
b) Utstyret defineres i klasse 4 «sensitiv» iht «RL5860 Regional retningslinje for sikring av informasjon»

4.3.2 Utstyr som oppbevarer/lagrer personopplysninger eller virksomhetskritisk styringsinformasjon skal kunne skilles fra annet utstyr

a) Administrative systemer som kan inneholde personopplysninger eller virksomhetskritisk styringsinformasjon skal kunne isoleres fra annet utstyr.
b) Utstyret og systemene defineres i klasse 3 «skjermet» iht «RL5860 Regional retningslinje for sikring av informasjon»

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.13: Communications security

Nasjonal sikkerhetsmyndighet grunnprinsipper kap. 2.2, 2.3, 2.7, og 2.10
https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/

Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgssektoren kap. 5.4.3
https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet

Dokumentansvarlig: Jan Harald Solberg
Godkjent av: Frank Daniel Fredriksen
Gyldig for: Helse Nord
Dokumentnummer: RL6924
Versjon: 1

1. Informasjonssikkerhet i IKT-anskaffelser

Dokumentsamlingen «Informasjonssikkerhet i IKT-anskaffelser» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Informasjonssikkerhet i IKT-anskaffelser», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Informasjonssikkerhet i IKT-anskaffelser» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene i styringssystemet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Sikkerhetskravene i dette dokumentet gjelder alle IKT-anskaffelser av utstyr, programvare og tjenester. Med «tjenester» menes også tjenester som kjøpes av eksterne leverandører men som nås helt eller delvis gjennom den regionale IKT-infrastrukturen.

Kravene omhandler også håndtering av informasjon i gjennomføring av anskaffelser, og går mer i dybden på områdene anskaffelser av utstyr/programvare, anskaffelser av tjenester og outsourcing av utvikling, samt sikkerhetsmessige krav til testing før produksjonssetting.

3. Formål

Kravene skal sikre at anskaffelser og innføring av systemer som skal koples til Helse Nord sin infrastruktur ivaretar Helse Nord sine sikkerhetsmessige behov. Kravene skal sikre at utstyr,

programvare og tjenester som anskaffes i Helse Nord ikke reduserer eksisterende nivå på informasjonssikkerheten. Dette understøtter også regionens behov for å ivareta tilstrekkelig personvern, som i mange tilfeller vil være helt avhengig av tiltak på informasjonssikkerhetssiden.

4. Krav til IKT-anskaffelser

Selve anskaffelsesprosessen må i seg selv gjennomføres på en tilstrekkelig sikker måte, både for å ivareta sikkerheten for Helse Nords informasjon og infrastruktur, og for å sørge for en korrekt gjennomføring av anskaffelsen.

4.1 Generelt

4.1.1 For anskaffelser som kan påvirke informasjonssikkerheten i Helse Nord skal det gjennomføres en risikovurdering. Basert på denne skal det utarbeides relevante sikkerhetskrav

a) Den som initierer og er ansvarlig for anskaffelsen i helseforetaket skal vurdere om det må gjennomføres risikovurdering og personvernkonsekvensvurdering, og er i tilfelle ansvarlig for at dette blir gjennomført.
b) Beslutning om det skal gjennomføres risiko- og eventuelt en personvernkonsekvensvurdering skal tas på bakgrunn av kravene i sikkerhetsområde «03 Risikovurdering og risikostyring» og sikkerhetsområde «13 Overføring av personopplysninger til utlandet».
c) Vurderingene skal være dokumentert.
d) Den som initierer og er ansvarlig for anskaffelsen i helseforetaket skal sørge for at det utarbeides dekkende sikkerhetskrav, jf punkt 4.2.1 **Feil! Fant ikke referansekilden.**.

4.1.2 Informasjon relatert til anskaffelsen skal behandles etter hvor sensitiv den er

a) Ansvarlig for anskaffelsen i helseforetaket skal sørge for at informasjonen vurderes opp mot informasjonsklassene definert i RL5860 «Regional retningslinje for sikring av informasjon» og håndteres i tråd med denne.
b) Utveksling av informasjon med leverandører, eller andre eksterne parter skal skje gjennom tilstrekkelig sikre kanaler.
c) Den som gjennomfører anskaffelsen skal sørge for at tilgang til sensitiv informasjon om anskaffelsen kun gis til de som har tjenstlig behov.

