Innledning

Instruks for IKT -sikkerhet ***(sikkerhetsinstruksen) gjelder for alle ansatte, vikarer, studenter, 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 virksomhetenes plikt til å sikre opplysningenes tilgjengelighet og integritet for å kunne gi livsviktig helsehjelp. I tillegg har alle som benytter seg av tjenestene som virksomhetene yter, rett til å stole på at helse- og personopplysninger om han/henne blir behandlet fortrolig (konfidensialitet) 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. På læringsportalen finner du e-læringskurs i informasjonssikkerhet. Instruksen med de bestemmelser den inneholder er en del av de vilkår du har forpliktet deg til. For tjenesteleverandører til virksomhetene 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 virksomheten. Dette kan derfor få personalmessige konsekvenser eller konsekvenser for kontraktsforholdet med virksomheten.

Generelt aktsomhetskrav

Det faktum at du i kraft av ditt ansettelsesforhold eller kontraktsforhold til virksomheten 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 deling og lagring av informasjon på nettet, samt hvilke søk og nedlastinger av materiale som foretas.

Du må også være aktsom i forhold til hva som kommuniseres ut, f.eks. på internett via sosiale medier. 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 virksomhetens informasjonssystem plikter du aktivt å hindre at uvedkommende får tilgang til dokumenter eller andre medier som inneholder opplysninger som er underlagt taushetsplikt. Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte taushetsbelagte opplysninger uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

Bruk av virksomhetens informasjonssystemer
Eierskap og ansvar
Informasjonssystemet og alt tilhørende utstyr, programvare og lagret informasjon, 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 enkeltes dokumenter og e-post. Vilkårene for slikt innsyn er regulert særskilt i egen instruks i styringssystemet for IKT-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. Ved mistanke om urettmessig innsyn, vil dette bli håndtert i henhold til virksomhetens retningslinjer.

Privat bruk av informasjonssystemet
Utgangspunktet er at virksomhetens informasjonssystem kun skal brukes til virksomhetsrelaterte oppgaver. Det tillates imidlertid begrenset bruk av informasjonssytemet til private formål innenfor samme regler som ellers gjelder. 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 bør lagres 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 og programvare
Det er kun tillatt å bruke IKT-utstyr, lagringsmedia og programvare *anskaffet av virksomheten* i virksomhetens nett. Nedenfor er listet noen eksempler.
- 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.
- 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.
- Oppkobling mot eksterne nettverk 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 (PC, mobiltelefon, brikke/kort

for fjernaksess osv) og programvarelisenser til virksomheten, 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 el.
- Passord skal bestå av min. 8 tegn og skal ikke lett kunne knyttes til brukeren.
- Dersom det er mistanke om at passordet er blitt kjent av andre, skal det byttes.
- Passordbeskyttet skjermsparer (ctr+alt+del) skal benyttes når arbeidsplassen/maskinen forlates.
- 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 skjermen skal låses.
- "Fellesbruker" skal ikke benyttes til annet enn den er godkjent for.
- Studenter skal ikke bruke studentkonto når de utfører arbeid som ansatt/vikar i foretaket.

Informasjonshåndtering

Personopplysningsloven omfatter personvern og setter krav til beskyttelse av helse- og personopplysninger. 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. Et register skal meldes til personvernombudet (eller Datatilsynet) før det opprettes for å vurdere rettslig grunnlag for behandling av personopplysningene. IKT-sikkerhetsleder (og ev. Helse Vest IKT) skal vurdere om registeret tilfredsstiller virksomhetens sikkerhetskrav.
- For all annen behandling av sensitive personopplysninger enn til direkte helsehjelp, innsamling til pålagte meldinger og andre lovbestemte behandlinger, skal det som hovedregel innhentes samtykke fra de inkluderte.
- Kvalitetssikring av helsehjelpen/helsetjenesten skal meldes til personvernombudet og kvalitetsregistre som opprettes skal lagres på spesielt tilviste områder (Kvalitetsserver).
- Forskningsprosjekter som faller inn under helseforskningsloven skal håndteres i henhold til Internkontrollsystem for medisinsk og helsefaglig forskning <link>.
- Forskningsprosjekt som faller utenfor helseforskningsloven skal meldes til personvernombudet for virksomheten og lagres på spesielt tilvist område (Forskningsserver).
- Helse- og personopplysninger i virksomheten skal ikke gjøres tilgjengelig for uautorisert personell eller andre uvedkommende, herunder også egne ansatte som ikke har tjenestelig behov.
- Det må kontrolleres at det skrives ut til rett skriver og utskrifter skal hentes umiddelbart.

Lagring

- 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 IKT-sikkerhetsleder <link>.
- Sensitive personopplysninger skal ikke lagres på noe flyttbart lagringsmedium (inkl. c-disken på stasjonær PC) uten tilstrekkelig sikring (for eksempel kryptering).
- Det er ikke tillatt å benytte løsninger der det ikke kan garanteres at data lagres sikkert på et angitt sted. "Nettskyen" kan være et eksempel på et usikkert lagringssted.
- Kvalitetssikringsdata og forskningsdata skal lagres på dedikerte områder (Kvalitetsserver og Forskningsserver).

