HELSE SØR-ØST

Sikkerhetsinstruks

Signerbar versjon

Versjonsnummer	**Dato**	**Godkjent av**
1.0	22.12.2016	
1.1	23.10.2018	
1.2	3.9.2019	Øyvind Grinde

1 Hensikt og omfang

Denne instruksen etablerer et felles sett med sikkerhetsregler for alle medarbeidere ved bruk av virksomhetens IKT-løsninger (informasjonssystemer) og elektronisk produserte og lagrede opplysninger. Dette omfatter både om opplysningene er direkte identifiserbare ved navn, fødselsnummer, pasient-ID, eller indirekte identifiserbare personopplysninger hvor et referansenummer gir koblingen til navn og andre direkte kjennetegn, og ellers annen informasjon som krever beskyttelse.

Instruksen er en del av virksomhetens styringssystem for informasjonssikkerhet, slik som beskrevet i pasientjournalloven, helseregisterloven, helseforskningsloven, personopplysningsloven med flere.

Denne sikkerhetsinstruksen gjelder for alle medarbeidere, leverandører, konsulenter, vikarer og andre som gis tilgang til virksomhetens elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer, inkludert, men ikke begrenset til, stasjonært og bærbart utstyr, nettverk, pasientsystemer og andre behandlingsrettede helseregistre, programvare, medisinsk-teknisk utstyr m.m.

Instruksen skal være lest og gjennomgått før det gis tilganger til virksomhetens elektroniske tjenester.

Sikkerhetsinstruksen suppleres spesielt av følgende dokumenter:

- Bruk av e-post og telefaks
- Bruk av e-post og telefaks for kommunikasjon med og om pasienter
- Bruk av mobiltelefon
- Fellesregional passordpolicy for helseforetakene i Helse Sør-Øst
- Grunnlag for oppslag i journal
- Lagring, arkivering og sletting av helse- og personopplysninger
- Bruk av databehandler - Lagring av personopplysninger hos annen juridisk enhet
- Anonymisering av helse- og personopplysninger

2 Ansvar

- Virksomheten skal sørge for at instruksen er lett tilgjengelig for alle ledere og medarbeidere i virksomheten.
- Enhver leder er ansvarlig for å informere om denne instruks og gjøre den tilgjengelig for sine medarbeidere.
- Brukerne, medarbeidere, midlertidig ansatte, innleide og andre som skal gis tilgang til virksomhetens IKT-system, er selv ansvarlig for å gjøre seg kjent med og følge reglene i denne instruks. Virksomheten forutsettes å ha nødvendig instruksjonsmyndighet på den som skal gis tilgang til virksomhetens IKT-system.
- Ved ansettelse har virksomheten nødvendig instruksjonsmyndighet. Tilsvarende må også sikres ved all innleie av personell som vil kunne komme i berøring med personopplysninger og virksomhetens IKT-system. Innleie kan gjøres så sant virksomheten selv har et behov og eier formålet med innleie.

3 Fremgangsmåte

3.1 Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger

Som medarbeider vil du kunne ha teknisk tilgang til mer opplysninger enn du trenger for å utføre ditt arbeid. Det er forbudt å søke etter pasientopplysninger og annen taushetsbelagt informasjon, f.eks. informasjon om medarbeidere, familiemedlemmer og kjente personer, uten at dette er nødvendig for ditt arbeid (tjenstlig behov), at du har grunnlag for å søke opp informasjonen og at taushetsplikten herunder er ivaretatt. Brudd på taushetsplikt kan få konsekvenser for arbeidsforholdet og vil kunne medføre straffansvar.

3.2 Pålogging og avlogging, brukernavn, passord og skjermsparer

Passordet (og eventuelt brikke/kort for tilgang/passordkalkulator/og tilsvarende) er den ansattes personlige nøkkel til virksomhetens datasystem og skal ikke deles med andre. Den enkelte ansatte/innleide har et personlig ansvar for å sørge for at andre ikke får tilgang til passord, kort og pin-kode, passordkalkulator og pålogget tilgang.

- Det er ikke tillatt å bruke en annens brukertilgang/passord.
- Passord skal ikke skrives ned.
- Ved mistanke om at passordet er blitt kjent av andre, skal passordet byttes uten ugrunnet opphold.
- Passordbeskyttet skjermsparer skal benyttes og/eller kontordør låses når arbeidsplassen/maskinen forlates i kortere perioder.
- Brukeren skal alltid logge ut sin personlige tilgang før maskinen overlates til andre.

Mer informasjon om grunnlag for oppslag i journal, finnes i dokumentet Grunnlag for oppslag i journal.

