1. Sikkerhetsinstruks

Sikkerhetsinstruksen er en del av Helse Nords regionale styringssystem for informasjons-sikkerhet.

2. Område for sikkerhetsinstruksen

Sikkerhetsinstruksen 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.

Som bruker av virksomhetens informasjonssystem plikter du aktivt å hindre at uvedkommende får tilgang til opplysninger som er underlagt taushetsplikt.

3. Sikkerhetsbrudd

Hendelser som bryter med sikkerhetsinstruksen anses som sikkerhetsbrudd. Brudd på sikkerhetsinstruks ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for informasjonssikkerhet, og vil bli behandlet som personalsak. Alvorlige brudd på reglene i sikkerhetsinstruksen kan også resultere i strafferettslige reaksjoner.

3.1 Taushetsplikt

Alle pasienter og brukere av helse- og omsorgstjenester har rett til vern mot spredning av opplysninger om personlige og helsemessige forhold. Taushetsplikten innebærer både en passiv plikt til å tie og en aktiv plikt til å hindre at uvedkommende får tilgang til taushetsbelagt informasjon. All bruk av elektronisk journal etterlater elektroniske spor, ofte kalt logg. Loggen er en del av pasientens journal, som pasienten har rett til innsyn i.

1. Bare den som har tjenstlige behov for opplysninger i behandlings-, diagnostisk eller pleiemessig øyemed, eller for å administrere og kvalitetssikre helsehjelpen til den enkelte skal ha tilgang til journalopplysninger.
2. All tilgang til journalopplysninger gis og kontrolleres på individuell basis. Rettigheter må ikke lånes bort til andre, verken ved å gi fra seg passord eller ved å la andre benytte egen innlogget bruker.
3. Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i helsepersonelloven § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

3.2 IKT-utstyr og programvare

Det er kun tillatt å bruke IKT-utstyr, lagringsmedia og programvare anskaffet og/eller kontrollert av virksomheten i virksomhetens nett.

1. Bruk av annen programvare enn det som virksomheten tilbyr som standard programvare, må godkjennes av autorisert personell i foretaket og Helse Nord IKT.

2. Det er ikke tillatt å benytte andre løsninger for deling/fjernstyring av skjerm, møter etc. enn de som tilbys av Helse Nord IKT.
3. Utstyr som ikke tilhører virksomheten, skal ikke kobles i virksomhetens nett. Slikt utstyr kan kobles mot virksomhetens gjestenett. Særskilte behov for tilkobling av eget utstyr skal avklares med autorisert personell i foretaket og Helse Nord IKT.
4. Brukerkonto, eventuelle passord og adgangskort for mobilt kontor med tilhørende PIN-kode er den ansattes nøkkel til virksomhetens datasystem, og skal ikke oppgis eller lånes ut til noen andre.
5. Adgangskort skal ikke forlates i PC, og bør ikke oppbevares i nærheten av PC.
6. Eventuelle nedskrevne passord skal alltid oppbevares nedlåst.
7. Dersom det er mistanke om at passordet er blitt kjent av andre, skal det endres umiddelbart.
8. PC skal alltid låses (Windowstast + L) når arbeidsplassen/ PC-en forlates.
9. Fellesbruker skal ikke benyttes til annet enn den er godkjent for[3].
10. Bruker skal alltid logge ut av egen brukerkonto før maskinen overlates til andre. Dersom det er brukt fellesbruker skal det logges ut fra programmer, og PC skal låses.
11. Oppkobling mot eksterne nettverk og/eller deling av trådløse nett samtidig som maskinen er tilkoblet det interne nettverket, er ikke tillatt.
12. Dataskjermer skal plasseres slik at uvedkommende hindres innsyn.
13. Ansatte som slutter eller går ut i permisjon, skal levere alt utlevert IKT-utstyr (PC, mobiltelefon etc.) til foretaket, dersom ikke annet er avtalt.
14. Oppdatering av operativsystem og programvare som Helse Nord IKT sender til datamaskinen skal aksepteres, og maskinen omstartes ved første mulighet.
15. Helse Nord IKT kan påtvinge installering og omstart av maskiner dersom det er sikkerhetsmessig behov for det. Filer og opplysninger som ikke er lagret kan da gå tapt.

3.3 Privat bruk

Virksomhetens e-post anbefales ikke brukt til privat kommunikasjon. Skulle den ansatte motta privat e-post eller lagre private data på foretakets utstyr, må dette lagres i mapper merket «Privat». Foretaket vil respektere slik merking og vil ikke skaffe seg tilgang til data lagret på slike områder uten å ha særskilt hjemmelsgrunnlag. Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale[4] beskriver dette inngående.

Hovedregler ved privat bruk:

1. Begrenset tekstbehandling, beregning, sending og mottaking av e-post, samt lesing av websider (så lenge innholdet på sidene ikke er lovstridig) er tillatt.
2. Begrens bruk av din e-postadresse hos Helse Nord til private formål.
3. Lagring av private bilder, musikk, videoer (og andre store filer) på Helse Nords lagringsområder er ikke tillatt.

