HELSE NORD

STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

HELSE FINNMARK
FINNMÁRKKU DEARVVAŠVUOHTA

VI BRYR OSS · SAMMEN TAR VI ANSVAR
UNN

NORDLANDSSYKEHUSET

HELGELANDSSYKEHUSET
HELGELAANTEN SKIEMTJE-GÅETIE

SYKEHUSAPOTEK NORD
DAVVI BUOHCCEVIESSOAPOTEHKA

Versjon 2.1 august 2012

1 INNLEDNING

1.1 Bakgrunn

Styringssystemet er initiert med bakgrunn i Nasjonal IKT sin vedtatte strategiplan, "Overordnet IKT-strategi for de regionale helseforetakene (versjon 2.5 april 2005)". Tiltakets mål er å etablere et felles styringssystem for informasjonssikkerhet for de regionale helseforetakene / helseforetakene og Norsk Helsenett AS.

1.2 Formål/Hensikt

Økt samhandling på tvers av foretaksgrensene/regioner har gjort det nødvendig å ha et overordnet styringssystem for informasjonssikkerhet for de regionale helseforetakene/helseforetakene og Norsk Helsenett AS som tilrettelegger for slik samhandling. Styringssystemet skal baseres på det lovverk som styrer aktørene (Helseregisterlov, Personopplysningslov og forskrift, med flere) inklusiv Norm for informasjonssikkerhet og aktørenes behov. Informasjonssikkerhetsforumet i Helse Nord (IS-FORUM) har tilrettelagt for et felles informasjonssikkerhetssystem for virksomhetene i regionen. Et resultat av dette arbeidet medfører at virksomhetene i Helse Nord på enkelte områder vil ha felles prosedyrer (se vedlegg 3 for oversikt).

1.3 Omfang

For å utføre oppgaver innen spesialisthelsetjenesten, behandler den enkelte virksomhet person-opplysninger om medarbeidere, pasienter og andre personer som er i kontakt med virksomheten. Disse opplysningene behandles i overveiende grad elektronisk og omfatter også bruk av medisinskteknisk utstyr (MTU), og annet tilsvarende utstyr.

Dette styringssystemet gjelder for all informasjonsbehandling av personopplysninger. Styrings-systemet dekker også metoder for sikring av virksomhetenes øvrige informasjon (eksempelvis økonomiske og strategiske opplysninger).

1.4 Målgruppe

Målgruppen er alle ansatte, med spesiell fokus på lederne i virksomhetene.
Dette dokumentet fremstår som et styrende dokument og i noen grad kontrollerende.
Foretakene og lederne må beskrive/etablere gjennomførende prosedyrer tilpasset den enkelte virksomhet.

1.5 Dokumentasjon/revisjon

IS-FORUM sørger for at dette dokumentet blir revidert årlig og ligger i dokumentsamlingen Informasjonssikkerhet i Helse Nord i Docmap: DS6121. Ledere og ansatte plikter å holde seg oppdatert på relevante prosedyrer i DocMap.

2 SIKKERHETSPOLICY

Foretakene i Helse Nord skal drives på en måte som ivaretar sikkerheten til pasienter, pårørende, gjester og ansatte og som sikrer informasjonen, dokumentasjon og de materielle verdier som foretaket forvalter.

Informasjonssikkerhet omfatter fire grunnleggende aspekter som må ivaretas:

Tilgjengelighet – det du trenger når du trenger det!

Konfidensialitet – at opplysninger, verdier og materiell ikke er tilgjengelig for uvedkommende!

Kvalitet og Integritet – at informasjon er sikret mot utilsiktet endring, og verdier og materiell er intakte og til å stole på!

Ivaretakelse av disse aspektene skal bidra til å:

*a) **Sikre personer mot uønskete hendelser!***

*b) **Sikre de materielle verdiene mot uønskete hendelser!***

3 SIKKERHETSMÅL

Foretakene i Helse Nord skal behandle personopplysninger i samsvar med kravene i helseregisterloven og personopplysningsloven med tilhørende forskrifter. Ingen helse- og personopplysninger skal samles inn, bearbeides, lagres eller slettes uten at den opplysningene omhandler har gitt sitt samtykke, eller det er fastsatt i lov at det er adgang til slik behandling. Følgende sikkerhetsmål skal oppnås:

a) kun personell med autorisert tilgang kan benytte informasjonssystemene[1] (konfidensialitet)
b) alle ledere og ansatte skal kjenne til og etterleve sitt ansvar for sikkerhet – også rengjøringspersonalet.
c) at autorisert personell har korrekt tilgang til tjenester og informasjon til rett tid og riktig sted (tilgjengelighet)
d) det skal treffes tiltak som hindrer uautorisert eller utilsiktet endring av person- og helseopplysninger slik at informasjonen til enhver tid er et resultat av rettmessige registreringer og kontrollerte aktiviteter (integritet)
e) at informasjonen til enhver tid er fullstendig, oppdatert og korrekt[2] (kvalitet)
f) at den registrertes rettigheter ivaretas
g) krav og planer for sikkerhet skal integreres og samordnes i vanlig plan- og oppfølgingsarbeid i foretaket
h) sikkerhet skal være integrert i intern-kontrollsystemet i alle foretak
i) pasienter, ansatte og besøkende skal vernes mot tyveri, trusler, og andre uheldige situasjoner slik at de føler seg trygge
j) bygninger, utstyr og materiell skal vernes og beskyttes slik at de er operative og tilgjengelige, og ikke utsettes for uønskede handlinger eller er tilgjengelig for uvedkommende
k) det skal gis veiledning, støtte og opplæring til sykehus, klinikker, avdelinger og ansatte på sikkerhetsemner
l) alle som ber om det, skal få generell informasjon om det enkelte foretaks behandling av personopplysninger

[1] Tilgang til opplysninger vil også reguleres av taushetsplikten i lover.

[2] Ansvar i fm faglig innhold og forsvarlighet i dokumentasjon tilligger ikke dette styringssystemet.

3.1 Akseptabel risiko

Sikkerhetsbrudd aksepteres ikke. Foretakene i Helse Nord erkjenner like fullt at det eksisterer sannsynlighet for at sikkerhetsbrudd kan forekomme. For å angi hvilket risikonivå som kan aksepteres for uønskede hendelser, etableres akseptkriterier knyttet til risiko.

Sikkerhetstiltak skal etableres slik at:

a) tiltakene omfatter både rutiner medarbeiderne forutsettes å følge, og tiltak som ikke kan påvirkes eller omgås av medarbeiderne med uaktsomhet.
b) tiltakene ikke kan omgås av eksterne, selv om disse opptrer med forsett.
c) der er liten sannsynlighet for at sensitive personopplysninger/helseopplysninger kompromitteres.
d) øvrige personopplysninger skal minimum sikres med tiltak som gir moderat grad av sannsynlighet for kompromittering, forutsatt at dette ikke øker sannsynligheten for kompromittering av sensitive personopplysninger.
e) det går flere måneder mellom hendelser med moderat konsekvens for helsehjelpen [3], forholdet til pasienten[4], foretaket/-personellet [5] og for øvrige medarbeidere[6].
f) hendelser med alvorlig konsekvens er enda vanskeligere å forårsake og inntreffer enda sjeldnere

3.2 Organisering av informasjonssystemet

Det enkelte foretak, ved direktør/administrerende direktør, har et selvstendig og det overordnede ansvar for at informasjonssikkerheten blir ivaretatt i henhold til gjeldende krav i sitt foretak.
Overordnet koordinering og samhandling av informasjonssikkerhetsarbeidet i regionen ivaretas av IS-FORUM.
Helse Nord IKT v/direktør er tillagt det operative ansvar for drift av informasjonssystemet.
Foretakets Sikkerhetssjef IKT/informasjonssikkerhetsansvarlig har det overordnede operative ansvar for informasjonssikkerheten som beskrevet i egen stillingsbeskrivelse og skal konsulteres i forbindelse med alle endringer som vil kunne ha informasjonssikkerhetsmessige konsekvenser.
Foretakets Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig rapporterer til Direktør/Administrerende direktør i sikkerhetsspørsmål.