Mer informasjon om regler for passordpolicy, finnes i dokumentet Fellesregional passordpolicy for helseforetakene i Helse Sør-Øst.

3.3 Logging

All bruk av virksomhetens informasjonssystemer kan bli loggført. Loggene brukes til administrasjon, for å følge opp virksomhetens retningslinjer for informasjonssikkerhet og for lovpålagt kontroll av oppslag i behandlingsrettede helseregistre (eks. DIPS).

Mer informasjon ligger i dokumentet Loggføring av aktivitet og kontroll av logger.

3.4 Om privat bruk

Virksomhetens informasjonssystemer er beregnet for jobbrelaterte formål og skal som den klare hovedregel benyttes til dette. Noe privat bruk tillates, men privat bruk skal ikke gå ut over virksomhetsrelaterte oppgaver og funksjoner. Privat bruk som krever stor lagringsplass er ikke tillatt. Følgende er gjeldende:

- 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. Privat e-post som lagres skal legges i mappe merket "Privat".

- Mindre mengder private filer kan lagres i egen katalog på personlig område i sykehusnettet, forutsatt at katalogen er merket "privat". Av plass og kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres i sykehusnettet.

Ansatte skal ikke bruke sin e-postadresse ved foretaket når de opptrer som privatpersoner på internett, for eksempel på sosiale nettsteder.

3.5 Eierskap til programvaren

Sykehuspartner HF eier all programvare som er installert på maskinen ved utlevering eller ved senere oppdateringer av driftsenheten, og virksomheten disponerer utstyr og programvare. Programvare kan normalt ikke installeres av bruker, med mindre dette er uttrykkelig godkjent. Bruker skal av sikkerhetsgrunner ikke endre oppsett på datamaskiner eller bevisst forsøke å omgå logiske eller tekniske sikringstiltak. Handlinger i strid med dette vil kunne påtales av arbeidsgiver. Sykehuspartner HF kan fjerne programvare hvis denne påvirker drift av IKT.

3.6 Eierskap til data/informasjon

Virksomheten eier all virksomhetsrelatert informasjon. Dette gjelder alle personopplysninger, forskningsdata og administrative opplysninger. Bruk av slik informasjon utover virksomhetens behov er ikke tillatt. Bruk av andre offentlige registre som virksomheten har tilgang til, skal skje i tråd med de vilkår som er stilt for bruken.

3.7 Innsynsrett

Virksomheten har ved behov rett til innsyn i all informasjon lagret i informasjonssystemer. Innsynsretten har begrensninger og følger egne prosedyrer.

3.8 IKT-utstyr, inkludert medisinsk teknisk utstyr

Det er ikke tillatt å benytte privat utstyr av noe slag i virksomhetens nett. Dette inkluderer, men er ikke begrenset til, nettbrett, mobiltelefon, kamera, minnekort og minnepinne.

Det er kun tillatt å benytte utstyr levert og installert av Sykehuspartner HF. Unntak fra dette skal være skriftlig avtalt med Sykehuspartner HF. Unntaket forutsetter sikkerhetsmessig risikovurdering og hvor det er konkludert med akseptabelt risikonivå av egen og Sykehuspartner HFs informasjonssikkerhetsleder.

Installasjon av alt utstyr og programvare skal gjøres av medarbeidere fra Sykehuspartner HF, eller av de som av Sykehuspartner HF er utpekt til å gjøre denne jobben. Unntak fra dette skal være skriftlig avtalt med Sykehuspartner HF, etter å ha vært gjenstand for sikkerhetsmessig risikovurdering som er konkludert med akseptabelt risikonivå av egen og Sykehuspartner HFs informasjonssikkerhetsleder.

Bruk av annen programvare eller maskinvare utenom det som virksomheten tilbyr som standard programvare, må godkjennes i henhold til foretakets prosedyrer for anskaffelser, IKT og informasjonssikkerhet.

Eksterne konsulenter og vikarer skal ikke koble til egne PC-er i virksomhetens nett, men få tildelt maskin av virksomheten. Særskilte behov for egne PC-er skal avklares med informasjonssikkerhetsleder. Det skal ikke tilkobles separate eksterne forbindelser til virksomhetens nett (for eksempel via ekstra nettverkskort, trådløst forbindelse/aksesspunkt, modem og lignende). Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

IKT-utstyr skal ikke flyttes eller lånes til andre rom/lokaler uten avtale med Sykehuspartner HF. Dataskjermer skal plasseres slik at det ikke er innsyn for uvedkommende.