4.2 Utstyr og programvare

Kravene her gjelder utstyr og programvare som installeres og kjører under kontroll og administrasjon av helseforetak i regionen. All programvare og alt utstyr som anskaffes og koples til Helse Nords infrastruktur kan påvirke sikkerheten i denne og eksisterende systemer.

4.2.1 I alle anskaffelser skal det gjøres en vurdering av hvilke sikkerhetskrav som skal tas med for den konkrete anskaffelsen

a) Dokumentet «Kundens tekniske plattform» inneholder informasjon til leverandører om Helse Nord IKTs infrastruktur. Innholdet i dette dokumentet skal anses som krav til programvare og utstyr som anskaffes, dvs. at det som anskaffes i utgangspunktet skal kunne kjøres på eksisterende plattform. Gjeldende versjon av dokumentet fås ved henvendelse til helseforetakets kundekontakt i Helse Nord IKT.
b) Det skal utarbeides en sjekkliste med detaljerte sikkerhetskrav til anskaffelsene av programvare og utstyr i samarbeid med Helse Nord IKT.
c) Sikkerhetsområdet «17 Kryptografi» angir krav til sikring ved bruk av kryptografiske teknikker. Disse skal følges for produkter der slike teknikker anvendes.
d) Utstyr/programvare som anskaffes må kunne forvaltes i henhold til sikkerhetsområde «16 Kontroll på utstyr og verdier i Helse Nords nettverk».

4.3 Tjenester levert over offentlige/åpne nettverk

Offentlige/åpne nettverk er nettverk Helse Nord ikke administrerer selv. I de fleste tilfeller vil dette være Internett, men det kan også dreie seg om andre kommunikasjonsnett. Selv om eksterne tjenester i liten grad er direkte koplet til Helse Nords infrastruktur, skal de likevel forvalte informasjon tilhørende Helse Nord. Konfidensialiteten, integriteten og tilgjengeligheten til denne informasjonen må sikres.

4.3.1 Alle tjenester som leveres over offentlige nettverk (f.eks. Internett, Norsk Helsenett mv.) skal sikres

a) Ekstern leverandør skal ha gjennomført og dokumentert en risikovurdering av tjenesten, som omfatter hensyn til kundens informasjonssikkerhetsbehov. Dokumentasjonen skal gjøres tilgjengelig for Helse Nord.
b) Kommunikasjon mellom infrastruktur i Helse Nord og eksterne skal sikres slik at konfidensialitet, integritet og tilgjengelighet ivaretas.
c) Kommunikasjon skal foregå over veldefinerte og dokumenterte grensesnitt basert på standardprotokoller som definert i 4.2.1 a) og c).
d) Helse Nord IKT forvalter en sjekkliste som gir detaljerte krav til tjenesteleveranser. Den som er ansvarlig for gjennomføring av anskaffelsen skal sørge for at det gjøres en dokumentert vurdering av hvilke krav i sjekklista det eventuelt kan avvikes fra. Sjekklisten fås ved henvendelse til Helse Nord IKTs kundeavdeling.
e) Sikkerhetsområdet «17 Kryptografi» angir krav til sikring ved bruk av kryptografiske teknikker, disse skal følges for tjenesteleveranser der slike teknikker anvendes.

4.4 Eksternt utviklingsmiljø

Disse kravene gjelder der eksterne leverandører utvikler programvare på vegne av Helse Nord, ikke for kjøp av standard programvare (hyllevare). Kravene kommer i tillegg til de som er angitt i sikkerhetsområdet «22 Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare» og sikkerhetsområdet «13 Overføring av opplysninger til utlandet». Den som er ansvarlig for anskaffelsen må dokumentere vurderingene som ligger til grunn for eventuelle avvik fra noen av disse kravene.

4.4.1 Ved bruk av eksternt utviklingsmiljø skal informasjonssikkerheten ivaretas av leverandør

a) Leverandør skal ha gjennomført og dokumentert risikovurdering av utviklingsmiljøet med hensyn til sikkerhet for kundens informasjon og sikkerhet i programvaren som utvikles. Dokumentasjonen skal gjøres tilgjengelig for Helse Nord på forespørsel.
b) Eierskap til kildekoden, og eventuelle lisenser, skal være avklart og avtalt.
c) Helse Nords rett til å revidere leverandøren og utviklingsmiljøet skal være avtalt.

4.5 Akseptansetesting

Krav i forbindelse med test er i hovedsak angitt i sikkerhetsområdet «23 Informasjonssikkerhet i test». Akseptansetest er tett knyttet opp mot det formelle løpet i en anskaffelsesprosess, og er derfor inkludert her.

