HELSE VEST IKT

Taushetserklæring

Bakgrunn
Taushetsplikten 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 pasienten skal ha tillit til helsetjenesten og at pasienten skal oppsøke helsetjeneste for å 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, opplysninger 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.

For mer informasjon om taushetsplikt i helse- og omsorgstjenesten se:
https://helsedirektoratet.no/taushetsplikt/taushetsplikt-i-helse-og-omsorgstjenesten

Lovkrav
Det følgende beskriver lovpålagt taushetsplikt

- 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 pasientjournalloven § 15 har alle som behandler helseopplysninger etter denne lov, taushetsplikt
- i henhold til helseregisterloven § 17 har alle som behandler helseopplysninger etter denne loven, taushetsplikt etter helsepersonelloven §§ 21
- i henhold til pasient- og brukerrettighetsloven § 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

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

I henhold til straffeloven §§ 209, 210 er det straffbart å krenke taushetsplikt pålagt i henhold til lovbestemmelse eller gyldig instruks.

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 Helse Vest IKT betraktes taushetsbrudd som tjenesteforsømmelse/brudd på avtale med virksomheten.

Fødselsdato	Signatur	Navn med blokkbokstaver
DD.MM.ÅÅÅÅ		NN

HELSE VEST IKT

Taushetserklæring – Vedlegg til skjema

Oversikt over aktuelle lover

Lov av 2. juli 1999 nr. 64 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. 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. Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å ivareta behovene til pasientens mindreårige barn eller mindreårige søsken, jf. § 10 a.

Personell som nevnt i første, andre og tredje 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. Ved samarbeid om behandlingsrettede helseregistre etter pasientjournalloven § 9 kan slike opplysninger også gis til ledelsen i samarbeidende virksomhet. 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. 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 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 20. juni 2014 om helseregistre og behandling av helseopplysninger (helseregisterloven)

§ 17 Taushetsplikt

Enhver som behandler helseopplysninger etter denne loven, har taushetsplikt etter helsepersonelloven §§21 flg. Andre som får samme adgang eller kjennskap til helsepersonellopplysninger fra helseregistre, har samme taushetsplikt.

§ 18.Forbud mot urettmessig tilegnelse av taushetsbelagte helseopplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven, uten særskilt hjemmel i lov eller forskrift.

HELSE VEST IKT

Taushetserklæring – Vedlegg til skjema

Lov av 2. juli 1999 nr. 63 om pasient- og brukerrettigheter (pasientrettighetsloven)
§ 3-6 Rett til vern mot spredning av opplysninger
Opplysninger om legems- og sykdomsforhold samt andre personlige opplysninger skal behandles i samsvar med gjeldende bestemmelser om taushetsplikt. Opplysningene skal behandles med varsomhet og respekt for integriteten til den opplysningene gjelder. Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker. Dersom helsepersonell tilgjengeliggjør opplysninger som er undergitt lovbestemt opplysningsplikt, skal den opplysningene gjelder, så langt forholdene tilsier det, informeres om at opplysningene er gitt og hvilke opplysninger det dreier seg om.

Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven)
§ 13 Taushetsplikt
Enhver som utfører tjenester eller arbeid for et forvaltningsorgan, plikter å hindre at andre får adgang eller kjennskap til det han i forbindelse med tjenesten eller arbeidet får vite om:
1) noens personlige forhold
2) tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den som opplysningene angår

Som personlige forhold regnes ikke fødested, fødselsdato og personnummer, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted, med mindre slike opplysninger røper et klientforhold eller andre forhold som må anses som personlige. Kongen kan ellers gi nærmere forskrifter om hvilke opplysninger som skal regnes som personlige, om hvilke organer som kan gi privatpersoner opplysninger som nevnt i punktumet foran og opplysninger om den enkeltes status for øvrig, samt om vilkårene for slike opplysninger. Taushetsplikten gjelder også etter at vedkommende har avsluttet tjenesten eller arbeidet. Han kan heller ikke utnytte opplysninger som nevnt i denne paragraf i egen virksomhet eller i tjeneste eller arbeid for andre.