Medarbeidere som slutter eller går ut i permisjon, skal levere alt utlevert IKT-utstyr (mobil PC, mobil-telefon, nettbrett, sertifikat, brikke for fjerntilgang/passordkalkulator osv) og programvarelisenser til leder eller den leder beslutter, dersom ikke annet er avtalt.

Ta kontakt med Sykehuspartner HF dersom du har mistanke om feil eller problemer med tilgang til systemer, tjenester eller informasjon

Alt arbeid som skal utføres av eksternt personell på virksomhetens systemer og utstyr, skal bestilles gjennom Sykehuspartner HF. Se beskrivelse av bruk av leverandører i dokumentet Sikkerhetsstrategi.

3.9 Kassering/Håndtering av utstyr og lagringsmedier

Harddisker, minnepinner, minnekort, utstyr som inneholder harddisker og andre elektroniske lagringsmedier, skal leveres til Sykehuspartner HF for forsvarlig destruksjon. Lagringsmedia som CD, DVD, disketter osv. som inneholder personopplysninger (inkluderte kodede), eller media med andre opplysninger, skal leveres til Sykehuspartner HF for destruksjon. Pr. tid gjøres dette gjennom skjema i Min Sykehuspartner.

3.10 Lagring og behandling av personopplysninger

Det er som hovedregel kun tillatt å behandle sensitive personopplysninger i godkjente fagapplikasjoner i virksomhetens nettverk. Lagring og behandling av personopplysninger utenfor etablerte fagsystemer krever avklart lovlig grunnlag (samtykke, hjemmel i lov, godkjenning fra Personvernombudet, informasjonssikkerhetsleder eller REK, dispensasjon mm.) og med informasjonssikkerhet avklart og i tråd med lov og Norm for informasjonssikkerhet. All behandling av personopplysninger skal være risikovurdert og godkjent før databehandling starter.

Bruk av ikke-fagsystemer som Word, Excel, SPSS mm. for behandling av personopplysninger skal kun benytte forhåndsgodkjente dedikerte filområder i henhold til virksomhetens prosedyrer.

Forskningsdata skal behandles i henhold til prosedyrer og rutiner for forskning.
Kvalitetsregistre skal behandles i henhold til prosedyrer og rutiner for kvalitetsregistre.

Når lagringsmedia eller dokumenter med registre eller sensitive personopplysninger ikke er under direkte oppsyn, skal de oppbevares nedlåst eller sikres på annen måte slik at uvedkommende ikke får tilgang.

Mer informasjon ligger i dokumentet Lagring, arkivering og sletting av helse- og personopplysninger.

3.11 Kommunikasjon

Sensitive personopplysninger skal ikke sendes på åpen e-post, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. Risikovurdering skal gjennomføres og godkjennes av informasjonssikkerhetsleder. Ved tvil skal informasjonssikkerhetsleder kontaktes for informasjon om godkjente elektroniske forsendelsesmetoder

Dokumenter med sensitive personopplysninger skal alltid forsendes i gjenlimt konvolutt/forseglet innpakning og lagringsmedia som inneholder sensitive personopplysninger skal som hovedregel

krypteres før forsendelse. Unntak fra disse føringene må avklares og godkjennes av virksomhetens informasjonssikkerhetsleder.

Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for opplysningene. Sensitive personopplysninger kan kun utleveres dersom det foreligger nødvendig lovlig grunnlag (hjemmel). Utlevering uten slik hjemmel vil være et lovbrudd og et alvorlig brudd på retningslinjene for informasjonssikkerhet.

Det skal utvises aktsomhet ved mottak av e-post. Vedlegg kan inneholde virus. Ved tvil skal avsender eller Sykehuspartner HF kontaktes eller e-postmeldingen slettes. Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.

Den som mottar personopplysninger man ikke er autorisert for å behandle, skal straks gjøre avsender oppmerksom på dette og på eget tiltak tilbakelevere eller slette opplysningene. Den som mottar sensitive personopplysninger over e-post, skal gjøre avsender oppmerksom på at dette er brudd med Sikkerhetsinstruks, melde avvik i virksomhetens avvikssystem, og slette opplysningene fra e-postsystemet. Dersom man er autorisert for å motta opplysningene, skal de flyttes over på godkjent lagringsområde og så slettes fra e-postsystemet. Sletting av e-post innebærer at "Papirkurven"/"Slettede elementer" også er tømt.

Mer informasjon om e-post og telefaks finnes i dokumentet Bruk av e-post og telefaks.