3.4 Lagring

1. Sensitive personopplysninger (inkl. avidentifiserte personopplysninger) skal ikke lagres på fellesområder eller brukerens hjemmeområde uten tilstrekkelig sikring av tilgang. Hva som er tilstrekkelig sikring må avklares med Informasjonssikkerhetsansvarlig i foretaket.
2. Sensitive personopplysninger skal ikke lagres på noe flyttbart lagringsmedium (inkludert c-disk på PC og minnepenn) uten tilstrekkelig sikring (for eksempel kryptering).
3. Det er ikke tillatt å benytte løsninger der det ikke kan garanteres at data lagres sikkert på et angitt sted. Alle nye lagringsløsninger skal godkjennes av autorisert personell i foretaket og Helse Nord IKT.
4. Kvalitetssikringsdata og forskningsdata skal lagres på dedikerte sikre områder.

3.5 Sending av helse- og personopplysninger

Helsenorge.no er den offentlige helseportalen for innbyggere i Norge. Det arbeides kontinuerlig med utvikling av nye tjenester for kommunikasjon med pasient via portalen.

1. Sensitive personopplysninger skal ikke sendes via vanlig e-post, telefaks, SMS, Skype eller tilsvarende løsninger. Det er heller ikke lov å sende fødselsnummer (11 siffer) på denne måten.
2. Dokumenter og lagringsmedia med sensitive personopplysninger skal alltid være forsvarlig sikret og forsendes i gjenlimt konvolutt / forseglet innpakning.
3. Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for mottak av de sensitive opplysningene.
4. Helsenorge.no skal benyttes til digital kommunikasjon med pasient i de tilfeller det er mulig.

3.6 Makulering/ sletting/ kassering

1. Dokumenter med helse- og personopplysninger skal makuleres[1] ved avhending.
2. Ansatte som slutter skal rydde i egne filområder, e-post, mobiltelefon og annet elektronisk utstyr og sikre at all relevant virksomhetsinformasjon blir lagret i relevante kataloger. Annen informasjon skal slettes. Helse Nord IKT vil slette gjenværende informasjon på brukerens områder når ansettelsesforholdet er avsluttet.
3. Harddisker, minnepinner eller annet utstyr som inneholder harddisker og andre elektroniske lagringsmedier (for eksempel nettbrett og smarttelefon), skal leveres til autorisert personell for forsvarlig destruksjon.
4. Ansatte som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutinene over.

3.7 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 du ansvarlig for at taushetsplikten blir overholdt og at pasienters og ansattes integritet blir ivaretatt.

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

3.8 E-post og kalender

Mange ansatte har delt møtekalender. Dette gjør at opplysninger som legges i møtekalenderen blir tilgjengelig for flere. Ved å krysse av for «Privat» i møteinnkallingen blir den bare tilgjengelig for møtedeltakerne. Ved mistanke om svindelforsøk (spam, whaling, phishing etc.) kan Helse Nord IKT slette e-post uten å involvere brukerne.

1. Massedistribusjon av informasjon skal være jobbrelatert og ansvarlig for distribusjonen skal være kritisk til innholdet i informasjonen og hvem den sendes til.
2. E-postmeldinger skal i utgangspunktet kun sendes til mottakere som trenger informasjonen.
3. Automatisk videresending til e-postkonto utenfor Helse Nord er ikke tillatt.

4. Det skal utvises aktsomhet ved mottak av e-post. Vedlegg kan inneholde virus. Ved tvil skal avsender eller Helse Nord IKT kontaktes eller e-postmeldingen slettes.
5. Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.
6. Møtekalenderen skal ikke brukes til sensitive helse- og personopplysninger, for eksempel som timebok for pasienter.
7. Vær varsom med hva du skriver i møteinnkallinger.
8. Dokumenter som inneholder sensitiv/ følsom informasjon skal ikke vedlegges i møteinnkallinger.
9. Signatur bør brukes ved sending av e-post, og ved sending fra felles e-postkontoer skal avsender legitimere seg med minimum navn.

3.9 Systemsvakheter og sikkerhetsbrudd

1. HN IKT logger aktivitet på enheter og nettverk til drifts- og sikkerhetsformål. Slike opplysninger vil kun anvendes for å motvirke og eventuelt følge opp sikkerhetsbrudd eller straffbare handlinger.
2. Det er ikke tillatt å foreta kartlegging/testing av mulige systemsvakheter, eller forsøke å trenge inn i interne eller eksterne systemer.
3. Det er ikke tillatt å forsøke å deaktivere eller forbigå etablerte sikkerhetsmekanismer (f.eks. antivirus), tilegne seg uautoriserte tilgangsrettigheter på lokal maskin, eller utnytte eventuelle sikkerhetssvakheter.
4. Mistenkelige hendelser og observerte sikkerhetsbrudd skal meldes som avvik i henhold til gjeldene avviksrutiner.

3.10 Forskning og kvalitetssikring

1. Alle forsknings- og kvalitetsregistre (prosjekter) skal meldes foretakets personvernombud.
2. For øvrige prosedyrer relatert til forskning og kvalitet henvises det til foretakets kvalitetssystem.

4. Eksterne referanser

NS-ISO/IEC 27002 kapittel 5 – Sikkerhetspolicyer og kapittel 7 – Personellsikkerhet
Norm for personvern og informasjonssikkerhet i helse- og omsorgstjenesten – Faktaark 27-Retningslinjer for daglig informasjonssikkerhet
[1]RL2801 – Makulering av utskrifter
[2]Etiske retningslinjer for ansatte i Helse Nord
[3]HN-ISMS-10 Tilgangsstyring
[4] Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale