ENDRINGER FRA FORRIGE VERSJON: Presisert rutine for arkivering av signert utgave

KILDE
Dette dokumentet er en forenklet utgave av sikkerhetsinstruksen, opprinnelig basert på HSØ sitt Regionalt ledelsessystem for informasjonssikkerhet, dokument NO-13 v1.2: *«Sikkerhetsinstruks (signatur)»*. Oppdatert etter personopplysningslov av 20. juli 2018.

HENSIKT

Sikre at forenklet sikkerhetsinstruks er kjent for alle som gis tilgang til virksomhetens Sørlandet sykehus (SSHF) sine informasjonssystemer.

MÅLGRUPPE

Alle brukere av SSHF sine informasjonssystemer, både egne ansatte (faste og midlertidige), studenter, hospitanter, innleide og eksternt ansatte som gis tilgang.

ANSVAR

- **Alle brukere** av informasjonssystemer er selv ansvarlig for å gjøre seg kjent med og følge reglene i denne instruksen.
- **Enhver leder** er ansvarlig for å informere om denne instruksen og gjøre den tilgjengelig og kjent for sine medarbeidere i SSHF. Leder med ansvar for å gi elektronisk tilgang eller fysisk adgang til eksternt personell uten et ansettelsesforhold til SSHF, skal påse at instruksen blir signert. Signert kopi sendes til dokumentsenteret, med informasjon om at den skal scannes inn i personalmappe/samlemappe.

Om signatur-delen (siste side)

- For alle ansatte i SSHF som bekrefter å ha lest denne instruksen i SSHF sin Kompetanseportal anses dette som en elektronisk og bindende signering. Det er derfor ikke påkrevet å fysisk signere på siste siden av denne instruksen.
- For alt øvrig personell og eksternt ansatte som innvilges tilgang til SSHF sine systemer skal denne instruksen signeres og leveres til SSHF før tilgang eller adgang gis.

Om taushetsplikten

- Alt helsepersonell har lovpålagt taushetsplikt gjennom Helsepersonelloven kap 5, uavhengig av ansettelsesforhold. Taushetserklæringen skal leses, men det er ikke påkrevet å signere denne.
- Alle offentlige ansatte har lovpålagt taushetsplikt gjennom Forvaltningsloven § 13-13e, jf. Spesialisthelsetjenesteloven § 6-1. Taushetserklæringen skal leses, men det er ikke påkrevet å signere denne. Se utdypende informasjon: Taushetsplikten - informasjon og lover SSHF
- For alt øvrig personell skal leder (se ansvar ovenfor) påse at taushetserklæringen (EK, skjemaet Taushetsplikten - informasjon og signatur SSHF) signeres og oppbevares i tråd med gjeldende rutiner.
- Taushetsplikten gjelder uten tidsbegrensning, med mindre den enkelte løses fra denne plikt av SSHF.

Definisjoner

Se eget dokumentet Kilder og definisjoner for styrende dokumenter for informasjonssikkerhet og personvern

For fullstendig sikkerhetsinstruks, se HSØ Sikkerhetsinstruks

SIKKERHETSINSTRUKS FOR ANSATTE OG ØVRIG PERSONELL

Om privat bruk

Sørlandet sykehus (SSHF) sine informasjonssystemer er beregnet for jobbrelaterte formål og skal som den klare hovedregel kun benyttes til dette. Noe privat bruk tillates, men det skal ikke gå ut over virksomhetsrelaterte oppgaver og funksjoner.

Mindre mengder private filer kan lagres i egen katalog på personlig område i sykehusnettet, forutsatt at katalogen er merket "privat". Privat bruk som krever stor lagringsplass er ikke tillatt.

Du skal ikke bruke din e-postadresse ved SSHF når du opptrer som privatperson.

Pålogging og skjerming av innsyn

Påloggingsinformasjonen er din unike personlige nøkkel til SSHF sine datasystem og skal ikke deles med andre.