3.12 Bruk av mobiltelefon/nettbrett

Mobiltelefon/nettbrett med synkronisering krever minimum registrering og godkjenning fra informasjonssikkerhetsleder, inkludert gjennomført og akseptert risikovurdering.

Mobiltelefonen skal:

- Kun synkronisere e-postens innbokser, kalenderen, notater, kontaktpersoner og oppgaver
- Ha aktivisert automatisk tastelås
- Ha aktivisert kodelås for åpning av telefonen når tastelåsen er aktiv

Det er ikke tillatt å ta bilder av pasienter eller pårørende med mobiltelefon, eller å lagre andre sensitive opplysninger på denne.

Mer informasjon om dette finnes i dokumentet Bruk av mobiltelefon.

3.13 Makulering/sletting av dokumenter

Dokumenter med personopplysninger som skal avhendes, skal makuleres ved 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.

3.14 Opphør av arbeidsforhold

Medarbeidere som slutter, skal rydde i egne filområder og e-post og sikre at all relevant informasjon blir lagret på avdelingens filområde. Arkivverdig informasjon skal lagres i virksomhetens sak/arkivsystem.

Medarbeidere som slutter, skal makulere eller avlevere egne dokumenter som beskrevet over.

E-post og personlig filområde vil bli slettet omgående ved endt arbeidsforhold.

3.15 Sikkerhetskopiering

Det tas regelmessige sikkerhetskopier av all informasjon lagret i virksomhetens fagapplikasjoner og av virksomhetens filservere. For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på eller eventuelt systematisk kopieres til virksomhetens fagapplikasjoner eller filservere.

Ved behov for rekonstruksjon av informasjon på sykehusnettet, kontakt Sykehuspartner HF.

Det blir ikke tatt sikkerhetskopier av informasjon lagret på lokale lagringsmedier som for eksempel minnepinner, eksterne harddisker eller lokal harddisk på ordinære PC-er i sykehusnettet. Informasjon på lokal harddisk på ordinære PC-er i sykehusnettet kan uten varsel bli slettet av Sykehuspartner HF.

3.16 Internett

Medarbeiderens oppslag på Internett kan spores tilbake til virksomheten og den PC/brukeridentitet som var i bruk da oppslaget ble gjort. Internett skal kun benyttes til lovlig aktivitet 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 laste ned og installere programvare på virksomhetens IKT-utstyr uten godkjenning fra informasjonssikkerhetsleder.

Bruk av fildelingstjenester er ikke tillatt.

For bruk av sosiale medier, se virksomhetens egne retningslinjer. Les ogsåmer om dette her: https://www.difi.no/fagomrader-og-tjenester/klart-sprak-og-brukerretting/sosiale-medier

3.17 Kartlegging og utnyttelse av systemsvakheter

Medarbeideren 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.

Ved mistanke om svakheter, sårbarheter, feil eller mangler i informasjonssystemer, skal dette meldes Sykehuspartner HF.

3.18 Fysisk adgang

Alle medarbeidere, herunder innleide og andre som utfører arbeid på virksomhetens lokasjoner, skal bære gyldig ID-kort synlig og følge virksomhetens retningslinjer for fysisk adgang.

Den som mottar besøkende eller leverandører, er ansvarlig for at disse ikke oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av en medarbeider. Den enkelte medarbeider skal hindre at uvedkommende får adgang til datamaskiner, skrivere, dokumenter, flyttbare lagringsmedier og annet utstyr som kan gi tilgang til taushetsbelagte opplysninger eller annen beskyttelsesverdig informasjon og kritiske IKT-tjenester. Uvedkommen adgang skal varsles iht. foretakets rutiner.

3.19 Avvikshåndtering

Alle medarbeidere skal ved mistenkelige hendelser og observerte sikkerhetsbrudd, registrere avviket inn i virksomhetens avvikssystem i henhold til etablerte prosedyrer for avvikshåndtering, eller rapporteres til nærmeste leder, eller til informasjonssikkerhetsleder.

4 Definisjoner

Se eget dokumentet Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet

5 Avvik eller dissens

Avvik på denne instruks meldes i virksomhetens avvikssystem. Informasjonssikkerhetsleder og/eller personvernombud skal varsles.

6 Referanser

- Sikkerhetsregulerende lovverk gjeldende for helseforetaksgruppen
- Overordnede prinsipper for regionalt styringssystem for informasjonssikkerhet

7 Signatur

Jeg har lest og forstått denne sikkerhetsinstruksen og forplikter meg til å overholde den.

Fornavn - Etternavn: _____

Brukernavn: _____

Stilling: _____

Virksomhet: _____

_____ _____

Sted/dato **Signatur**