4.5.1 Sikkerhet skal ivaretas som en integrert del av akseptansetesting av systemer og applikasjoner

a) Den som er ansvarlig for anskaffelsen i virksomheten skal sette krav til akseptansetester.
b) Leverandøren skal gi anbefaling til relevante sikkerhetskrav som bør med i testplan for akseptansetest.
c) Som del av akseptansetesten skal leverandør legge fram dokumentasjon på gjennomførte interne sikkerhetsrelaterte tester og resultatet av disse.
d) Nye eller alternative tiltak som iverksettes under akseptansetesting skal risikovurderes av den som er ansvarlig for anskaffelsen.

5. Feilkilder

Ingen identifiserte

6. Eksterne referanser

ISO Internasjonal standard for informasjonssikkerhet 27001/27002 A.14: System acquisition, development and maintenance

Nasjonal sikkerhetsmyndighet – Grunnprinsipper for IKT-sikkerhet kap 2.1

1. Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare

Dokumentsamlingen «Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Informasjonssikkerhet og personvern ved utvikling og forvaltning av programvare» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Kravene i styringssystemet omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for all utvikling og forvaltning av programvare i og for Helse Nord.

3. Formål

For å ivareta nødvendig sikkerhet og oppfylle kravene i gjeldende regelverk for informasjonssikkerhet og personvern, skal personvern og sikkerhet være en integrert del av utvikling og vedlikehold av

programvare og integrasjoner som benyttes i Helse Nord. Kravene skal sikre at informasjonssikkerhet er utformet og iverksatt i hele utviklingsprosessen og ved endringer, jf. sikkerhetsområdet 14 Innebygd personvern.

4. Sikkerhetskrav

4.1 Personvern og informasjonssikkerhet ved programvareutvikling

4.1.1 All programvareutvikling skal ivareta prinsippet om innebygd personvern og informasjonssikkerhet

a) Alle som utvikler programvare skal ha opplæring i prinsippene om innebygd personvern og informasjonssikkerhet. Nærmeste leder er ansvarlig for å at dette ivaretas.
b) Alle helseforetak i Helse Nord som gjør programvareutvikling skal ha spesifiserte retningslinjer for hvordan krav til personvern og informasjonssikkerhet skal ivaretas.
c) For å ivareta prinsippene om innebygd personvern og sikkerhet i programvareutvikling skal Datatilsynets veileder for innebygd personvern følges.

4.1.2 Krav til personvern og informasjonssikkerhet skal ivaretas i design og arkitektur

a) Krav til personvern og informasjonssikkerhet skal identifiseres og fastsettes i designfasen.
b) Spesifikasjonen av løsningen/systemet skal ivareta nødvendige krav til innebygd personvern og informasjonssikkerhet.
c) Den som bestiller utviklingsoppdraget skal bekrefte at fastsatte krav til personvern og informasjonssikkerhet er implementert.

4.1.3 Programvareutvikling skal gjøres i tråd med anerkjente prinsipper for sikker kodeutvikling

Anerkjente prinsipper for sikker kodeutvikling finnes bl.a. i Microsoft Security Development Lifecycle (SDL) og OWASP Flagship projects

a) Alle helseforetak i Helse Nord som gjør systemutvikling skal ha retningslinjer for sikker kodeutvikling og metodikk.
b) Før bruk av kildekode og biblioteker fra tredjepart skal lisensiering og eventuell support/oppdatering av disse avklares.
c) Alle helseforetak i Helse Nord som gjør systemutvikling skal etablere og vedlikeholde en oversikt over hvilke kildekoder og biblioteker fra tredjepart som benyttes i hvilke systemer/programmer.

4.1.4 Programvare skal forvaltes gjennom hele livssyklusen

a) Systemeier skal sikre at programvare vedlikeholdes og oppdateres når det er nødvendig, herunder retting av feil eller sårbarheter.
b) Systemeier skal sikre at programvare jevnlig revideres og testes for feil eller sårbarheter.
c) Systemeier er ansvarlig for at det inngås avtale om at direkte og indirekte identifiserbare helseopplysninger slettes, overføres til nytt system eller arkiveres i tråd med gjeldende regelverk, ved utfasing av programvare.