Lov 20. mai 2005 nr. 28 om straff (straffelova)
§ 209 Brudd på taushetsplikt
Med bot eller fengsel inntil 1 år straffes den som røper opplysning som han har taushetsplikt om i henhold til lovbestemmelse eller forskrift, eller utnytter en slik opplysning med forsett om å skaffe seg eller andre en uberettiget vinning.
Første ledd gjelder tilsvarende ved brudd på taushetsplikt som følger av gyldig instruks for tjeneste eller arbeid for statlig eller kommunalt organ. For den som arbeider eller utfører tjeneste for et statlig eller kommunalt organ, rammer første og annet ledd også brudd på taushetsplikt etter at tjenesten eller arbeidet er avsluttet.

Grovt uaktsom overtredelse straffes på samme måte.
Medvirkning er ikke straffbar.

§ 210 Grovt brudd på taushetsplikt
Grovt brudd på taushetsplikt straffes med fengsel inntil 3 år.
Ved avgjørelsen av om taushetsbruddet er grovt skal det særlig legges vekt på om gjerningspersonen har hatt forsett om uberettiget vinning og om handlingen har ført til tap eller fare for tap for noen.

HELSE VEST IKT

Sikkerhetsinstruks

Hensikt
Personvernforordningen og helselovgivningen stiller strenge krav til behandling av personopplysninger. Dette er for det første begrunnet i virksomhetenes plikt til å sikre opplysningers tilgjengelig og integritet for å kunne gi livsviktig helsehjelp. Vi skal verne om personopplysningene vi behandler. I tillegg har alle som benytter seg av tjenestene som virksomhetene yter, rett til å stole på at personopplysninger om han/henne blir behandlet fortrolig (konfidensialitet) og er sikret mot at personell som ikke er autorisert får innsyn i disse opplysningene.

Omfang og målgruppe
Alle ansatte er omfattet av denne instruksen. IKT-sikkerhetsinstruksen gjelder for alle ansatte, vikarer, studenter, leverandører, konsulenter og andre som gis tilgang til virksomhetens informasjonssystem (omtalt som brukere i instruksen). Kravene i denne instruksen er minimumskrav som må ivaretas av alle for å sikre at det ikke skjer brudd på lovkravene. IKT-sikkerhetsinstruksen er et kortfattet utdrag av styringssystemet for informasjonssikkerhet og personvern som gjelder for virksomheten.

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. Dette er obligatorisk for ansatte i Helse Vest IKT, og skal være bestått ved tiltredelse og repeteres minst hvert tredje år. IKT-sikkerhetsinstruksen med de bestemmelser den inneholder, er en del av de vilkår du har forpliktet deg til.

Ansvar

Utforming/vedlikehold av rutinen:	Utvalg for regional IKT-sikkerhet
Utførelse:	Daglig leder skal beslutte og signere IKT-sikkerhetsinstruksen
Etterlevelse:	Alle brukere av IKT-systemene

Brudd på de rutiner og bestemmelser som IKT-sikkerhetsinstruksen inneholder innebærer brudd på dine forpliktelser overfor virksomheten. Dette kan derfor få personalmessige konsekvenser eller konsekvenser for kontraktsforholdet med virksomheten.

Sikkerhetsregler

Generelt aktsomhetskrav

Det faktum at du i kraft av ditt ansettelses- eller kontraktsforhold til virksomheten kan benytte virksomhetens informasjonssystem, forplikter deg spesielt til å opptre med aktsomhet og god etikk. Den enkelte skal derfor ha et reflektert forhold til deling og lagring av informasjon. Vær også bevisst rundt 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.

Ivaretakelse av taushetsplikten - tilgang til dokumenter
Du som bruker av virksomhetens informasjonssystem plikter aktivt å hindre at uvedkommende får tilgang til dokumenter eller andre medier som inneholder personopplysninger som er underlagt taushetsplikt. Brudd på taushetsplikten kan medføre både personalmessige konsekvenser og/eller straffeansvar.

Helseopplysninger
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, jamfør helsepersonellovens § 21 a og pasientjournallovens § 16.

Aktsomhet for å hindre innsyn fra andre/uvedkommende
I arbeid med helse- og personopplysninger skal det iverksettes tiltak for å hindre innsyn fra personer som ikke har tjenstlig behov for å se informasjonen som behandles.

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 rutine i styringssystemet for informasjonssikkerhet og personvern.

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

Brukere 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.

Privat bruk av informasjonssystemet
Utgangspunktet er at virksomhetens informasjonssystem kun skal brukes til virksomhetsrelaterte oppgaver. Det tillates imidlertid begrenset bruk av informasjonssystemet til private formål innenfor samme regler som ellers gjelder.