All bruk av informasjonssystemet utføres i samsvar med på forhånd fastlagte rutiner og i henhold til foretakets sikkerhetsinstruks (vedlegg 1).
Det påhviler den enkelte medarbeider å rapportere avvik eksempelvis i form av sikkerhetsbrudd, til nærmeste overordnede og til foretakets Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig.

Foretakene skal ha en oppdatert oversikt over behandlinger av helseopplysninger (Registeroversikt).
Foretakets informasjonssystem skal være konfigurert i samsvar med konfigurasjonskart. Kun utstyr og program som er eid/disponert av foretaket skal inngå i informasjonssystemet. Det

[3] Eksempelvis hendelser som kan medføre helseopplysninger med utilstrekkelig kvalitet
[4] Eksempelvis hendelser som kan medføre at personlig integritet og privatlivets fred ikke ivaretas
[5] Eksempelvis hendelser som kan medføre bøtestraff eller suspensjon av autorisasjon, lisens eller spesialistgodkjenning
[6] Eksempelvis hendelser som kan medføre betydelig – men gjenopprettelig – økonomisk tap

påhviler Helse Nord IKT å ha oversikt over gyldig programvare som brukes samt systemteknisk godkjenne slik programvare for bruk i informasjonssystemet.
Bruk av privateid utstyr i forbindelse med hjemmekontor er behandlet i eget reglement, *se prosedyre Hjemmekontor.*

3.3 Ansatte/medarbeidere og bruk av informasjonssystemet

Medarbeidere med tjenestelig adgang til informasjonssystemet skal ha tilstrekkelig kunnskap om bruk av informasjonssystemet og nødvendig kompetanse i informasjonssikkerhet. Det påhviler den enkelte klinikksjef/avdelingsleder å se til at dette oppnås.

Medarbeider gis kun tilgang til personopplysninger i den grad dette er nødvendig for å utføre pålagte oppgaver. Alle medarbeidere er informert om og har underskrevet taushetserklæring samt signert egenerklæring om bruk av informasjonssystemet.

3.4 Tjenesteytere og leverandører

Foretakets bruk av tjenesteytere og leverandører reguleres av kontrakter, hvor også bestemmelser om informasjonssikkerhet inngår.
Alle som utfører arbeid for foretaket – ansatte, midlertidig ansatte og oppdragstakere – har lovbestemt taushetsplikt.

Ved valg av tjenesteyter eller leverandør vurderes ikke bare pris, leveringsdyktighet og leveransekvalitet, men også tjenesteyteren/leverandørens mulighet for å følge opp og vedlikeholde leveransen over tid.

I den grad personell hos tjenesteyter eller leverandør, inklusiv håndverkere, får adgang til utstyr, område eller programmer hvor personopplysninger behandles og/eller til informasjon om sikring av slike opplysninger, har foretaket oversikt over hvilke personell dette gjelder. Foretaket skal sørge for at angjeldende personell er informert om den taushetsplikt som gjelder samt påse at taushetserklæring underskrives.

3.5 Konfidensialitet – tilgjengelighet – integritet - kvalitet

Følgende krav skal oppfylles for å oppnå nødvendig grad av informasjonssikkerhet:

a) For å sikre en enhetlig og effektiv administrering av brukere i Helse Nord samt sikre at de underliggende krav oppnås, skal BAS (Bruker Administrativt System) tas i bruk i hele regionen. Klinikksjef/Avdelingssjef er ansvarlig for at det utnevnes BAS-ansvarlige i egen enhet.
b) Tilgang til systemer og personopplysninger gis kun til medarbeidere etter tjenstlig behov og på individuell basis, se *prosedyre for tilgangsstyring og passordpolicy i Helse Nord.*
c) Det skal forhindres at uvedkommende får tilgang til systemer og informasjon, herunder sørge for at alle maskiner har aktivert automatisk tidsstyrt låsing ved fravær.
d) Det skal forhindres at personer bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.
e) Det skal sikres at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
f) Det skal sikres nødvendig tilgjengelighet til systemer/tjenester og informasjon til rett tid for de personer som er autorisert til dette, se bl.a. *Prosedyre for nødrutiner*.

g) Det skal etableres et entydig ansvar for å sikre at medarbeidere ikke lenger har tilgang til systemet når behovet opphører, se *prosedyre for tilgangsstyring og passordpolicy i Helse Nord.*
h) Autentiseringsmekanismer, som bruk av passord, skal utformes på en slik måte at man kan ha tilfredsstillende tillit til at kun rett person får tilgang, *se prosedyre for tilgangsstyring og passordpolicy i Helse Nord.*
i) Ekstern kommunikasjon av sensitive personopplysninger skal sikres med kryptering eller tilsvarende mekanismer.
j) Dersom man befinner seg utenfor virksomheten og skal gis tilgang til sensitive personopplysninger, skal tilkoblingen sikres med nivå 4[7] autentisering.
k) Utstyr (bærbare PC, USB minnepinner, smartphones med mer) som både brukes utenfor og innenfor virksomheten skal sikres på en slik måte at risikobildet for virksomhetens informasjonssystemer ikke forringes, herunder kryptering av bærbare PCer og USB minnepinner. Ved tilkobling utenifra til virksomhetens nettverk skal en to-faktor autentisering benyttes.
l) Det skal utarbeides rutiner for kassering, transport og service av IKT-utstyr inneholdende minne/lager, slik at ikke uvedkommende får tilgang og innsyn. I tillegg skal det innføres prosedyrer som sikrer at utstyr som stjeles ikke kan brukes innenfor virksomhetens nettverk. *Se Prosedyre for kassering, transport og service av IKT-utstyr.*
m) IKT-løsningene må ha viruskontroll og sikres mot øvrig ondsinnet kode på en slik måte at en oppnår dobbel kontroll.
n) Det skal gjennomføres adgangskontroll på områder som ikke er åpent for publikum. Alle som oppholder seg i slike områder, skal bære synlig adgangskort.
Se prosedyre fysisk sikring.
o) Sensitive personopplysninger og øvrige sikringsverdige opplysninger skrevet ut på papir eller lagret elektronisk på flyttbare media, skal sikres mot at uvedkommende og uautoriserte får utskrift/innsyn
p) Felles brukerkonti skal bare være tilknyttet spesifikke maskiner. Felles brukerkonti skal ikke ha tilgang til eksterne nett (internett m.v.) og kun unntaksvis ha tilgang til kliniske systemer. Unntakene skal dokumenteres.
Se prosedyre for tilgangsstyring og passordpolicy i Helse Nord..

3.6 Sikkerhetsnivå for sensitive personopplysninger

a) Sikkerhetsnivå for foretakets IKT-løsning etableres ved bruk av risikovurdering. Vedtatte akseptkriterier legges til grunn. Videre kreves det at sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og skal ikke være begrenset til handlinger som den enkelte forutsettes å utføre.
Se prosedyre for risikovurdering.