4.2 Personvern og informasjonssikkerhet i utviklingsmiljø

4.2.1 Helse Nords krav og retningslinjer for personvern og informasjonssikkerhet som gjelder i produksjonsmiljøet Se sikkerhetsområde «19 Sikkerhet i IKT produksjonsmiljø», gjelder også for utviklingsmiljøet

a) Tiltak skal iverksettes for å hindre uautorisert tilgang til utviklingsmiljø.
b) Tiltak skal iverksettes for å hindre uautorisert endring av kode i utviklingsmiljø.
c) Det skal iverksettes tiltak mot uautorisert programvare i utviklingsmiljø.
d) Det skal iverksettes tiltak for å hindre at utviklingsmiljø påvirker informasjonssikkerheten i produksjonsmiljøet.

4.3 Informasjonssikkerhet ved test av programvare

4.3.1 Det skal foreligge krav til testing av programvare som utvikles i eller for Helse Nord

a) Kravene i sikkerhetsområdet «23 Informasjonssikkerhet i test» skal følges ved testing.

4.4 Krav til logging

4.4.1 For programvare som skal behandle helse- og personopplysninger skal det finnes funksjonalitet for logging, jf. krav i Bransjenorm for personvern og informasjonssikkerhet og i helse- og omsorgstjenesten, dersom dette ikke ivaretas av loggfunksjonalitet i andre systemer.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

1. ISO 27002: A.14: System acquisition, development and maintenance
2. Lov om behandling av personopplysninger («personopplysningsloven» https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven)
3. EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL).
4. Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
5. Datatilsynets veileder for programvareutvikling med innebygd personvern https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/

- Sjekkliste for krav https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf

6. Datatilsynets veileder om grunnleggende personvernprinsipper https://www.datatilsynet.no/regelverk-og-skjema/veiledere/grunnleggende-personvernprinsipper-etter-nytt-regelverk/?id=7770
7. Datatilsynets veileder om anonymisering av personopplysninger https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/

1. Informasjonssikkerhet i test

Dokumentsamlingen «Informasjonssikkerhet i test» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Informasjonssikkerhet i test», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Informasjonssikkerhet i test» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene som er beskrevet i dette dokumentet gjelder for all testing av IT-løsninger og IT-systemer som behandler helse- og personopplysninger og som skal kobles til IKT-infrastrukturen i Helse Nord. Se også sikkerhetsområdet «19 Sikkerhet i IKT produksjonsmiljø».

3. Formål

Kravene i dette dokumentet skal sikre at informasjonssikkerhet blir ivaretatt i Helse Nords testprosesser og alle ulike testmiljø, i tråd med til enhver tid gjeldende regelverk innen informasjonssikkerhet.

Dette gjelder både testmiljø og QA-miljø. Helse Nord IKT sitt testsenter er *ett* slikt testmiljø. Dette benevnes heretter som Helse Nord IKTs Testsenter. Kravene gjelder også for testing som foregår i andre testmiljø og i alle utviklingsmiljø i Helse Nord.

Kravene gjelder også bruken av testdata, for å ivareta personvern og informasjonssikkerhet for direkte og/eller indirekte identifiserbare helse- og personopplysninger brukt ved testing.

Kravene skal sikre akseptabel risiko og forhindre uønsket påvirkning mellom alle testmiljø, inkludert QA-miljø, og produksjonsmiljø.

Kravene knyttet til testing skal bidra til å forhindre, samt begrense omfang og konsekvenser, av eventuelle sikkerhetshendelser i produksjon.

4. Sikkerhetskrav

4.1 Informasjonssikkerhet i testmiljø

4.1.1 Helse Nords retningslinjer og prosedyrer for tilgangsstyring, sikring av konfidensialitet og integritet for produksjonsmiljø gjelder også for miljø som benyttes til testing

a) Der det er nødvendig å teste integrasjoner mot andre systemer, skal disse systemene og integrasjonene som hovedregel også etableres i testmiljøet.
b) Dersom integrasjoner ikke kan testes i testmiljø, må risiko relatert til personvern og informasjonssikkerhet vurderes og risikoreduserende tiltak foreslås/iverksettes om nødvendig. Avviket/unntaket skal godkjennes av dataansvarlig eller den som dataansvarlig utpeker. De som bestiller testingen er også ansvarlig for at risikovurdering blir gjennomført.

