## 1. Endringer siden siste versjon

Begrensninger i bruk av e-post ifm journal- og helsespørsmål fra publikum/pasienter.

Erstatter og utfyller databrukerkontrakt.

## 2. Definisjoner

**Konsesjon –** tillatelse fra Datatilsynet til å behandle sensitive personopplysninger. Tillatelsen er gitt med vilkår i konsesjon og lov, og er begrenset til prosjektets angitte formål og sikkerhetsregulering som konsesjonen er gitt for.

**Melding –** selverklæring når det gjelder behandling og sikkerhetsregulering av personopplysninger med vilkår i lov, og gir forutsetninger for behandlingen av opplysningene. Vil være grunnlag for eventuelt tilsyn.

**Personopplysninger** – opplysninger og vurderinger som kan knyttes til en enkeltperson.

**Sensitive personopplysninger** – opplysninger om

a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,

b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,

c) helseforhold,

d) seksuelle forhold,

e) medlemskap i fagforeninger

**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.

## 3. Formål

Formålet med denne instruksen er å etablere et felles sett med sikkerhetsregler for alle medarbeidere ved bruk av sykehusets IKT-løsninger og elektronisk produserte opplysninger.

Instruksen er en del av UUS internkontrollsystem, slik som beskrevet i helseregisterloven (hlsregl) og personopplysningsloven (popplyl).

## 4. Omfang

Denne sikkerhetsinstruks gjelder for alle ansatte, leverandører, konsulenter, vikarer og andre som gis tilgang til virksomhetens elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer, inkludert stasjonært og bærbart utstyr, nettverk, pasientsystemer, programvare m.m.

## 5. Ansvar

Enhver leder er ansvarlig for å informere og gjøre tilgjengelig denne instruks for sine medarbeidere. Brukerne er selv ansvarlig for å

gjøre seg kjent med og følge reglene i denne instruks.

## 6. Fremgangsmåte

**Fysisk adgang**

- Alle ansatte skal bære gyldig ID-kort
- Den enkelte medarbeider skal, ved hjelp av fysiske sikringstiltak og/eller tilsyn, hindre at uvedkommende får adgang til dokumenter, flyttbare medier og annet utstyr som inneholder opplysninger det gjelder taushetsplikt for.
- Dersom ID kort/nøkler mistes/blir stjålet, må dette straks meldes til ID-kontoret på (221)18126, eller til portvakten på (221)18001.
- Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/nøkkelkort tilbake til ID-kontoret dersom ikke annet er avtalt.
- Den som mottar besøkende, er ansvarlig for at disse ikke oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av en ansatt.
- Personer som oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av ansatt, uten ID-kort eller uten godkjennelse fra leder ansvarlig for området, skal bortvises.

**Bruk av UUS informasjonssystemer**

*Logging*

Internett- og nettverkstrafikk blir logget for administrasjon og for å følge opp sykehusets sikkerhetsretningslinjer. Det betyr at den ansattes /-medarbeiders aktiviteter på nettet og ved bruk av program blir registrert, og at det er mulig å spore tilbake til den enkelte om det oppdages brudd på sykehusets retningslinjer.

Loggføringen omfatter aktivitet i nettverket, bruk av tjenester og programmer, og spesielt bruk og aktivitet i systemer som inneholder pasientopplysninger. Autorisert personell gjennomgår loggene og iverksetter tiltak om nødvendig. Brudd på sykehusets sikkerhetsretningslinjer vil rapporteres til nærmeste overordnede.

*Om privat bruk*

Sykehusets informasjonssystemer er beregnet og skal primært benyttes for jobbrelaterte formål. Eventuell privat bruk skal ikke gå ut over virksomhetsrelaterte oppgaver og funksjoner.

- Noe privat bruk tillates, inkludert mindre mengder e-post, nyheter og opplysningstjenester. Dette må imidlertid ikke påvirke jobbrelaterte oppgaver, eller være i strid med denne instruks, lover eller allmenne normer for oppførsel og sosial atferd.
- Mindre mengder private filer kan lagres i egen katalog på personlig område på Ullevål-nettet forutsatt at katalogen er merket "privat". Av plass og kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres på Ullevål-nettet.

*Eierskap og ansvar*

Informasjonssystemet og alt tilhørende utstyr, programvare og lagret informasjon (også på klienter), er sykehusets eiendom og ansvar.