3.7 Forvaltning – oppfølging – forbedring

a) Det skal være mulig å spore relevante sikkerhetshendelser.
b) Det skal være etablert rutiner og løsninger for å håndtere uønskede, inkludert virksomhetskritiske, hendelser.
Se prosedyre for Avvik.
c) Det skal være etablert systematiske lærings- og forbedringsprosesser ved uønskede hendelser, slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres.

[7] Jfr. krav i Norm for informasjonssikkerhet i Helse sektoren

d) For å sikre at endringer og nyinstallasjoner ikke uønsket påvirker sikkerheten, skal det alltid gjennomføres og dokumenteres konsekvens- og risikovurdering før realisering. Avdekkede nødvendige sikkerhetstiltak skal inkluderes i gjennomføringsplan. *Se Prosedyre for risikovurdering*.
e) For å sikre at forutsatt sikkerhetsnivå virkelig er etablert og følges, skal det jevnlig foretas revisjoner. Avvik skal følges opp og lukkes iht. rasjonell fremdriftsplan. Det må sørges for at revisjonsteamet har tilstrekkelig kompetanse, og uavhengighet til revisjonsobjektet.
Se prosedyre for oppfølging av informasjonssikkerhet.
f) Ledelsen skal ved minimum årlig gjennomgang av kritiske avvik funnet ved revisjoner, risikovurderinger og tilsyn, samt rapporterte alvorlige sikkerhetshendelser, vurdere behov for tiltak og endringer i sikkerhetsmål og -strategi, samt budsjettere for utvikling og iverksetting av nye sikkerhetstiltak. Behov for endring av sikkerhetsmål og -strategi som krever endring i dette styringssystemet, må sikres gjennomført hos alle virksomheter.
Se prosedyre for ledelsens gjennomgang.
g) Det skal være etablert beredskaps- og krisehåndtering som sikrer nødvendig oppetid og tilgjengelighet av kritiske systemer.
Se prosedyre for beredskap og nødrutiner.
h) Rutiner for bruk av informasjonssystemet og annen informasjon av betydning for informasjonssikkerheten, skal dokumenteres. Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny utgave. Registrering av autorisert bruk av informasjonssystemet, samt forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten.
i) Opplæring i informasjonssikkerhet skal tilrettelegges for den enkelte ved å ta i bruk e-læring.

4 SIKKERHETSSTRATEGI

Arbeidet med informasjonssikkerhet inngår som en integrert del av de oppgaver som påhviler foretaket og dets klinikker og avdelinger. Sikkerhetsarbeid er et ledelsesansvar. Gjennom sikkerhetsstrategien ønsker ledelsen å sikre at foretaket ivaretar de pålagte krav til informasjonssikkerhet i henhold til gjeldende lover og regler. Minimum 1 gang i året skal prosedyre for ledelsens gjennomgang gjennomføres.
Klinikksjef/avdelingsleder skal påse at tilfredsstillende informasjonssikkerhet oppnås ved behandling av personopplysninger innen den enkeltes myndighetsområde.

Driftstekniske oppgaver i tilknytning til informasjonssystemet påhviler i første rekke Helse Nord IKT.
Vedlikehold og feilretting som utføres av leverandører skal være gjort i henhold til kontraktsfestede avtaler.
Sensitive personopplysninger som behandles i informasjonssystemet skal sikres tilstrekkelig i henhold til Personopplysningsloven og øvrige helselover.
Personopplysninger skal ikke distribueres i eksterne nett med mindre det er særskilt sikret og risikovurdert. Spesielt gjelder dette bruk av e-post både til internt og eksternt bruk.

Lokal administrator
Ingen ordinære brukerkontoer, dvs. brukerkontoer som benyttes til brukerens daglige arbeid, skal ha rettigheter som lokal administrator.

Verktøy i sikkerhetsarbeidet

DocMap.
Helse Nord sitt kvalitetsverktøy er DocMap. Styringssystemet sammen med felles IS-prosedyrer for Helse Nord og for det enkelte HF skal etableres som egen dokumentserie i DocMap. Felles prosedyrer og HF' spesifikke prosedyrer er listet opp i vedlegg 3 i dette dokumentet.

E-læring.
IS-FORUM har utviklet et eget e-læringskurs for informasjonssikkerhet. Alle ansatte og ledere skal ha bestått testen i dette kurset. Personer som ikke har bestått testen vil ikke få eller beholde tilgang til informasjonssystemene i Helse Nord sitt IT-systemet.

4.1 Sikre relevant hjemmelsgrunnlag ved databehandling av personopplysninger

Dersom ikke hjemmelsgrunnlaget for å behandle personopplysninger er gitt i lov eller forskrift, skal slik behandling som hovedregel være basert på samtykke, alternativt dispensasjon. Ved dispensasjon skal det vurderes om den registrerte likevel skal informeres.
Det skal føres oversikt over alle databehandlinger som omfatter personopplysninger, inkludert oversikt over hjemmelsgrunnlaget for slik behandling. Behandling av sensitive personopplysninger skal være gitt i medhold av lov (meldepliktig), i konsesjon eller tilrådd fra personvernombud der dette er oppnevnt.

4.2 Sikkerhetsorganisering og ansvar

4.2.1 SIKKERHETSLEDELSEN

Sikkerhetsorganisasjonen i det enkelte foretak forvalter og styrer organiseringen av sikkerhetsarbeidet og skal i størst mulig grad bestå av personer fra den administrative ledelsen, stab og kjernevirksomhet, samt representant fra de tillitsvalgte. Målet er å etablere en lærende organisasjon hvor sikkerhetsarbeid inngår som en naturlig og sentral del av organisasjonskulturen. Sikkerhetsarbeidet skal preges av kvalitet og tverrfaglig samarbeid.

Sikkerhetsledelsens medlemmer bør være:

- Administrerende direktør
- Stabsleder for stabene og klinikksjefer eller tilsvarende (Foretakledelsen)
- Sikkerhetssjef IKT/Informsjonssikkerhetsansvarlig
- Representant for de ansatte (tillitsvalgte)

Se oversikt Sikkerhetsledelse i det enkelte foretak (alle dokumenter kommer i ei ny felles dokument samling under DS6121).

4.2.2 FUNKSJONER SOM ER TILLAGT SÆRSKILT ANSVAR

Foretak som ikke har oppnevnt funksjonene nevnt over som bør inngå i sikkerhetsledelsen, må tildele ansvaret til personer med tilsvarende rolle.

4.2.3 ADMINISTRERENDE DIREKTØR (AD)

a) er databehandlingsansvarlig for all behandling av personopplysninger, herunder ansvarlig for å bestemme formålet med databehandlingene og ha dokumentert oversikt over disse
b) har det overordnede ansvar for informasjonssikkerheten og skal sikre at tjenester er tilgjengelig for å gjennomføre tiltak
c) har ansvar for at dette styringssystemet for informasjonssikkerhet blir implementert og vedlikeholdt
d) er ansvarlig for organiseringen av sikkerhetsarbeidet
e) har ansvar for at det fastsettes akseptabelt risikonivå som minimum tilfredsstiller kravene i dette styringssystemet
f) har ansvaret for at det finnes et definert regime for tilgang til helse- og personopplysninger.

