Innledning

Hvem sikkerhetsinstruksen gjelder for
Denne sikkerhetsinstruksen gjelder for alle ansatte, vikarer, leverandører, konsulenter og andre som gis tilgang til virksomhetens elektroniske tjenester.

Bakgrunn
Helselovgivningen sammen med personopplysningsloven stiller strenge krav til behandling av helse- og personopplysninger. Dette er for det første begrunnet i helseforetakenes plikt til å sikre opplysningenes tilgjengelighet og integritet for å kunne gi livsviktig helsehjelp. I tillegg har alle som benytter seg av tjenestene som helseforetaket yter, rett til å stole på at helse- og personopplysninger om han/henne blir behandlet fortrolig og er sikret mot at personell som ikke er autorisert får innsyn i disse opplysningene.

Kravene i denne instruksen er minimumskrav som må ivaretas av alle som er omfattet av instruksen, for å sikre at det ikke skjer brudd på lovkravene.

Ansvar
Alle som er omfattet av denne instruksen har et personlig ansvar for å gjøre seg kjent med instruksen og etterleve den. Instruksen med de bestemmelser den inneholder er en del av de vilkår du har forpliktet deg til som ansatt/vikar i helseforetaket. For tjenesteleverandører til helseforetaket gjelder det samme med bakgrunn i det kontraktsforhold disse har forpliktet seg til.

Brudd på de rutiner og bestemmelser som instruksen inneholder innebærer brudd på dine forpliktelser overfor helseforetaket enten som ansatt/vikar eller som tjenesteleverandør. Dette kan derfor få personalmessige konsekvenser eller konsekvenser for kontraktsforholdet med helseforetaket.

Generelt aktsomhetskrav
Det faktum at du i kraft av ditt ansettelsesforhold eller kontraktsforhold til helseforetaket kan benytte virksomhetens informasjonssystem, forplikter deg spesielt til å opptre med aktsomhet og god etikk. Den enkelte bruker skal derfor ha et reflektert forhold til hvilke søk og nedlastinger av materiale som foretas.

Du må også være aktsom i forhold til hva som kommuniseres ut. Ta derfor utgangspunkt i at du aldri er anonym på nettet og at all kommunikasjon på nettet kan spores tilbake til maskinen du benytter.

Sikkerhetsregler

Ivaretakelse av taushetsplikten - tilgang til dokumenter
Som bruker av helseforetakets informasjonssystem plikter du aktivt å hindre at uvedkommende får tilgang til dokumenter eller andre medier som inneholder opplysninger som er underlagt taushetsplikt.

Bruk av virksomhetens informasjonssystemer

Eierskap og ansvar
Informasjonssystemet og alt tilhørende utstyr, programvare og lagret informasjon (også på klienter), bortsett fra privat informasjon, er virksomhetens eiendom og ansvar.

Under gitte omstendigheter og på nærmere bestemte vilkår kan arbeidsgiver ha rett til innsyn i den enkelte sine dokumenter og e-post. Vilkårene for slikt innsyn er regulert særskilt i egen instruks i styringssystemet for sikkerhet.

Logging
Internett- og nettverkstrafikk blir logget for å følge opp virksomhetens sikkerhetsregler. Det betyr at den ansattes aktiviteter på nettet, samt bruk av program og tjenester blir registrert, og at det er mulig å spore tilbake om det oppdages brudd på virksomhetens sikkerhetsregler.

Logg fra pasientjournaler blir gjennomgått jevnlig og ved mistanke om urettmessig bruk av autorisert personell, slik det er beskrevet i foretakets retningslinjer for dette.

Privat bruk av informasjonssystemet
Utgangspunktet er at virksomhetens informasjonssystem kun skal brukes til virksomhetsrelaterte oppgaver. Helseforetaket tillater imidlertid begrenset bruk av informasjonssytemet til private formål. Dette innbefatter:

- Tekstbehandling, beregning, sending og mottaking av e-post, samt lesing av websider så lenge innholdet på sidene ikke er lovstridig.

Private dokumenter og e-post i moderat omfang kan lagres i informasjonssystemet. Dette gjøres på område som er merket "privat". Dersom privat e-post ikke blir lagret på område som er særskilt avmerket for slike formål, har den ikke samme beskyttelse mot innsyn fra arbeidsgiver som hvis den merkes.

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

- Installasjon av alt utstyr og programvare skal gjøres av autorisert personell.
- Bruk av annen programvare enn det som virksomheten tilbyr som standard programvare, må godkjennes av autorisert personell.
- Det skal ikke tilkobles privat utstyr i virksomhetens nett. Dette gjelder også private USB lagringsenheter, PDA, mobiltelefon, fotoapparat og lignende.
- Eksterne konsulenter og vikarer skal ikke koble til egne PC'er i virksomhetens nett, men bruke gjestenettet eller få tildelt maskin av virksomheten. Særskilte behov for tilkobling av eget utstyr skal avklares med autorisert personell.
- Utstyr som ikke inngår i mobile løsninger skal ikke tilkobles andre nettverk enn det som er tilrettelagt på arbeidsplassen.
- Oppkobling mot eksterne nettverk, oppkobling med modem/ISDN og/eller deling av trådløse nett samtidig som maskinen er tilkoblet det interne nettverket er ikke tillatt.
- Dataskjermer skal plasseres slik at innsyn for uvedkommende hindres.