Sykehuset har innsynsrett i all informasjon lagret i informasjonssystemene begrunnet ut fra sykehusets behov. Dette inkluderer gjennomgang for å avdekke brudd på sykehusets sikkerhetsretningslinjer. Ved uforutsett fravær vil e-postkassen, personlig hjemmekatalog og lignende kunne åpnes for nærmeste leder sammen med en tillitsvalgt eller annen objektiv part for å hente ut tjenestemessige dokumenter. Det vil dersom mulig, innhentes samtykke fra den det gjelder, men dersom det ikke lar seg gjøre, vil personvernet ivaretas av tillitsvalgt eller annen objektiv part.

*IKT-utstyr*

Det er kun tillatt å bruke IKT-utstyr, lagringsmedia og programvare anskaffet av IT-senteret i Ullevålnettet:

- Installasjon av alt utstyr og programvare skal gjøres av IT-senterets ansatte eller av de som er utpekt til å gjøre denne jobben.
- Bruk av annen programvare utenom det som sykehuset tilbyr som standard programvare, må godkjennes av autorisert personell.

Det skal ikke tilkobles privat utstyr i sykehusets nett. Dette gjelder også privat PDA, mobiltelefon og

fotoapparat.

Eksterne konsulenter og vikarer skal ikke koble til egne PC'er i sykehusets nett, men få tildelt maskin av sykehuset. Særskilte behov for egne PC'er skal avklares med IKT-sikkerhetssjef.

Det skal ikke tilkobles separate eksterne forbindelser til sykehusets nett (for eksempel via ekstra nettverkskort, trådløst forbindelse, modem, ISDN el) uten IT-senterets godkjennelse og medvirkning. Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

IT-utstyr skal ikke flyttes eller lånes til andre rom/lokaler uten avtale med IT-senteret.

Dataskjermer skal plasseres slik at det ikke er innsyn for uvedkommende.

Ansatte som slutter eller går ut i permisjon, skal levere alt utlevert IKT-utstyr (mobil PC, mobiltelefon, PDA, brikke for fjerntilgang osv) og programvarelisenser til IT-senteret, dersom ikke annet er avtalt .

*Pålogging og avlogging, brukernavn, passord og skjermsparer*

- Passordet (og eventuelt brikke/kort for fjerntilgang) er den ansattes nøkkel til sykehusets datasystem og skal ikke oppgis til eller lånes ut til andre. Dette er et personlig ansvar
- Det er ikke tillatt å bruke en annens brukertilgang/passord
- Passord bør IKKE skrives ned. Eventuelle nedskrevne passord skal alltid oppbevares nedlåst el.
- Velg et passord som er lett å huske, men det skal ikke inneholde navn på familiemedlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.
- Passordet skal bestå av en kombinasjon av store og små bokstaver og tall/tegn og være minst 8 tegn. Siste 5 passord skal ikke gjenbrukes. Passord skal endres regelmessig, systemet sier i fra når dette skal gjøres (enkelte gamle systemer kan avvike fra dette)
- Dersom det er mistanke om at passordet er blitt kjent av andre, skal passordet byttes.
- Passordbeskyttet skjermsparer skal benyttes og/eller kontordør låses når arbeidsplassen/maskinen forlates i kortere perioder.
- Brukeren skal alltid logge ut før maskinen overlates til andre. Hurtiglogging fra DL-Pasdoc benyttes for å sikre rask innlogging igjen.

*Informasjonshåndtering*

Personopplysningsloven (POL) omfatter personvern og gir krav til beskyttelse av Person- og helseopplysninger. Den gjelder helt fra det er registrert enkle opplysninger vedrørende én enkelt person.

- Et personregister er etablert dersom det registreres mer personidentifikasjon enn fødselsår og initialer. Registre skal før det opprettes ha håndtert konsesjon eller melding. Behovet for dette sammen med behov for teknisk sikring vurderes av personvernombud. Instruks og meldeskjema finnes i sykehusets e-håndbok, på Intranett og Internett.
- For all annen bruk av sensitive personopplysninger og personregistre enn direkte helsehjelp og pålagte meldinger, skal det som hovedregel innhentes samtykke fra de inkluderte.
- Person- og helseopplysninger ved sykehuset skal ikke gjøres tilgjengelig for uautorisert personell eller andre uvedkommende, herunder også egne ansatte.
- Det skal ikke søkes etter pasientinformasjon eller andre opplysninger den ansatte ikke har bruk for i det daglig arbeid.
- Utskrifter skal hentes umiddelbart.