4.2.4 SYSTEMEIER

a) har ansvar for å stille krav til tilgjengelighet, konfidensialitet, integritet og kvalitet for det system vedkommende er systemeier for, slik at det oppfyller lovbestemte og andre krav
b) definerer tilgangsroller for sitt system innenfor rammene gitt av AD og å gjøre disse kjent
c) skal sørge for at det inngås skriftlige avtaler med IKT-leverandør/databehandler med krav til tjenestenivå, forvaltning og vedlikeholdsavtale
d) er ansvarlig for formalia i forhold til konsesjon/meldeplikt
e) skal sørge for at nødvendig opplæring blir gitt
f) overvåker risiko forbundet med informasjonsbehandling og forestår risikovurdering ved behov
g) Sørge for finansiering
h) Sørge for og ev. utarbeide og vedlikeholde rutiner for ikke planlagte stans (Nødrutiner)

4.2.5 KLINIKKSJEFER/AVDELINGSSJEF/AVDELINGSLEDERE

Enhver leder er ansvarlig for informasjonssikkerhet innen egen organisasjonsenhet. Ledere skal sørge for at underlagte enheter og ansatte der det er relevant:

a) er kjent med og etterlever sitt ansvar, virksomhetens styringssystem for informasjons-sikkerhet og sikkerhetsbestemmelser som er relevante, herunder kjenner til at Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig konsulteres i henhold til krav i pkt. 3.2
b) gjennomfører tilstrekkelig sikkerhetsopplæring av eget og innleid personell (inkl. renholdspersonell), slik at disse har en forståelse av hva som er forventet av dem
c) innhenter taushetserklæringer for alle ansatte og innleid personell og påser at disse er kjent med og etterlever styrende dokumenter som regulerer brukeratferd
d) tildeler og kontrollerer personellets tilgang til informasjon etter fastsatt tilgangsregime, *se prosedyre for tilgangsstyring og passordpolicy i Helse Nord.*
e) rapporterer og formaliserer registre, prosjekter og øvrige databehandlinger inneholdende person- og helseopplysninger iht. virksomhetens rutiner
f) følger opp det daglige sikkerhetsarbeidet gjennom et etablert system for avviksbehandling, gjennomfører nødvendige kontroller og iverksetter relevante tiltak

g) er ansvarlig for at beredskapsplaner ved bortfall av informasjonssystemer finnes
h) har nødvendige rutiner som sikrer tilgang, integritet, konfidensialitet og kvalitet i behandling av personopplysningene, herunder
    - har oversikt over hvilke personopplysninger som blir behandlet i klinikken/avdelingen,
    - har oversikt over hvilke register en har i klinikken,
    - klassifisere registrene
    - sørger for, sammen med Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig, innhenting av konsesjon / melding til Datatilsynet/Regional etisk komité (REK) der det er nødvendig
    - autorisasjon og deaktivering av tilgang
i) fastsetter akseptabel risiko på de viktigste områder i klinikken/avdelingen
j) gjennomfører risikovurdering med tilhørende handlingsplan og er ansvarlig for resultater, fremdrift og rapportering av sikkerhetsarbeidet innen eget ansvarsområde
k) ivaretar avvikshåndtering i samsvar med vanlig praksis i helseforetaket
l) sikrer at forholdet til tjenesteytere og leverandører (databehandlere, konsulenter, håndverkere, renholdere, vikarbyrå) er i samsvar med kravene i personopplysningsloven.
m) sikrer at dataoverføring av materiale som inneholder sensitive personopplysninger skjer i samsvar med gjeldende retningslinjer.
n) gir og tilbakekaller autorisasjon til elektroniske hjelpemiddel og lokaler, herunder påser at Sikkerhetsinstruksens bestemmelser om opphør av ansettelsesforhold følges når en ansatt slutter.
o) sørger for at klinikkens ansatte innehar nødvendig kompetanse, herunder informasjonssikkerhetskompetanse.
p) sørger for at klinikken har de nødvendige fysiske sikkerhetstiltak, og at personalet er informert om dette og hvordan installasjonene skal brukes.
q) gir melding i henhold til etablert prosedyre når tyveri oppdages på klinikken/avdelingen enten mot pasienter, ansatte, pårørende eller fra bygning og materiell

4.2.6 PERSONALSJEFEN

a) har særskilt ansvar for å sikre at alle ansatte får relevant informasjon ved ansettelse og underskriver taushetsløfte, og for planlegging og gjennomføring av relevant opplæring for ledere og ansatte.

4.2.7 DRIFT OG EIENDOMSSJEF/TEKNISK SJEF

a) har ansvaret for den bygningsmessige infrastrukturen, herunder strøm, vann og de fysiske sikringstiltak som HFet iverksetter.
b) har det totale fagansvaret for fysisk sikring av bygninger, materiell og utstyr, samt at pasienter, ansatte og besøkende har en trygg tilværelse i foretaket.
c) har ansvaret for planlegging, koordinering, saksbehandling og gjennomføring av sentrale sikkerhetstiltak, samt årlig rapportering av status til sikkerhetsledelsen.

4.2.8 SIKKERHETSSJEF IKT/INFORMASJONSSIKKERHETSANSVARLIG

Har det utøvende ansvar for foretakets sikkerhetsarbeid bl.a. gjennom å

a) forberede ledelsens årlige gjennomgang av bruk av informasjonssystemet og følge opp iverksetting av tiltak som er besluttet etter gjennomganger

b) lage årlige revisjonsplaner og forestå gjennomføring av sikkerhetsrevisjoner i virksomheten
c) vurdere rapporterte avvik og meddele avvik til virksomhetens ledelse i samsvar med rutine for avviksbehandling
d) forestå gjennomføring av risikovurderinger
e) drive opplysningsvirksomhet i foretaket mhp informasjonssikkerhet
f) være rådgiver i sikkerhetsspørsmål
g) utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområdet
h) være ansvarlig for å påse utvikling og vedlikehold av beredskaps-/varslingsplaner (katastrofeplan), samt kontinuitetsplaner relatert til IKT
i) iverksette og delta i revisjoner, risikovurderinger og egenkontroll
j) avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå
k) stille krav til nye/endrede sikkerhetsløsninger ved IT-drift, både for etablerte og nye behov som oppstår ved at nye IKT-løsninger innføres
l) påse at avvikshåndtering, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, heri om nødvendig å gi pålegg
m) iverksette korrektive og andre sikkerhetsrelaterte tiltak
n) bistå og tilrettelegge i relevante tilsynssaker

Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig rapporterer til administrerende direktør.
Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig deltar og er sekretær i sikkerhetsledelsen.

4.2.9 PERSONVERNOMBUD (PVO)

UNN og Nordlandssykehuset har, med godkjenning fra Datatilsynet, oppnevnt eget Personvernombud. De øvrige foretakene bruker Norsk Samfunnsvitenskapelige Datatjeneste (NSD) i Bergen som sitt Personvernombud når det gjelder forskning.
PVO sikrer følgende i forbindelse med foretakets behandling av personopplysninger:

a) Motta å behandle meldinger om behandling av personopplysninger
b) Er en ressursperson for forskere, helsepersonell og andre i foretaket i forbindelse med personvernspørsmål, og skal gi råd og veiledning til behandlingsansvarlig om behandling av personopplysninger.
c) Bistår i kontakten mellom foretaket/den enkelte forsker og Datatilsynet/REK. Vedlikeholder oversikt over foretakets konsesjoner, kvalitets- og forskningsregister og meldinger om personregister.
d) Bistår og eventuelt initierer revisjon av sikkerhet og oppfyllelse av lovverket som regulerer behandling av personopplysninger.
e) Bistår den registrerte med å ivareta deres rettigheter

Personvernombudet er, med hjemmel i Personopplysningsloven forskrift § 7-12, gitt myndighet av Datatilsynet til å motta meldinger på vegne av Datatilsynet. De foretakene som ikke har eget PVO må sende melding direkte til Datatilsynet om nye behandlinger av personopplysninger (for eksempel opprettelse av nye registre eller nye måter å behandle personopplysninger på, for eksempel ved bruk av telemedisin).

