



Sikkerhetsinstruks

1	Hensikt og omfang	4
2	Ansvarlige og dokumenter.....	4
3	Fremgangsmåte	4
3.1	Taushetsbelagte opplysninger.....	4
3.2	Pålogging og avlogging, brukernavn, passord og skjermsparer	5
3.3	Logging	5
3.4	Om privat bruk.....	5
3.5	Bruk av Sykehuspartner-brukerkonto for eksterne konsulenter.....	6
3.6	Eierskap til programvare	6
3.7	Eierskap til data/informasjon	6
3.8	Innsynsrett.....	6
3.9	IKT-utstyr, inkludert medisinsk-teknisk utstyr.....	6
3.10	Kassering/håndtering av utstyr og lagringsmedier	7
3.11	Lagring og behandling av personopplysninger.....	7
3.12	Kommunikasjon	8
3.13	Bruk av mobiltelefon/nettbrett.....	8
3.14	Makulering/sletting av dokumenter	8
3.15	Opphør av arbeidsforhold	9
3.16	Sikkerhetskopiering.....	9
3.17	Internett	9
3.18	Kartlegging og utnyttelse av systemsvakheter	9
3.19	Fysisk adgang.....	9
3.20	Avvikshåndtering.....	10

Versjon	Dato	Behandling/ending	Godkjent av
1.0	22.12.2016		
1.1	23.10.2018		
1.2	3.9.2019		Øyvind Grinde

1.6	19.8.2021	Oppdatert med informasjon fra taushets- klæring og bruk av Sykehuspartner HF's brukerkonto for eksterne konsulenter. Mindre justeringer i henhold til mål og stra- tegi for informasjonssikkerhet. Tilsluttet i regionalt sikkerhetsfaglig råd.	Øyvind Grinde
-----	-----------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------

1 Hensikt og omfang

Denne instruksjonen 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.

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

Denne sikkerhetsinstruksjonen 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.

Instruksjonen skal være lest og gjennomgått før det gis tilgang til virksomhetens elektroniske tjenester.

2 Ansvarlige og dokumenter

Virksomheten skal sørge for at instruksjonen er lett tilgjengelig for alle ledere og medarbeidere i virksomheten.

Enhver leder er ansvarlig for å informere om denne instruksjonen 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 instruksjonen. Virksomheten forutsettes å ha nødvendig instruksjonsmyndighet over 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 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.

Som medarbeider i Helse Sør-Øst er du kjent med:

- at Helse Sør-Øst forvalter taushetsbelagt informasjon, herunder opplysninger om helse og andre personlige forhold og forretningshemmeligheter.

- At dersom du gjennom utførelse av arbeid/oppdrag/tjeneste i Helse Sør-Øst får kjennskap til taushetsbelagt informasjon, forplikter du deg til ikke å bruke, utlevere eller på annen måte gjøre tilgjengelig denne kunnskap for internt eller eksternt uvedkommende og ikke benytte denne til andre formål enn de oppgaver du er pålagt av helseforetaket.
- at du plikter å gjøre deg kjent med bestemmelsene i Lov om behandlingsmåten i forvaltningssaker 10.2.1967 (forvaltningsloven) § 13, Lov om helseregistre og behandling av helseopplysninger 20.6.2014 nr.43 (helseregisterloven) § 17. Videre forplikter arbeidstaker seg til å overholde arbeidsgivers til enhver tid gjeldende etiske retningslinjer.
- at forsettlig eller uaktsomt brudd på taushetsplikten kan medføre disiplinære sanksjoner, erstatningsansvar og straffeansvar.
- at taushetsplikten gjelder uten tidsbegrensning, med mindre medarbeider løses fra denne plikt av hvert av helseforetakene medarbeider har jobbet for i Helse Sør-Øst.

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 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 sykehusnett, forutsatt at katalogen er merket «privat». Av plass og kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres i sykehusnett.

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

3.5 Bruk av Sykehuspartner-brukerkonto for eksterne konsulenter

Eksterne konsulenter skal kun bruke Sykehuspartner HF's utstyr og e-postadresse til Sykehuspartner-relatert formål, jmfør kapittel 3.7. Dette innebærer at Sykehuspartners informasjon ikke skal sendes til egen virksomhets informasjonssystemer. Dersom det er formålstjenlig kan konsulenter utstyr og e-postadresse brukes, men dette skal begrunnes og godkjennes av oppdragsgiver på forhånd.

3.6 Eierskap til programvare

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 skal normalt ikke installeres av bruker, med mindre dette er uttrykkelig godkjent. Bruker skal av sikkerhetsgrunner ikke endre oppsett på datamaskiner eller forsøke å omgå logiske eller tekniske sikkeringstiltak. Handlinger i strid med dette vil kunne påtales av arbeidsgiver. Sykehuspartner HF kan fjerne programvare hvis denne påvirker drift av IKT.

3.7 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.

3.8 Innsynsrett

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

3.9 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 HF's 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 akseptert i eget helseforetak og i overensstemmelse med Sykehuspartner HF's bruksvilkår.

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 nettkort, trådløst forbindelse/aksesspunkt, modem og lignende). Nettkort 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.

3.10 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.

3.11 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 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](#).

3.12 Kommunikasjon

Sensitive personopplysninger skal ikke sendes på åpen e-post, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. 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 med 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](#).

3.13 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-post, kalenderen, notater, kontakter og oppgaver
- Ha aktivisert automatisk tastelås
- Ha aktivisert lås 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](#).

3.14 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.

3.15 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.

3.16 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 sykehusnett, 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 sykehusnett. Informasjon på lokal harddisk på ordinære PC-er i sykehusnett kan uten varsel bli slettet av Sykehuspartner HF.

3.17 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 også mer om dette her: <https://www.digdir.no/digitalisering-og-samordning/privat-bruk-av-sosiale-medium/1956>

3.18 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.

3.19 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.

3.20 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.