*Lagring*

Det er som hovedregel kun tillatt å lagre sensitive personopplysninger i godkjente fagapplikasjoner på Ullevål-nettet. Unntak fra dette er:

- Bruk av ikke-fagapplikasjoner (som Word) for skriving av journaler, sakkyndig rapporter og tilsvarende er KUN tillatt dersom dette er tiltenkt som midlertidig lagring. Navn personnummer og andre direkte identifiserbare kjennetegn skal skrives inn så sent som mulig og slettes straks de er skrevet ut, slik at disse opplysninger elektronisk kun er tilgjengelig i minimalt tidsrom. Denne midlertidige lagring skal bare skje på avdelingens fellesområde / hjemmeområde på serveren. Notatene SKAL slettes etter de er godkjent, eventuelt lagt inn i fagapplikasjoner og skrevet ut.
- Person- og helse- opplysninger skal bare lagres lokalt på PC eller på portabelt utstyr som bærbar PC, og minnepinner eller lignende dersom det er innhentet godkjenning fra Personvernombudet og forutsatt at lagring skjer med løsninger godkjent av IKT-sikkerhetssjef. Dette gjelder også kodede (avidentifiserte) opplysninger.

- Slike opplysninger skal ikke lagres på PDA, mobiltelefon, MP3 spillere eller tilsvarende og aldri på privat utstyr. Bruk av kamera må sikres med egne rutiner og må ikke være privat kamera.
- Sensitive personopplysninger, inkludert kodede (avidentifiserte personopplysninger) skal aldri lagres i UiO-nettet.
- Forskningsstudier skal som hovedregel lagres på dedikert forskningsserver. Unntak skal være registrert og avtalt i melding til sykehusets Personvernombud.
- Kvalitetsregistre skal som hovedregel lagres på dedikert kvalitetssikringsserver. Unntak skal være registrert og avtalt i melding til sykehusets Personvernombud.

Når lagringsmedia eller dokumenter med registre eller sensitive personopplysninger ikke er under direkte oppsyn, skal kontor avlåses eller alternativt media/dokumenter nedlåses i skap/skuff slik at uvedkommende ikke kan få tilgang.

*Forsendelse*

Sensitive personopplysninger skal ikke sendes på åpen epost, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. IKT-sikkerhetssjef skal alltid involveres i nødvendig risikovurdering før slikt utstyr benyttes.

Dokumenter og lagringsmedia med sensitive personopplysninger skal alltid forsendes i gjenlimt konvolutt/forseglet innpakning.

Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for opplysningene.

Sensitive personopplysninger kan kun utleveres dersom det foreligger nødvendig hjemmel. Utlevering uten slik hjemmel vil være et alvorlig sikkerhetsbrudd.

*Makulering/sletting av dokumenter*

Dokumenter med person og helseopplysninger skal makuleres ved avhending gjennom bruk av makuleringsenhet, avlåste beholdere eller avlåste dedikerte rom for mellomlagring. Dersom ekstern leverandør benyttes for makulering, må det kontrolleres at dokumentene aldri er tilgjengelig for uvedkommende og at makulering skjer uten unødvendig opphold hos leverandør.

Ansatte som slutter, skal rydde i egne filområder og e-post og sikre at all relevant virksomhetsinformasjon blir lagret på relevante kataloger. IT-senteret vil når ansettelsesforholdet er avsluttet, slette gjenværende informasjon på brukerens områder.

Ansatte som slutter, skal makulere eller avlevere egne dokumenter i henhold til rutinene over.

*Kassering/Håndtering av utstyr og lagringsmedier*

Harddisker, minnepinner eller utstyr som inneholder harddisker og andre elektroniske lagringsmedier, skal leveres til IT-senteret for forsvarlig destruksjon.

Lagringsmedia som CD, DVD og floppy-disker osv som inneholder sensitive person- og helseopplysninger (inkluderte kodede), skal leveres til IT-senteret for destruksjon, mens media med andre opplysninger klippes/brekkes i biter og kastes som avfall. Alternativt kan tilsvarende løsninger selv etableres og benyttes etter godkjenning av IKT-sikkerhetssjef.

Ansatte som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutinene over.

*Sikkerhetskopiering*

For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på eller eventuelt systemtisk kopieres til Ullevålnettet. IT-senteret tar regelmessige sikkerhetskopier av all informasjon på Ullevålnettet. Lokal harddisk på PC-er i Ullevålnettet blir det ikke tatt sikkerhetskopier av.