4.2.10 SUPERBRUKERE

For de viktigste kliniske og administrative systemene skal det etableres superbrukere. Ansvaret for at slike blir utnevnt hviler på klinikksjefene/avdelingssjefer. Det enkelte HF er ansvarlig for at det etableres en ordning som skal sørge for at nødvendige administrative og faglige oppgaver blir ivaretatt.
Oppgavene vil variere fra system til system. Det utarbeides egne oppgavebeskrivelser for den enkelte superbruker.

Eksempel på administrative oppgaver

- oversikt over superbrukere for det enkelte system
- tilrettelegging av kursvirksomhet og oppdatering av superbrukere
- ta imot henvendelser fra klinikker på ønsker om assistanse og prioritere disse
- praktisk tilrettelegging av undervisning som superbrukerne skal gjennomføre

Eksempel på faglige oppgaver

- faglig innhold i opplæringen av superbrukere
- bestemme omfang av superbrukere
- faglig innhold i undervisningen av brukere og jevnlige møter med superbrukere for bl.a. å gjennomgå deres ansvar
- være bindeledd mellom HF'et og RHF'et ved uttesting, planlegging av nye versjoner, rapportering om feil og forbedring.

Eksempel på oppgaver for superbruker

- superbruker for alle yrkesgrupper
- kursing/opplæring
- kvalitetssikring av rutiner
- testing av nye versjoner
- prosjektdeltager
- gi innspill til forbedringer
- initiere og delta i ROS-analyser

4.2.11 BRUKER/MEDARBEIDER:

Den enkelte medarbeider er ansvarlig for å:

a) følge virksomhetens sikkerhetsbestemmelser inkludert sikkerhetsinstruks
b) ha en forståelse av hva som er forventet av dem (adferd)
c) søke informasjon ved usikkerhet eller tvil
d) forhindre eller rapportere hendelser som kan innebære avvik
e) rapportere avvik når disse oppstår til nærmeste leder eventuelt Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig

Enhver ansatt oppfordres til å bidra aktivt med synspunkter og komme med forslag til forbedringer knyttet til sikkerhet.

4.2.12 BAS-ANSVARLIG

For å administrere avdelingens egne brukere skal BAS (**B**ruker**A**dministrasjons**S**ystem) tas i bruk på alle avdelinger. Ansvaret for at BAS tas i bruk påhviler henholdsvis Klinikksjef / avd. direktør / apotekere / fagsjef RHF / avdelingsledere HN-IKT.
Hver avdeling skal ha 1-3 BAS-ansvarlige som oppnevnes av avdelingsledelsen. BAS-ansvarlige skal gjennomgå obligatorisk opplæring før bruk av BAS. BAS-ansvarlig skal ikke opprette eksterne brukere (leverandører, service m.m.)

Eksempel på oppgaver for BAS-ansvarlig

- Opprette nye brukerkonti (påloggingskonti) i Helse Nords nettverk
- Resette passord for pålogging i nettverket
- Fjerne tilganger når brukere slutter
- Endre tilgang på brukerkonto når brukere flytter mellom avdelinger/klinikker/foretak
- Oppdatere e-post distribusjonslister for egen avdeling (Outlook)
- Bestille EPJ-tilgang
- Sammen med avdelingsleder årlig å gjennomføre kontroll av brukertilganger på egen avdeling.

4.2.13 IKT-BESTILLER

Er foretakets kontakt mot Helse Nord IKT og eksterne leverandører. IKT-bestiller skal ivareta foretakets behov som kunde overfor de ulike leverandører og skal ha oversikt over foretakets IKT-utstyr. I de tilfeller hvor leverandørkontakt gjøres direkte fra avdeling skal IKT-bestiller involveres.

Eksempel på oppgaver for IKT-bestiller

- Gjennomføring av forhandling og følge opp SLA for drift og supporttjenester
- Ivareta foretakets sikkerhetsstrategi ved anskaffelse av IKT-utstyr samt implementert utstyr, herunder å forestå risikovurderinger ved behov.
- Ha tett dialog med ledere, brukere og foretakets sikkerhetsorganisasjon ved anskaffelse/drift av IKT-utstyr.

4.2.14 INFORMASJONSSIKKERHETSFORUM HELSE NORD (IS-FORUM)

IS-forumet som funksjon i Helse Nord er gjennom styringsdokumentet i 2005 et pålegg til HFene om å slutte opp omkring forumet.
Formålet med forumet er å sikre en mest mulig enhetlig tilnærming til området informasjonssikkerhet og forumet skal særlig ha fokus på en felles informasjonssikkerhetspolicy i regionen og der igjennom synergier som kan hentes ut ved samarbeid.
Forumet erstatter ikkje virksomhetens selvstandige ansvar kva angår informasjonssikkerhet, j.fr. pkt. 3.2 første avsnitt.

Oppgaver:

a) Sikre en felles overordnet regional informasjonssikkerhets policy og strategi

b) Legge til rette for gjenbruk av prosedyre rig rutinebeskrivelser HFene i mellom

c) Representere et konsulterende fora ved systemanskaffelser for Helse Nord hvor informasjonssikkerhet er av vesentlig betydning

d) Representere et fora hvor RHF og HFene kan drøfte saker av betydning for den regionale/lokale informasjonssikkerhetsarbeidet

e) Gjensidig drive informasjonsutveksling knyttet til de lover og forskrifter som fremkommer fra offentlige myndigheter

f) Foreslå fellesløsninger og sikre samhandling i saker av vesentlig betydning for fellesskapet innen informasjonssikkerhetsområdet

g) Foreslå sikkerhetspolicy, tilknytningsavtale og eventuelt andre sikkerhetstiltak i regionen

h) Foreslå samordning av HFenes strategiplaner eventuelt andre viktige planer av vesentlig betydning for fellesskapet knyttet til informasjonssikkerhet

i) Kunne bidra ved utforming av regionale innspill i forhold til nasjonale myndigheter med relevans for informasjonssikkerhet

j) Det skal hvert år utformes en statusrapport knyttet til informasjonssikkerhet som oversendes Helse Nord RHF

Forumet er sammensatt med informasjonsansvarlige i HFene, samt representant fra Nasjonal Senter for telemedisin og samhandling, Helse Nord IKT og Helse Nord RHF. Forumet ledes av en av HFenes representant som utpekes av Helse Nord RHF.

4.2.15 HELSE NORD IKT

har ansvaret for anskaffelse samt leveranse av drift-, vedlikeholds- og utviklingsarbeid innen IKT-området på oppdrag fra foretakene, herunder også infrastrukturen.

Dette inkluderer å

a) overvåke risiko forbundet med informasjonsbehandling og forestå risikovurderinger ved behov
b) utarbeide beredskapsplan for IKT-området
c) følge opp tjenesteytere, leverandører og andre databehandlere som har betydning for informasjonssikkerheten
d) håndtere meldte avvik iht gjeldende avviksprosedyre i DocMap (PR12311-Avvikshåntering)
e) å sørge for at bruk av personopplysninger begrenses til det som er avtalt
f) sørge for å utvikle og etterleve driftsdokumentasjon
g) sørge for å utvikle og etterleve dokumentasjon for konfigurasjons- og endringskontroll
h) å etablere tiltak for å hindre uautorisert bruk og adgang til informasjonssystemene
i) å etablere tiltak for å registrere sikkerhetsavvik, hindre forsøk på uautorisert bruk og tilhørende avvikshåndtering
j) å etablere tiltak for å motstå angrep fra ondsinnet programvare

Det henvises til Lov om personopplysninger med forskrift

4.3 Den registrertes rettigheter

Den registrertes rettigheter til innsyn, retting, sletting og sperring er hjemlet i pasientrettighetsloven og det enkelte HF har implementert en prosedyre for å sikre dette.
Den registrerte skal informeres om sine rettigheter til innsyn, retting og sletting av personopplysningene.
For nærmere informasjon om håndtering av person- og helseopplysninger, se prosedyren Pasientjournal, kap. 7.8 – sperring av journa/-notat.