4.2 Informasjonssikkerhet i forbindelse med testing

4.2.1 Testing skal ikke påvirke informasjonssikkerheten i produksjonsmiljøet

a) Miljøer i Helse Nord IKTs Testsenter skal etableres på separate nettverk atskilt fra produksjon.
b) Det skal være en separat brukerkatalog for Helse Nord IKTs Testsenter.
c) Det skal ikke være mulig å utilsiktet få tilgang til helse- og personopplysninger i produksjon via et testmiljø.
d) Det skal ikke være mulig å endre helse- og personopplysninger i produksjon via et testmiljø.
e) Det skal som hovedregel utføres verifikasjon i et produksjonslikt miljø før produksjonssetting, for å sikre at nye systemer og oppgraderinger ikke påfører skade på produksjonsmiljøet, og for å sikre at nye systemer og oppgraderinger fungerer på en korrekt og sikker måte.
f) Tilgang til testmiljø skal godkjennes av de som eier testmiljøet.
g) Kun klienter som oppfyller Helse Nords sikkerhetskrav skal kunne kople seg opp mot testmiljøene.
h) Alle nye testmiljø skal som hovedregel plasseres innenfor Helse Nord IKTs Testsenter. Unntak må godkjennes av dataansvarlig, basert på risikovurdering med begrunnelse for avviket fra de som har bestilt testen.

4.2.2 Tilstrekkelig informasjonssikkerhet og personvern skal ivaretas ved testing

a) Dataansvarlig og databehandler for systemet eller tjenesten som skal testes, har ansvar for at testing gjennomføres i henhold til gjeldende krav og retningslinjer for informasjonssikkerhet.
b) Brukeroppslag på identifiserbare helse- og personopplysninger skal logges og loggene skal være tilgjengelige for dataansvarlig.
c) Dataansvarlig og databehandler har ansvar for at de som er involvert i testingen
    - sikres nødvendig opplæring i eller har kunnskap om sikkerhetstesting, innebygd personvern og sikkerhet.
    - **gjøres kjent med eller involveres i risikovurderinger som er relevante for å kunne vurdere hvilke testmiljø og testdata som skal benyttes.**
    - **gjøres kjent med at de skal vurdere hvilke sikkerhetskrav og -funksjonalitet som bør testes.**

4.2.3 Testing av sikkerhetskrav og krav til personvern skal ivaretas

a) Funksjonalitet for å ivareta konfidensialitet, integritet og sporbarhet skal testes for systemer og løsninger som behandler helse- og personopplysninger.
b) Det skal sjekkes at tiltak fra eventuelle personvernkonsekvensvurderinger er implementert og fungerer etter hensikten.

4.3 Informasjonssikkerhet ved bruk av testdata

4.3.1 Testing skal i størst mulig grad gjøres på syntetiske data / ikke-personidentifiserbare data. Formålet er å begrense bruk av personidentifiserbare data ved testing til et minimum

a) Anonymisering skal gjøres i samsvar med veileder om anonymisering av personopplysninger fra Datatilsynet https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/.
b) Direkte eller indirekte personidentifiserbare data skal kun brukes til testing der det ikke er mulig å oppnå tilstrekkelig testkvalitet ved bruk av syntetiske og/eller anonymiserte data. I slike tilfeller skal bruk av personidentifiserbare data begrenses.
c) Ved testing på personidentifiserbare data skal det gjøres en dokumentert vurdering av formålet med testingen. De som bestiller testingen skal gjøre vurdering av personvernkonsekvenser og risiko før testing gjennomføres, samt tiltak for å minimere bruk av personopplysninger. Dette skal godkjennes av dataansvarlig, basert på risikovurdering med begrunnelse fra de som har bestilt testen.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

1. ISO 27002: A.14: System acquisition, development and maintenance
2. Lov om behandling av personopplysninger («personopplysningsloven» https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven)

3. EU forordning 2016/679/EC av 27.april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL).
4. Bransjenorm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten https://ehelse.no/personvern-og-informasjonssikkerhet/norm-for-informasjonssikkerhet
5. Datatilsynets veileder for programvareutvikling med innebygd personvern https://www.datatilsynet.no/regelverk-og-skjema/veiledere/programvareutvikling-med-innebygd-personvern/
- Sjekkliste for krav https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf
6. Datatilsynets veileder om grunnleggende personvernprinsipper https://www.datatilsynet.no/regelverk-og-skjema/veiledere/grunnleggende-personvernprinsipper-etter-nytt-regelverk/?id=7770
7. Datatilsynets veileder om anonymisering av personopplysninger https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/hvordan-anonymisere-personopplysninger/

Dokumentansvarlig: Jan Harald Solberg
Godkjent av: Frank Daniel Fredriksen
Gyldig for: Helse Nord
Dokumentnummer: RL6927
Versjon: 1

1. Administratortilganger

Dokumentsamlingen «Administratortilganger» er en del av Helse Nords regionale styringssystem for informasjonssikkerhet. Oversikt over dokumentsamlingene er beskrevet i punkt 4.1.2 i dokumentet i «01 Styring av informasjonssikkerhet».