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

Pålogging og avlogging, brukernavn, passord og skjermsparer

- Passordet (og eventuelt brikke/kort for fjernaksess) er den ansattes nøkkel til virksomhetens datasystem, og skal ikke oppgis eller lånes ut til andre, eller forlates i PC'en. Dette er et personlig ansvar.
- Det er ikke tillatt å bruke en annens brukertilgang.
- Passord bør IKKE skrives ned. Eventuelle nedskrevne passord skal alltid oppbevares nedlåst e.l.
- Passord skal ikke inneholde navn på familiemedlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.
- Dersom det er mistanke om at passordet er blitt kjent av andre, skal det byttes.
- Passordbeskyttet skjermsparer (ctr+alt+del) skal benyttes og/eller kontordør låses når arbeidsplassen/maskinen forlates.
- Brukeren skal *alltid* logge ut av nettverket før maskinen overlates til andre. Dersom det er brukt "fellesbruker" skal det logges ut fra programmer, og skjermen skal låses.
- "Fellesbruker" skal ikke benyttes til annet enn det den er godkjent for.
- Studenter skal ikke bruke studentkonto når de utfører arbeid som ansatt/vikar i foretaket.

Informasjonshåndtering

Personopplysningsloven (POL) omfatter personvern og setter 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 fått konsesjon eller blitt meldt. Behovet for dette, sammen med behov for teknisk sikring, vurderes av personvernombud (når det gjelder forskning) eller annen autorisert innenfor IT-sikkerhet (IKT-sikkerhetsleder og ev. Helse Vest IKT).
- 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 i virksomheten skal ikke gjøres tilgjengelig for uautorisert personell eller andre uvedkommende, herunder også egne ansatte.
- Det er ikke tillatt å søke etter pasientinformasjon eller andre opplysninger den ansatte ikke har bruk for i det daglig arbeid.
- Det må kontrolleres at det skrives ut til rett skriver.
- Utskrifter skal hentes umiddelbart.

Lagring

- Sensitive personopplysninger skal ikke lagres på fellesområder (f:) eller brukerens hjemmeområde (h:) uten tilstrekkelig sikring av tilgang. Hva som er tilstrekkelig sikring må avklares med IKT-sikkerhetsleder.
- Sensitive personopplysninger skal ikke lagres på noe flyttbart lagringsmedium (inkl. c-disken på stasjonær PC) uten tilstrekkelig sikring.

Forsendelse

- Sensitive personopplysninger skal ikke sendes via vanlig e-post, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger.
- Dokumenter og lagringsmedia med sensitive personopplysninger skal alltid være forsvarlig sikret og forsendes i gjenlimt konvolutt/forseglet innpakning.
- Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for mottak av de sensitive opplysningene.

Makulering/sletting av dokumenter

- Dokumenter med person- og helseopplysninger skal makuleres ved avhending.
- Ansatte som slutter skal rydde i egne filområder og e-post og sikre at all relevant virksomhetsinformasjon blir lagret i relevante kataloger. Helse Vest IKT vil slette gjenværende informasjon på brukerens områder når ansettelsesforholdet er avsluttet.
- 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 Miljøhallen for forsvarlig destruksjon.
- Ansatte som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutinene over.

Internett

Internett skal benyttes med varsomhet og i samsvar med vanlige etiske normer for virksomheten. Virksomhetsrelaterte oppgaver og funksjoner, samt opplysninger virksomheten behandler, skal ikke bli skadelidende. Aktiviteter på Internett kan spores tilbake til virksomheten og den PC/brukerkode oppslaget er utført fra.

- Det er ikke tillatt å laste ned og/eller lagre filer (program, grafikk, audio, video mv.) til foretakets informasjonssystem med mindre dette utføres som en del av jobbrelatert virksomhet.

E-post og viruskontroll

- Det skal skilles på intern og ekstern e-post. Merking med IS: (det står for Ikke Sensitiv) først i emnefeltet skal bekrefte at det som sendes ut ikke inneholder sensitive personopplysninger. Ekstern e-post som ikke er merket slik, blir blokkert av sikkerhetssystemet. Intern e-post skal ikke merkes med IS:.
- Fødselsnummer skal ikke sendes med e-post.
- Den personlige brukerkoden skal ikke oppgis i ekstern e-postadresse.

- Massedistribusjon av informasjon skal være jobbrelatert og ansvarlig for distribusjonen 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 driftsenheten kontaktes eller e-postmeldingen slettes.
- Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.

Outlook møtekalender
Mange ansatte har delt møtekalender. Dette gjør at opplysninger som legges i møtekalenderen blir tilgjengelig for hele foretaket.
- Møtekalenderen skal ikke brukes til sensitive helse- og personopplysninger, for eksempel som timebok for pasienter.
- Vær varsom med hva du skriver i møteinnkallinger.
- Vær varsom med å sende dokumenter som vedlegg til møteinnkallinger. Ved å krysse av for "privat" i møteinnkallingen blir den bare tilgjengelig for møtedeltakerne.

Kartlegging og utnyttelse av systemsvakheter
Det er ikke tillatt å 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.

Sikkerhetsbrudd

Mistenkelige hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste leder og/eller IKT-sikkerhetsleder. Hendelser knyttet til at denne sikkerhetsinstruksen ikke følges, vurderes som sikkerhetsbrudd. Brudd på sikkerhetsinstruks ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for IKT-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.