5 GJENNOMFØRING AV RISIKOVURDERING OG BESKRIVELSE AV TILTAK

Foretakenes behandling av person- og helseopplysninger er regulert gjennom helselovene og personopplysningsloven med dens forskrifter. For å kunne få behandlingen i samsvar med lovene må det derfor gjennomføres risikovurdering i forhold til informasjonssikkerheten hva angår tilgjengelighet, konfidensialitet, integritet og kvalitet.
Det presiseres at sikkerhetstiltakene skal stå i forhold til sannsynligheten og konsekvensen av sikkerhetsbrudd (POF § 2-1)

Risikovurdering skal gjennomføres ved alle endringer som kan ha betydning for helse, miljø og sikkerhet, informasjonssikkerhet og kvalitet.

Risikovurderingen gjennomføres som en stegvis prosess og skal gjennomføres ved følgende:

a) Større endringer som kan påvirke kvalitet og sikkerhet
b) Endringer i pasientbehandlingen
c) Organisasjonsendringer inkl. bemanning
d) Ny-/og endring i oppgavefordelingen
e) Ny teknologi eller endringer av teknologi
f) Nye bygg eller endring av eksisterende bygg

Veiledning i gjennomføring av risikovurdering (ROS) for informasjonssikkerhet og personvern er nærmere beskrevet i veileder for gjennomføring av risikovurdering. Som bakgrunn for denne veiledningen har en tatt utgangspunkt i Norm for informasjonssikkerhet og veilederen fra Datatilsynet.
Denne veilederen er mer tilpasset informasjonssikkerhet enn Helse Nords: Retningslinjer for risikostyring i Helse Nord, RL1602, som er basert på samme metodikk.

Det gjennomføres en grov analyse for å avdekke om endringer i risikobildet krever en systematisk risikovurdering. Ved tvil om eller ved økt/endret risikobilde skal en systematisk risikovurdering gjennomføres.
Risikovurdering i forbindelse med informasjonssikkerhet utføres ved hjelp av et elektronisk verktøy (SBA Scenario). Se veiledning Gjennomføring ROS.

Vedlegg 1: Sikkerhetsinstruks

Sikkerhetsinstruks

1. Område for denne instruksen

Denne instruksen gjelder for bruk av foretakets IKT-system. Med "IKT-system" forstås maskiner, arbeidsstasjoner, skrivere, programmer, data, flyttbare lagringsmedia, utskrifter m.v. som benyttes av eller stilles til disposisjon av foretaket, inklusive alle former for nettverk og de systemene som man får tilgang til gjennom slike nettverk. Reglene gjelder for ansatte, studenter og andre som får tilgang til foretakenes IKT-system, heretter kalt bruker.
Brukeren plikter å holde seg informert om den til enhver tid gjeldende instruks. Instruksen skal være oppslått på egnede steder. Den finnes hos din leder og kan også fås ved henvendelse til Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig.
Alle data/registre som er fremkommet i forbindelse med foretakets virksomhet eies i henhold til lover og forskrifter av institusjonen. Programvare som er utviklet i arbeidsforholdet eller i prosjekter der foretaket deltar, er institusjonens eiendom dersom ikke annet er skriftlig avtalt.

2. Generelle krav

a) Foretakets IKT-systemer skal kun benyttes til virksomhet som har direkte tilknytning til faglig virksomhet, administrasjon, egen forskning, studier eller organisasjonsarbeid i forening ved foretaket, med unntak som nevnt i pkt. 8.
b) Ved all bruk av systemet skal brukeren identifisere seg ved å oppgi eget brukernavn og passord.
c) En bruker har plikt til å følge anvisninger om bruk av systemet og tjenester knyttet til systemet. En bruker skal sette seg inn i aktuelle bruksanvisninger og dokumentasjon, for på den måten å hindre feilbruk eller driftsforstyrrelser.
d) Når arbeidsplassen forlates, skal brukeren alltid logge seg av systemet eller låse arbeidsstasjonen. Dette bidrar til å hindre at ikke-autoriserte får innsyn i IKT-systemene.
e) Alle ansatte eller andre som skal ha tilgang til de elektroniske informasjonssystemene i foretaket må gjennomføre og bestå e-lærings kurset om informasjonssikkerhet.
f) Brukernavnet er strengt personlig. Bruk eller forsøk på bruk av andre brukeres brukernavn og/eller passord ved pålogging er ikke tillatt. Det er ikke tillatt å utgi seg for å være en annen person ved bruk av foretakets IKT-systemer.
g) Passordet skal være på 8 eller flere tegn, og skal inneholde både tall, bokstaver og tegn for å gjøre det vanskeligere å avsløre passordet for uvedkommende. Navn, brukernavn, fødselsdato eller lignende skal ikke benyttes. Husk at passordet er din nøkkel til de opplysningene som finnes på foretaket.
h) En bruker skal beskytte passord og liknende sikkerhetselementer slik at disse ikke blir kjent for andre. Dersom brukeren har mistanke om at slikt er blitt kjent, skal bruker sørge for at passord m.v. skiftes umiddelbart.
i) En bruker skal forhindre at ikke-autoriserte personer får tilgang til bruk av systemet eller tilgang til rom hvor utstyr er tilgjengelig.
j) En bruker skal rapportere forhold som kan ha betydning for systemets sikkerhet eller integritet i henhold til gjeldende rutine for melding av avvik. Alvorlige hendelser eller tilstander rapporteres i tillegg umiddelbart til Sikkerhetssjef

IKT/Informasjonssikkerhetsansvarlig/Helse Nord IKT, *se prosedyre Melding om avvik informasjonssikkerhet – PR26149.*

k) En bruker skal ikke benytte seg av muligheten til innsyn i informasjon som brukeren i utgangspunktet vet han/hun ikke har tilgang til. Dette gjelder uavhengig av om dataene er beskyttet eller ikke (snoking).
l) Modem eller lignende kommunikasjonsutstyr er ikke tillatt brukt på foretakets IKT-systemer (hjemmekontorløsninger er omfattet av eget reglement).
m) Reparasjon av utstyr skal alltid organiseres av Helse Nord IKT.
n) Det er ikke tillatt å importere programmer fra eksterne nett uten at dette er godkjent. Kun programvare som er lisensiert til foretaket og som Helse Nord IKT har godkjent, kan benyttes på foretakets IKT-system. Kopiering av foretakets programvare uten tillatelse er forbudt!
o) Datafiler skal virussjekkes før bruk i IKT-systemet. Normalt er dette en prosedyre som utføres automatisk på den enkelte maskin. Dersom en bruker har mistanke om at en slik kontroll ikke blir utført skal Sikkerhetssjef IKT/Helse Nord IKT varsles umiddelbart.
p) Private maskiner/utstyr er ikke tillatt å koble til foretakets system/nettverk (produksjon), men kan kobles til et eget nett som er tilrettelagt for dette formål. Alt utstyr som skal kobles til foretakets IKT-system skal være godkjent av Helse Nord IKT.
q) Ved opphør av ansettelsesforhold skal brukeren rydde sitt reserverte område. Skjer ikke dette vil Helse Nord IKT slette filer og deaktivere brukernavnet. For øvrig henvises det til personalrutinene vedrørende avvikling av arbeidsforhold.