Forsendelse

- Sensitive personopplysninger skal ikke sendes via vanlig e-post, telefaks, sms eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. Det er heller ikke lov å sende fødselsnummer på denne måten.
- 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 helse- og personopplysninger skal makuleres ved avhending.
- 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 Vest IKT vil slette gjenværende informasjon på brukerens områder når ansettelsesforholdet er avsluttet.

Kassering/håndtering av utstyr og lagringsmedier

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

Internett

Internett skal benyttes med varsomhet og i samsvar med 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, lyd, video mv.) til virksomhetens informasjonssystem, med mindre dette utføres som en del av jobbrelatert virksomhet. Slik nedlasting av programvare må avklares med autorisert personell.
- Det er ikke tillatt å benytte online møteplasser (deling av skjerm, filer, lyd/bilde) som ikke tilbys av virksomheten.

E-post og viruskontroll

- Det skal skilles på intern og ekstern e-post. Merking med Ikke Sensitiv (IS:) 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:*
- Din personlige brukerkode 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.

Sosiale media

Ved bruk av sosiale media er du ansvarlig for at taushetsplikten blir overholdt og at pasienters og ansattes integritet blir ivaretatt. Den enkelte virksomhet har utarbeidet veiledning/retningslinjer for slik bruk. Vær oppmerksom på at sosiale media også er utsatt for virusangrep.

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 meldes som avvik 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 og kan resultere i strafferettslige reaksjoner.

Utarbeidet av		**Utvalg for regional IKT-sikkerhet (sign)**
Godkjent av		**Erik Magne Hansen – Administrerende Direktør Helse Vest IKT AS (sign)**
Ref dok	**204**	**Instruks for innsyn i e-post og dokumenter**
Bare nettversjonen av dette dokumentet er gyldig versjon		

Helse Vest IKT AS

Seksjon	Dok nr.	Versjon	Tittel	Nivå	Side
Tiltak	**603**	**28.11.2013**	**Taushetserklæring – skjema**	**1**	**1/3**

Bakgrunn

Taushetsplikten i helsetjenesten verner om private interesser og er begrunnet i ønsket om beskyttelse av enkeltmenneskers personlige forhold og private sfære. Taushetsplikten er et sentralt element i personvernet. Taushetsplikten begrunnes også med at pasienter skal få behandling. Dersom helsepersonell og andre ikke har taushetsplikt kan dette medføre at pasienten eller pårørende unnlater å oppsøke hjelp av frykt for spredning av opplysninger.

Omfang

Taushetsplikten gjelder opplysninger om folks legems- eller sykdomsforhold, opplysinger om andre personlige forhold, opplysninger om tekniske innretninger, fremgangsmåter og forretningsforhold av konkurransemessig betydning, opplysninger av betydning for informasjonssikkerheten og opplysninger som det av andre grunner må sikres konfidensialitet for – som undertegnede får tilgang til i arbeidet. **Taushetsplikten gjelder også etter at tjeneste eller arbeid er avsluttet.**

Lovkrav

Det følgende beskriver lovpålagt taushetsplikt (utdrag av de aktuelle bestemmelsene er gitt på erklæringens side 2):

- i henhold til helsepersonelloven § 21 skal helsepersonell hindre at andre får kjennskap om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell. Det skal heller ikke leses, søkes etter eller besittes slik informasjon uten at det er begrunnet i helsehjelp, administrasjon av denne eller har annen lovhjemmel.
- i henhold til spesialisthelsetjenesteloven § 6-1 har alle som utfører tjeneste for helseinstitusjon som omfattes av loven taushetsplikt etter forvaltningsloven § 13
- i henhold til helseregisterloven § 15 har alle som behandler helseopplysinger etter helseregisterloven taushetsplikt etter forvaltningsloven § 13 og taushetspliktbestemmelsene i helsepersonelloven
- i henhold til pasientrettighetsloven § 3-6 skal opplysninger om legems- og sykdomsforhold og andre personopplysninger behandles i samsvar med gjeldende bestemmelser om taushetsplikt
- i henhold til forvaltningsloven § 13 plikter enhver som utfører tjeneste for et forvaltningsorgan å hindre at andre får kjennskap til det han gjennom tjenesten får vite om noens personlige forhold og om tekniske innretninger, fremgangsmåter og forretningsforhold av konkurransemessig betydning
- i henhold til personopplysningsforskriften § 2-9 skal medarbeidere pålegges taushetsplikt for personopplysninger det må sikres konfidensialitet for. Det skal sikres mot uautorisert innsyn i så vel personopplysninger som i informasjon med betydning for informasjonssikkerheten, jf. § 2-11.

Taushetsbrudd

I henhold til helsepersonelloven § 67 er det straffbart å overtre bestemmelsene i helsepersonelloven, herunder bestemmelsene om taushetsplikt.

I henhold til straffeloven § 121 er det straffbart å krenke taushetsplikt pålagt i henhold til lovbestemmelse eller gyldig instruks.