Private dokumenter og e-post i moderat omfang kan lagres i informasjonssystemet. Dette bør lagres på område som er merket "privat".

Det gjøres oppmerksom på at arbeidsgiver under gitte forutsetninger har mulighet for innsyn i dokumenter og e-postkonto. Dette er omtalt i «G28 - Instruks for innsyn i e-post, personlig område mv».

Pålogging og avlogging, brukernavn, passord og låsing av arbeidsstasjon
- Passordet (og eventuelt brikke/kort for fjernaksess) er brukerens 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 (ctrl+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 Helse Vest IKT.

Lagring
- Helse- og personopplysninger (inkl. avidentifiserte personopplysninger) skal ikke lagres på fellesområder, flyttbart lagringsmedium eller brukerens hjemmeområde uten tilstrekkelig sikring av tilgang. Hva som er tilstrekkelig sikring må avklares med IKT-sikkerhetsleder.
- Det er ikke tillatt å benytte løsninger der det ikke kan garanteres at data lagres sikkert på et angitt sted. Lagring utenfor virksomhetens kontroll, herunder skytjenester skal betraktes som usikkert lagringssted og skal ikke benyttes, med mindre dette er risikovurdert og eksplisitt tillatt.
- Kvalitetssikringsdata og forskningsdata skal lagres på dedikerte områder (tilpasses den enkelte virksomhet).

Forsendelse
- Helse- og personopplysninger skal ikke sendes via vanlig e-post, telefaks, sms eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. Det er heller ikke lov å sende 11-siffret fødselsnummer på denne måten.
- Dokumenter og lagringsmedia med 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 personopplysningene, og autentisert på tilstrekkelig nivå.

Håndtering av dokumenter
- Utskrift skal skrives ut til rett skriver og utskrifter skal hentes umiddelbart, dersom ikke sikker utskrift benyttes.
- Utskrifter med personopplysninger skal makuleres når formålet med utskriften er ivaretatt
- Saksdokumenter skal arkiveres iht gjeldende regler
- Brukere 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.
- Brukere som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutinene i virksomheten.

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.) i virksomhetens informasjonssystem, med mindre dette utføres som en del av jobbrelatert virksomhet. Slik nedlasting 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

- Særlige kategorier av personopplysninger [1] skal aldri sendes i usikret e-post.
- 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 opplysninger som ikke skal ut av virksomheten. 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.
- Privat eller annen virksomhets e-postadresse skal ikke brukes når aktivitet blir utført på vegne av Helse Vest IKT.
- 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 kalender

- Mange brukere har delt kalender. Dette gjør at opplysninger som legges i møtekalenderen blir tilgjengelig for hele selskapet og andre virksomheter i Helse Vest.
- Møtekalenderen skal ikke inneholde særlige kategorier av personopplysninger, for eksempel timebok for navngitte 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 medarbeideres 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, uten godkjenning, 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 aktiviteter og observerte sikkerhetsbrudd skal så raskt som mulig meldes som avvik til nærmeste leder og/eller IKT-sikkerhetsleder. Hendelser knyttet til at denne IKT-sikkerhetsinstruksen ikke følges, vurderes som sikkerhetsbrudd. Brudd på IKT-sikkerhetsinstruksen ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for informasjonssikkerhet, og vil bli behandlet som personalsak. Alvorlige brudd på reglene i IKT-sikkerhetsinstruksen vil få konsekvenser for brukerens arbeidsforhold og kan resultere i strafferettslige reaksjoner.

Hvis du oppdager informasjon på avveie eller har mistanke om at noen har snoket i dine eller andres personopplysninger, må det meldes fra til nærmeste leder og/eller sikkerhetsleder. Det er bedre å varsle en gang for mye enn en gang for lite. Sikkerhetsavvik meldes i avvikssystemet.

Du kan ved varsling kontakte IKT-sikkerhetsleder, personvernombud, tillitsvalgte eller verneombud, og be om at din identitet ikke avsløres videre i virksomheten.

Tap eller tyveri av utstyr

Tap eller tyveri av utstyr som er eid av virksomheter i Helse Vest eller er driftet av Helse Vest IKT skal meldes til døgnbemannet Kundesenter i Helse Vest IKT (55 97 65 40) og nærmeste leder. Det er viktig at dette varsles umiddelbart, slik at det kan iverksettes tiltak.

[1] Med særlige kategorier av personopplysninger menes: rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.