3. Elektronisk post (e-mail/e-post)

a) Alle brukere ved helseforetaket har egen postkasse som skal brukes til mottak og sending av e-post. Foretaket bruker e-post som en av de viktigste informasjonskanaler over for de ansatte. Den enkelte ansatte bør daglig sjekke sin innboks.
b) E-post skal ikke brukes til å sende pasientrelaterte eller andre sensitive opplysninger uten at dette er spesielt sikret (kryptert i h t Datatilsynets krypteringskrav) og godkjent av sikkerhetsledelsen. Enkelte skannere har innebygd funksjonalitet for å sende e-post til brukeren med de skannede dokumentene. Slik funksjonalitet skal ikke benyttes for å sende pasientsensitive opplysninger til en selv eller andre.
c) E-post skal kun sendes til personer som kan ha nytte av å motta den fra deg jfr. pkt. 3a i denne instruksen.
d) Innsyn i e-post, se § 9-3 i Personopplysningsforskriften samt pkt. 6 i denne instruksen.
e) Dersom e-post skal være tilgjengelig på mobiltelefon skal dette sikres særskilt og virksomheten skal ha oversikt over brukere med mobilt tilgang.
f) Privat bruk, se pkt. 8.

4. Web (intranett/internett)

Foretaket legger inn viktig informasjon på sine interne intranett-sider. De ansatte skal gjøre seg kjent med innholdet og bør daglig sjekke disse sidene.
Brukere kan få adgang til Internet og ekstern e-post etter autorisasjon fra sin avdelingsleder og etter at Egenerklæring om bruk av informasjonssystemer er akseptert og signert.
Privat bruk se pkt. 8

5. Forhold til gjeldende lover

a) Bruker skal gjøre seg særlig kjent med de regler som gjelder for behandling av personrelaterte opplysninger. Avdelingsleder skal ha disse reglene tilgjengelig ved behov.

b) Alle som utfører arbeid for foretaket – ansatte, midlertidige ansatte og oppdragstakere – er underlagt lovbestemt taushetsplikt. Plikten gjelder både i arbeidet og privat, og den varer også etter avsluttet arbeidsforhold, jfr. Taushetserklæring
c) Etablering av elektroniske registre (for eksempel overføring av pasientinformasjon til et regneark, Access og lignende) med opplysninger om fysiske eller juridiske personer er underlagt bestemte offentlige krav og regler og skal registreres. Skal du opprette slike registre eller overføre slike data, ta kontakt med Sikkerhetssjef IKT/Informsjonssikkerhetsansvarlig.
d) All bruk av klipp- og lim-funksjoner fra pasientrelaterte systemer er forbudt.
e) Det skal ikke forekomme videreformidling av konfidensielle opplysninger til ikke-autoriserte personer.
f) Pasientrelatert informasjon lagret på foretakets IKT-systemer skal oppbevares med Datatilsynets tillatelse og i henhold til offentlige lover og regler. Dette gjelder også informasjon som ikke er oppbevart i foretakets sentrale pasientregistre, eller på sentrale servere (frittstående maskiner/register).
g) Foretaket behandler og oppbevarer konsesjonsbelagt informasjon og informasjon underlagt taushetsplikt. Foretaket skal behandle og sikre data etter de vilkår som konsesjonen setter og etter lov og forskrifter gitt av offentlige myndigheter, vår taushetsplikt og foretakets egne krav til sikkerhet. Det er derfor ikke tillatt å koble internettforbindelser opp mot foretakets nettverk uten særskilt tillatelse.

6. Utvidet adgang

Hver bruker har sitt personlige reserverte område, vanligvis P:\. Dette området har ingen andre brukere tilgang til. I spesielle tilfeller er det likevel nødvendig for Helse Nord IKT og/ eller Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig å benytte seg av sin særskilte autorisasjon til å skaffe seg tilgang til den enkelte brukers reserverte område:

a) for å administrere systemene og sikre anleggets funksjonalitet
b) for å bistå en bruker i problemløsning/opplæringssammenheng. Brukeren skal være informert om dette
c) for å avdekke og/eller oppklare brudd på sikkerheten
d) når det foreligger skjellig grunn til mistanke om at brukeren har brutt Sikkerhetsinstruksen og det kan være av stor betydning for foretakets ansvar og renommé.

Hvis tilgang søkes i henhold til a) skal brukeren som hovedregel varsles på forhånd.
Hvis tilgang søkes i henhold til c) eller d) skal dette dokumenteres og loggføres i en sikkerhetslogg.

Innsyn i personlig e-postkasse skal som utgangspunkt ikke finne sted.
I enkelte situasjoner er det likevel mulig å foreta innsyn for å hente ut virksomhetsrelatert e-post. I slike tilfeller skal prosedyren for Innsyn i e-post følges, jfr. kapittel 9 i Personopplysningsforskriften. For å redusere behovet for innsyn bør den enkelte ansatt:

- lagre personlig e-post i egen mappe
- benytte fraværsassistenten når planlagt fravær gjennomføres
- gi arbeidsgiver anledning til å benytte fraværsassistenten på vegne av ansatt ved uforutsett fravær
- sørge for at arkivverdig materiale blir registrert i arkiv-/saksbehandlingssystemet (ePhorte).

Helse Nord IKT har taushetsplikt med hensyn til opplysninger om brukeren eller brukerens virksomhet som Helse Nord IKT får på denne måte. Unntak fra dette er forhold som kan representere brudd på Sikkerhetsinstruksen. Slike forhold kan meddeles til overordnete instanser.

7. Hjemmekontor/Bærbare maskiner/Smartphone
Hjemmekontor og bærbare maskiner er omfattet av eget reglement som administreres av Helse Nord IKT.
Se Prosedyre Hjemmekontor og bærbare enheter.

8. Privat bruk
Foretakets IKT-systemer er beregnet og skal primært (jfr. pkt. 3) benyttes for jobbrelatert formål. Noe privat bruk tillates imidlertid som:

- Mindre mengder e-post, nyheter og nødvendige opplysningstjenester
- Mindre mengder private filer kan lagres i egen katalog (normalt P:\) på personlig område. Av plass og kapasitetshensyn skal ikke private bilder, video, musikk eller lignende som krever stor plass, lagres på foretakets sentrale servere.

Privat bruk må imidlertid ikke påvirke jobbrelaterte oppgaver eller være i strid med denne instruks, lover eller allmenne normer for oppførsel og sosial atferd.

Vedlegg 2: Taushets- og egenerklæring om bruk av informasjonssystemer i Helse Nord

Denne erklæringen gjelder for all bruk av informasjonssystemer, maskiner, program og data ved foretaket. Av sikkerhetshensyn blir all bruk av informasjonssystemet lagret i sporingslogger for å avdekke eller oppklare sikkerhetsbrudd. Disse loggene inneholder oversikt over den enkeltes bruk av informasjonssystemet, f.eks. hvilke pasientjournaler den enkelte har vært inne i eller hvilke steder som oppsøkes på Internett, av hvem og tidspunkt.
Hvis det avdekkes at bruken av informasjonssystemet er i strid med foretakets bestemmelser vil det kunne bli iverksatt sanksjoner og få betydning for ditt arbeidsforhold.

Internett og ekstern e-post spesielt
Følgende er eksempler på **akseptabel** bruk:
Å oppdatere seg faglig gjennom tilgjengelige nettmedia som lovdata, offentlige utredninger, bibliotek register, nyheter og andre relevante kilder som f.eks. medisinske oppslagsverk og databaser.
Noe privat bruk i henhold til Sikkerhetsinstruksen, se Sikkerhetsinstruksen pkt 8.