Ved behov for rekontruksjon av informasjon på Ullevålnettet, kontakt IT-senteret.

*Internett*

Den ansattes oppslag på Internett kan spores tilbake til virksomheten og den PC/brukerkode oppslaget er utført fra.

Internett skal benyttes med varsomhet og i samsvar med vanlige etiske normer, slik at virksomhetsrelaterte oppgaver og funksjoner, samt opplysninger virksomheten behandler, ikke blir skadelidende.

- Det er ikke tillatt å surfe på sider eller laste ned og lagre filer som inneholder pornografi, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare), eller informasjon som er støtende, trakasserende, obskøne, truende eller rasistiske. Slike filer kan bli slettet automatisk
- Det er ikke tillatt å laste ned og instrallere programvare på UUS IKT-utstyr
- Fildelingstjenester tillates ikke
- Ressurskrevende ikke jobbrelaterte tjenester/applikasjoner, f.eks. radiolytting og TV/video streaming, tillates ikke.

*E-post og viruskontroll*

Det skal skilles på intern og ekstern e-post. Merking eller annen tilsvarende funksjonalitet skal bekrefte at det som sendes ut ikke inneholder sensitive personopplysninger. Ekstern e-post som ikke er merket slik, blir blokkert av sikkerhetssystemet.

E-post er ikke sikkert nok til å kommunisere sensitive personopplysninger/journalopplysninger med. Dersom pasienter likevel skulle sende forespørsel om egen eller andre navngitte personers helse via e-post, skal dette besvares med at e-post ikke kan benyttes for slik kommunikasjon. Henvendelsen fra pasient må ivaretas på annen måte, slik at forespørsel blir tilstrekkelig besvart.

Eventuell privat e-post skal lagres i en egen mappe merket ”privat”.

Massedistribusjon av informasjon skal eventuelt være jobbrelatert og ansvarlig for distribusjon skal være kritisk til innholdet i informasjonen og hvem den sendes til.

E-postmeldinger skal i utgangspunktet kun sendes til mottakere som trenger informasjonen.

Det skal utvises aktsomhet ved mottak av e-post. Vedlegg kan inneholde virus. Ved tvil skal avsender eller IT-senteret kontaktes eller e-post-meldingen slettes.

Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.

*Reparasjon, service, vedlikehold og brukerstøtte*

- Ta kontakt med IT-senteret dersom du har mistanke om feil eller problemer med tilgang til systemer, tjenester eller informasjon
- IKT-utstyr som skal til rearasjon, skal hentes av IT-senteret for utføring av nødvendige sikkerhetstiltak før utstyret videresende til reparasjon.
- Eventuelle feilmeldinger til utstyrsleverandører skal sendes til IT-senteret. Dette gjelder også utstyr som skal til sevice.
- Det er kun IT-senteret som skal initiere arbeid som skal utføres av ekstern personell på Ullevålnettest systemer og utstyr.

*Kartlegging og utnyttelse av systemsvakheter*

Den ansatte skal ikke på eget initiativ foreta kartlegging eller testing av mulige systemsvakheter, forsøke å trenge inn i interne eller eksterne systemer, forsøke å forbigå etablerte sikkerhetsmekanismer, tilegne seg utvidede tilgangsrettigheter på lokal maskin eller utnytte eventuelle sikkerhetssvakheter.

**Personell og sikkerhet - Sikkerhetsbrudd**

Mistenkelige hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste leder, Sikkerhetssjef ved fysisiske innbrudd eller IKT-sikkerhetssjef. Hendelser knyttet til at denne sikkerhetsinstruks ikke følges, vurderes som sikkerhetsbrudd. Brudd på sikkerhetsinstruks ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for sikkerhet, og vil bli behandlet som personalsak. Alvorlige brudd på reglene i sikkerhetsinstruksen vil få konsekvenser for ansattes arbeidsforhold samt eventuelt resultere i strafferettslige reaksjoner.

## 7. Handling ved dissens eller feilsituasjoner

Brudd på denne instruksen sees på som mislighold av arbeidsavtalen og UUS styringssystem for sikkerhet, og vil kunne ha påvirkning på arbeidsforholdet.

IKT-sikkerhetssjef/personvernombud kan benyttes for rådføring.

## 8. Referanser

Lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (helseregisterloven)

Lov av 2. juli 1999 nr. 64 om helsepersonell m.v. (helsepersonelloven)

Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Forskrift av 15. des. 2000 om behandling av personopplysninger (personopplysningsforskriften)