mellom

<Medarbeider>, <rolle>
<11-sifret fødselsnr>
og
Foretak HF
org.nr. XXXXXX

Det er i dag inngått følgende avtale:

1. **FORMÅL MED AVTALEN**
   Avtalene gir foretaket instruksjonsmyndighet over <medarbeideren> når vedkommende benytter foretakets informasjonssystem, eller direkte/indirekte inngår i tjenesteyting knyttet til foretakets virksomhet.

2. **OPPDRAGSBESKRIVELSE**
   <Medarbeideren> skal utføre arbeidsoppgaver for med de ressurser virksomheten stiller til disposisjon.

3. **FORUTSETNINGER FOR ARBEIDSFORHOLDET**
   Foretaket har instruksjonsmyndighet i forhold til <medarbeideren> i den perioden vedkommende utfører tjeneste for foretaket, jamfør Helseregisterloven § 13, 1. ledd.

TAUSHETSPLIKT OG SIKKERHETSINSTRUKS

Denne erklæringen gjelder informasjon medarbeideren tilegner seg gjennom deltakelse i virksomhet knyttet til foretaket og gjennomføring av IPS-tjenester, slik som f.eks. deltakelse i arbeidsrettet team og behandlerteam.

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. vil den avdekke hvilke steder som oppsøkes på Internett, av hvem og tidspunkt.

Hvis det avdekkes at bruken av informasjonssystemet er i strid med foretakets bestemmelser, herunder sniklesing i pasientjournaler, vil det kunne bli iverksatt sanksjoner.

JEG FORSTÅR:

- at jeg i mitt arbeid/praksis for foretaket vil få kjennskap til forhold som det av hensyn til pasienter, deres pårørende, barn og forelder/foresatte eller andre er nødvendig å bevare taushet om.
- at dette arbeidet krever ansvarsfølelse, lojalitet og plikttroskap.
- at brudd på taushetsplikten kan medføre straffeansvar og eventuelt fjernelse fra tjenesten.
- at taushetsplikten også gjelder etter at jeg har sluttet i tjenesten

Jeg er innforstått med at den taushetserklæring som jeg har undertegnet også gjelder for bruk av Internett og e-post.

Jeg er innforstått med at eiendomsretten til alt IT-utstyr ved foretaket, det være seg innhold, programvare, virksomhetsrelatert e-post og dokumenter som er lagret på Nordlandssykehusets maskiner, er å regne som foretakets eiendom. Med dette forstås at ingenting kan regnes som privat og ikke benyttes til andre formål enn det som denne erklæringen omfatter. Forskningsdata/-arbeid reguleres i tillegg av egne retningslinjer.

Når jeg bruker sykehusets 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. Det er ikke tillatt å benytte samme passord for pålogging til foretakets systemer som man benytter for pålogging til systemer eller tjenester som ikke tilhører foretaket.

Ved å signere denne avtalen bekrefter jeg å ha mottatt et eksemplar av Helse Nords Sikkerhetsinstruks for bruk av foretakets IT-system, har gjennomgått, forstått og akseptert dette. Sikkerhetsinstruksen vedlegges denne avtalen.

Jeg skal innrette meg etter den til enhver tid gjeldende sikkerhetsinstruks for foretaket og andre aktuelle internkontrollrutiner. **Jeg skal gjennomgå og må ha bestått** obligatorisk e-læringskurs i informasjonssikkerhet før tilgang blir gitt til foretakets informasjonssystem.

4. LØNNSUTBETALING

<Medarbeideren> mottar ikke lønn fra foretaket.

5. ENDRINGER

Eventuelle endringer og tillegg til nærværende avtale skal inngås skriftlig.

6. VARIGHET

Avtalen gjelder fra xx.xx.xxxx og så lenge <medarbeideren> utfører arbeid for foretaket. Tilgang til foretakets informasjonssystem skal stenges ved opphør av avtalen.

Denne avtale er undertegnet i 2 – to – eksemplar, hvorav hver part beholder 1 – ett – eksemplar. I forbindelse med signering av skjema skal nyeste versjon av Helse Nords sikkerhetsinstruks for bruk av foretakets IKT-system, RL0259, skrives ut og gjennomgås sammen med brukeren.

<sted>, den ……	<sted>, den……
……..	……
Leder	<Medarbeider>

(For NLSH: Underskrevet avtale vil bli oppbevart i ephorte 2017/2006 KAPH – taushetserklæringer)
(For UNN: Underskrevet avtale vil bli oppbevart i ephorte 2017/5108 Taushetserklæring NAV/IPS)

Saksgang: *Skjema er utarbeidet med utgangspunkt i Helse Nords mal for «avtale om tilgang og taushetsplikt for medarbeider som ikke er ansatt i eller lønnet av foretaket». Helse Nords policy er at slike avtaler i større grad skal utarbeides lokalt, jf prosjektet «helhetlig informasjonssikkerhet», prosjektnr 180066.*
Avtalen er tilrettelagt for bruk for IPS formål av KAPH, med bistand av Informasjonssikkerhetsansvarlig og personvernombud i NLSH, jurist Alisa Larsen.
Skjema, og særlige problemstillinger knyttet til taushetsplikt og IPS, har også vært tema for behandling i regionalt fagråd for informasjonssikkerhet i to møter, vår og høst 2017.

HELSE NORD	**Sikkerhetsinstruks (versjon 2.4)**

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 minimum 8 tegn og være en kombinasjon av store og små bokstaver og tall eller spesialtegn. 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. 2a 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)

a) Foretaket legger inn viktig informasjon på sine interne intranett-sider. De ansatte skal gjøre seg kjent med innholdet og bør daglig sjekke disse sidene.

b) 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.
c) 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/Informasjonssikkerhetsansvarlig.
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. 2) 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.