Følgende er eksempler på **uakseptabel** bruk:

- Å laste ned programvare og spill fra nettet uten at dette er godkjent på forhånd av Helse Nord IKT.
- Installasjon av programvare uten at dette er godkjent av Helse Nord IKT.
- Å laste ned pornografi, volds- og rasistisk prega materiale eller annet materiale som kan virke usømmelig uten at dette uttrykkelig er en nødvendighet i ens faglige arbeid og at Sikkerhetssjef IKT/Informasjonssikkerhetsansvarlig/Helse Nord IKT er orientert om dette på forhånd.
- Å utveksle personopplysninger og andre opplysninger av fortrolig karakter uten at opplysningene er spesielt sikret og at utveksling skjer i henhold til vedtatte lover og regler.
- Å koble ekstra internettforbindelse opp mot foretakets nettverk uten særskilt tillatelse.

Jeg forstår at jeg i mitt arbeid/praksis ved sykehuset vil kunne få kjennskap til forhold som det av hensyn til pasienter, deres pårørende eller andre er nødvendig å bevare taushet om. Jeg er klar over at:

- Brudd på taushetsplikten kan medføre straffeansvar og eventuelt fjernelse av tjenesten
- Taushetsplikten også gjelder etter at jeg har sluttet i tjenesten

Jeg er og innforstått med at eiendomsretten til alt IKT-utstyr ved foretaket, det være seg innhold, programvare, e-post og dokumenter som er lagret på foretakets maskiner, er å regne som foretakets eiendom med mindre annet er angitt i lov (se for øvrig Personopplysningsloven § 9 vedr tilgang til e-post). Med dette forstås at ingenting kan regnes som privat og benyttes til andre formål enn det som denne erklæringen omfatter. Forskningsdata/arbeid reguleres i tillegg av egne retningslinjer.
Når jeg bruker Internett og e-post så opptrer jeg på vegne av foretaket og må handle i tråd med dette. Passord som man bruker for å logge på foretakets systemer er et personlig passord og skal ikke utleveres til andre.

Jeg bekrefter herved at jeg har mottatt et eksemplar av foretakets styringssystem for informasjonssikkerhet inklusiv Sikkerhetsinstruksen og har gjennomgått, forstått og akseptert dette.

Dato:

Signatur:

For English version, click here

Vedlegg 3: Felles prosedyrer for HFene i Helse Nord, som ligger i dokumentsamling DS6121

Prosedyrenavn	Beskrivelse	Link til DocMap
Innsyn i e-post	Se Sikkerhetsinstruks	DS6270 Felles: PR31593
Hjemmekontor og bærbare enheter	Egen prosedyre	DS6271 Felles: RL0260
Logging av innsyn	Egen prosedyre	DS6272 Felles: PR1573 PR10021: veiledning
Tilgangsstyring og passord policy	Egen prosedyre	DS6273 Felles: PR04628
Sikkerhetsinstruks	Reglement-egen prosedyre	DS6274 Norsk: RL0259 Engelsk: RL0896
Taushets- og egenerklæring	Se Styringssystem	DS6275 Norsk: SJ1473 Engelsk: SJ2256
Veiledning gjennomføring ROS	Inkl akseptkriterier- egen prosedyre	DS6276 Felles: PR04659 (SBA) RL1602: Risikostyring
Nødrutiner journal	Egen prosedyre	DS6277 HFHF: DS2246 UNN: DS0428 APOTEKET: NLSH: DS2246 HLSH: DS2246
Ledelsens gjennomgang	Egen prosedyre	DS6278 Felles: PR6159
Registeroversikt	Egen prosedyre	DS6279 Under arbeid
Melding om avvik i informasjonssikkerhet	Egen prosedyre	DS6280 Felles: PR26149
Revisjon	Egen prosedyre	
Beredskap	Egen prosedyre	DS2681 Under arbeid
Sikkerhetsledelsen i HF	Oversikt	DS6282 HFHF: RL1910 UNN: RL0258 APOTEKET: RL3380 HNIKT: RHF: NLSH: RL0277 HLSH: RL2033
Kassering, transport og vedlikehold av IKT-utstyr med lagringsmedia	Egen prosedyre	DS6283 Felles: PR05755 PR30596 MTU

Pasientjournalen	Hoveddokument prosedyrer	DS6284 Felles: PR04663
Tjeneste ytere og leverandører Brukertilganger	Egen prosedyre	DS6285 Felles: PR6167
Fysisk sikring (HF) og Tilgangsstyring	Egen prosedyre Normen: Faktaark 17	DS6286 Felles: PR05786 Makulering: RL2801
Kryptering; fysiske media, e-post	Egen prosedyre	DS6287 Under arbeid
Veiledning for oppfølging av informasjonssikkerhet	Egen prosedyre ROS, internrevisjon, logganalyse, spørreundersøkelser m.v.	DS6288 Under arbeid
Bruk av mobiltelefon/smartphone		DS6289 Under arbeid
Bruk av lesebrett/nettbrett		DS6290 Under arbeid
Håndtering av pasientopplysninger lagret på medisinsk teknisk utstyr		DS6291/ Felles: PR30596
Korrekt utsending av epikriser og prøvesvar		DS6292 Felles: RL2693 Telefax: PR23087
Prosedyre for tyveri av medier som kan inneholde sensitive opplysninger		Under arbeid
Prosedyre for bruk av SMS overfor pasienter		DS6289 Felles: PR11703 Samtykke: SJ4323
Prosedyre for Databehandleravtale	Mal for databehandleravtale samt rutine	DS7534 Felles: AV0629

Vedlegg 4: Definisjoner

Emne	Definisjon
Autorisert tilgang	(Innen IKT) Godkjent og tildelt tilgang til et eller flere informasjonssystemer.
Behandling av helseopplysninger	Enhver formålsbestemt bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.
Databehandler	En juridisk enhet som behandler personopplysninger på vegne av den behandlingsansvarlige.
Databehandlingsansvarlig	Den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes.
Forsettelig	Hendelsen skjer ved en bevisst handling hvor en har kunnskap om at det som gjøres kan forårsake et sikkerhetsbrudd.
Helseopplysninger	Taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson.
Helseregisterloven	Lov om helseregistre og behandling av helseopplysninger, LOV 2001-05-18 nr 24.
Informasjonssystemet	Samlebetegnelse på alt PC-utstyr, systemer og nettverkskomponenter som inngår i virksomhetens elektroniske databehandling inklusiv medisinsk teknisk utstyr
Integritet	Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.
Kompromittering	Brudd på konfidensialitet, tilgjengelighet eller integritet.
Konfidensialitet	Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
Overlegg	Systematisk eller planlagt aktivitet som kan medføre et sikkerhetsbrudd.
Personopplysninger	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
Personopplysningsforskriften	Forskrift til personopplysningsloven, 15. desember 2000 nr. 1265.
Personopplysningsloven	Lov om behandling av personopplysninger, 14. april 2000 nr. 31.
Sensitive personopplysninger	Opplysninger om: • rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning. • at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling. • helseforhold. • seksuelle forhold. • medlemsskap i fagforeninger.
Sikkerhetshendelse	En hendelse som får konsekvenser for informasjonssikkerheten i virksomheten.
Tilgjengelighet	Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.
Uaktsomhet	Hendelsen skjer ved uhell, feil, tilfeldighet, ukyndighet eller tilsvarende som kan medføre et sikkerhetsbrudd.