Helse Nord sitt styringssystem for informasjonssikkerhet består av ulike nivåer, som er beskrevet nærmere i «MS0318 Regionale sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet i Helse Nord».

Dette kravdokumentet, «Administratortilganger», består av sikkerhetskrav som skal følges, og sier noe om hva som skal sikres. Dokumentet viser til prosedyrer som beskriver hvordan du som medarbeider og leder skal gå frem for å etterleve disse kravene.

Retningslinjene og prosedyrene som inngår i dokumentsamlingen «Administratortilganger» henger nøye sammen, og må derfor ses på samlet.

2. Omfang

Sikkerhetskravene som er beskrevet i dette dokumentet gjelder for alle medarbeidere og ledere i Helse Nord.

Med medarbeider menes enhver som utfører oppdrag på vegne av Helse Nord, og som skal ha tilgang til Helse Nords helse- og personopplysninger, systemer og infrastruktur, eller til adgangsregulerte områder.

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

Sikkerhetskravene omfatter alt av programvare og utstyr i Helse Nords infrastruktur og alle enheter og programvare som kobles til denne infrastrukturen, samt alle fysiske lokaliteter i Helse Nord der informasjon og informasjonssystemer er i bruk.

Kravene i dette dokumentet gjelder administratortilganger (privilegerte tilganger) til IKT-infrastruktur og systemer i Helse Nord, herunder nettverk, klienter, servere, databaser mv. Kravene gjelder også applikasjoner/systemer hvor det ikke kan skilles mellom funksjonelle og driftsrelaterte administratortilganger.

3. Formål

Helse Nord skal ha kontroll på digitale tilganger i Helse Nords infrastruktur. Det skal være tilsvarende kontroll på administratortilganger for leverandører som for egne medarbeidere.

For administratortilganger skal kravene sikre at slike tilganger kun gis til personell med tjenstlig behov, og i det tidsrom og omfang som er nødvendig.

Kravene skal forhindre uautorisert tilgang til systemer og opplysninger, samt utlevering, modifisering, fjerning eller utilgjengeliggjøring av informasjon.

4. Krav til administratorer

4.1 Administratortilganger

4.1.1 Administratortilganger skal bare gis til autoriserte personer i Helse Nord eller hos leverandør

a) Systemeier skal ha retningslinje for å godkjenne personell som skal ha administratortilganger.
b) Helse Nord IKT skal godkjenne bestillinger av administratortilganger på systemer/tjenester de har driftsansvar for.
c) Fag-/tjenesteansvarlig i Helse Nord IKT og bestiller definert av systemeier i helseforetakene kan bestille administratortilganger innenfor sitt tjenesteområde og foretak.
d) Administratorkonto skal kunne knyttes til en identifiserbar fysisk person. For leverandørtilganger der dette ikke er mulig, må det reguleres i avtale med systemeier hvordan tilganger skal gis og forvaltes. Helse Nord IKT må godkjenne dette på systemer/tjenester de har driftsansvar for.
e) Det skal være separate administratorkontoer til de ulike delene av IKT-infrastrukturen og systemer.
f) Ingen ordinære brukerkontoer skal ha administratorrettigheter.
g) Bruk av administratorkontoer skal logges.

4.1.2 Administratortilganger skal kun gis iht. tjenstlig behov

a) Den som godkjenner administratortilgangen skal gjennomføre vurdering og dokumentere hva som er nødvendig av tilganger for å kunne gjennomføre arbeidet, tidsbegrensning og når det tjenstlige behovet opphører.
b) Tilganger skal kun gis etter minste privilegiers prinsipp, og begrenses i størst mulig grad til det som er strengt nødvendig for å utføre arbeidet.
c) Tilganger skal være tidsbegrenset til det som er strengt nødvendig for å utføre arbeidet, og skal stenges så snart det tjenstlige behovet opphører.

5. Feilkilder

Ingen kjente feilkilder.

6. Eksterne referanser

ISO 27002-referanse: A.6.1 Internal organization, A.9.2.3 Management of privileged access rights

Nasjonal sikkerhetsmyndighet (NSM) grunnprinsipper kap. 1.3, 2.3, 2.5, 2.6
https://nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/