I henhold til straffeloven § 144 er det straffbart for leger, psykologer, apotekere, jordmødre og sykepleiere rettsstridig å åpenbare hemmeligheter de er betrodd i stillings medfør.

Virksomheten betrakter taushetsbrudd som tjenesteforsømmelse eller brudd på avtale med virksomheten. Taushetsbrudd kan få følger for ansettelses- eller avtaleforhold.

Erklæring

Undertegnede er kjent med den lovpålagte taushetsplikt som gjelder, herunder hvilke opplysninger som er omfattet av taushetsplikten og at taushetsbrudd kan medføre straffeansvar. Undertegnede er videre kjent med at i <Virksomhet> betraktes taushetsbrudd som tjenesteforsømmelse/brudd på avtale med virksomheten.

Dato	Avdeling/virksomhet	
Fødselsdato	Signatur	Navn med blokkbokstaver
Godkjent av	**Erik Magne Hansen – Administrerende Direktør Helse Vest IKT AS**	

Oversikt over aktuelle lover

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

§ 21 Hovedregel om taushetsplikt

Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell.

§ 21a. Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte opplysninger som nevnt i § 21 uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.

§25 Opplysninger til samarbeidende personell

Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp. For elektronisk tilgang til helseopplysninger på tvers av virksomheter gjelder helseregisterloven § 13 tredje og fjerde ledd.

Taushetsplikt etter § 21 er heller ikke til hinder for at personell som bistår med elektronisk bearbeiding av opplysningene, eller som bistår med service og vedlikehold av utstyr, får tilgang til opplysninger når slik bistand er nødvendig for å oppfylle lovbestemte krav til dokumentasjon.

Personell som nevnt i første og andre ledd har samme taushetsplikt som helsepersonell.

§26 Opplysninger til virksomhetens ledelse og til administrative systemer

Den som yter helsehjelp, kan gi opplysninger til virksomhetens ledelse når dette er nødvendig for å kunne gi helsehjelp, eller for internkontroll og kvalitetssikring av tjenesten, Opplysningene skal så langt det er mulig, gis uten individualiserende kjennetegn.

Den som yter helsehjelp, skal uten hinder av taushetsplikten i § 21 gi vedkommende virksomhets pasientadministrasjon pasientens personnummer og opplysninger om diagnose, eventuelle hjelpebehov, tjenestetilbud, innskrivnings- og utskrivningsdato samt relevante administrative data.

Reglene om taushetsplikt gjelder tilsvarende for personell i pasientadministrasjonen.

§ 45. Utlevering av og tilgang til journal og journalopplysninger

Med mindre pasienten motsetter seg det, skal helsepersonell som skal yte eller yter helsehjelp til pasient etter denne lov, gis nødvendige og relevante helseopplysninger i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte. For elektronisk tilgang til helseopplysninger på tvers av virksomheter gjelder helseregisterloven § 13 tredje og fjerde ledd. Det skal fremgå av journalen at annet helsepersonell er gitt helseopplysninger.

Helseopplysninger som nevnt i første ledd kan gis av den databehandlingsansvarlige for opplysningene eller det helsepersonell som har dokumentert opplysningene, jf. § 39.

Departementet kan i forskrift gi nærmere bestemmelser til utfylling av første ledd, og kan herunder bestemme at annet helsepersonell kan gis tilgang til journalen også i de tilfeller som faller utenfor første ledd.

§ 67 Straff

Den som forsettlig eller grovt uaktsomt overtrer eller medvirker til overtredelse av bestemmelser i loven eller i medhold av den, straffes med bøter eller fengsel i inntil tre måneder.

Offentlig påtale finner sted hvis allmenne hensyn krever det eller etter begjæring fra Statens helsetilsyn.

Lov av 2. juli 1999 nr. 61, Lov om spesialisthelsetjeneste (spesialisthelsetjenesteloven)

§ 6-1 Taushetsplikt

Enhver som utfører tjeneste eller arbeid for helseinstitusjon som omfattes av denne loven, har taushetsplikt etter forvaltningsloven §§ 13 til 13 e.

Taushetsplikten gjelder også pasientens fødested, fødselsdato, personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Opplysning om en pasients oppholdssted kan likevel gis når det er klart at det ikke vil skade tilliten til helseinstitusjonen.

Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13 b nr. 5 og 6 kan bare gis når dette er nødvendig for å bidra til løsning av oppgaver etter denne loven, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

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

§ 13a. Forbud mot urettmessig tilegnelse av helseopplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne

loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.
§ 15 Taushetsplikt
Enhver som behandler helseopplysninger etter denne lov, har taushetsplikt etter forvaltningsloven §§ 13 til 13e og helsepersonelloven.
Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, pseudonym, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted.
Opplysninger til andre forvaltningsorganer etter forvaltningsloven § 13 b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter loven her, eller for å forebygge vesentlig fare for liv eller alvorlig skade for noens helse.

Utarbeidet av		**Utvalg for regional IKT-sikkerhet**
Godkjent av		**Erik Magne Hansen – Administrerende Direktør Helse Vest IKT AS**
Ref dok	**602**	**Taushetsplikt – rutine**