Dette betyr at:

- Du skal aktivt hindre at andre får kjennskap til din påloggingsinformasjon
- Det ikke er tillatt å bruke en annens brukertilgang/passord
- Passord skal ikke skrives ned
- Ved mistanke om at passordet er blitt kjent skal passordet byttes umiddelbart
- Du skal aktivt hindre at personer som ikke har tjenstlig behov får tilgang til personopplysninger
- Passordbeskyttet skjermsparer skal benyttes når maskinen forlates
- Kontordør skal låses når arbeidsplassen/maskinen forlates

Forbud mot urettmessig tilegnelse av taushetsbelagte opplysninger

Du vil kunne ha teknisk tilgang til flere personopplysninger enn du trenger for å utføre arbeidet ditt. Det er forbudt å søke etter pasientopplysninger og annen taushetsbelagt informasjon, f.eks. informasjon om medarbeidere, familiemedlemmer og/eller kjente personer, utover det du har tjenstlig behov for å vite og som er innenfor taushetsplikten. Se også avsnitt om taushetsplikten i innledningen til denne instruksen.

Mht brudd på denne bestemmelsen: se avsnittet «brudd på sikkerhetsinstruks» under.

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

Fysisk adgang

Alle som utfører arbeid på SSHF lokasjoner skal bære gyldig ID-kort synlig og følge SSHF sin retningslinje fysisk adgang, se Ordensregler for Sørlandet sykehus HF. Den som mottar besøkende eller leverandører er ansvarlig for at disse ikke oppholder seg i avlåste/avsperrede i deler av SSHF sine lokaler uten følge av en medarbeider.

Den enkelte medarbeider skal hindre at eksterne får adgang til teknisk utstyr eller opplysninger utover tjenstlig behov. Uvedkommen adgang skal varsles iht. foretakets rutiner.

Se for øvrig også avsnittet «Leverandører» under

Logging

All bruk av SSHF sine informasjonssystemer kan bli loggført. Loggene brukes til administrasjon, for å følge opp SSHF sine retningslinjer for informasjonssikkerhet og for lovpålagt kontroll av oppslag i behandlingsrettede helseregistre (for eks. DIPS). Autorisert personell gjennomgår loggene og iverksetter tiltak om nødvendig.

Mer informasjon om dette finner du her: Loggføring av aktivitet og kontroll av logger

Innsynsrett

SSHF kan ha hjemmel til å føre tilsyn i alle informasjonssystemer. Innsynsretten må alltid være formåls- og forholdsmessig og følger egne prosedyrer.

Mer informasjon om dette finner du her: Innsyn i en ansatts hjemmeområde og e-postkonto

Lagring og behandling av personopplysninger

Det er som hovedregel kun tillatt å behandle personopplysninger i godkjente fagsystemer. Behandlingen, herunder all lagring skal skje i henhold til prosedyre: Lagring, arkivering og sletting av helse- og personopplysninger.

All behandling og lagring av helse- og personopplysninger i og utenfor fagsystemer skal godkjennes og dokumenteres i SSHF sin oversikt over *Informasjonssystemer* (modul i Kvalitetsportalen). Se også dokumentet Lagring av data utenfor fagsystemer, evt også «*Prosedyre for lagring av forskningsdata*»

Det er ikke tillatt å benytte privat utstyr til å behandle personopplysninger man får kjennskap til gjennom SSHF.

Makulering/sletting av dokumenter og elektronisk lagret informasjon

Dokumenter med helse- og/eller andre personopplysninger skal ikke etterlates, men skal makuleres ved bruk av makuleringsenhet, avlåste beholdere eller avlåste dedikerte rom for mellomlagring. Se beskrivelse i Avfallsrutiner.

Elektroniske lagringsmedier (harddisker, disketter, minnepinner el. –brikker, CD/DVD ol) med slike opplysninger skal makuleres på forsvarlig måte. Kontakt SSHF sin Informasjonssikkerhetsleder eller Personvernombud for råd om makulering.

Mottak og utlevering av personopplysninger

Du er ansvarlig for at den du oppgir personopplysninger til er riktig mottaker. Dette gjelder både ved utlevering via e-post, brev eller muntlig.
Helseopplysninger eller annen særlig kategori personopplysninger (omtales også som sensitive personopplysninger) skal ikke sendes på åpen e-post, telefaks eller tilsvarende løsninger (se Bruk av e-post, chat, telefaks og SMS for kommunikasjon med og om pasienter), men det må benyttes kryptering ved forsendelse. Ved behov for interne e-poster innen SSHF om pasienter, kan man benytte pasientens unike kode (eks. NPR-ID + journal-ID i DIPS, PARTUS ID og andre), men aldri fullt fødselsnummer (11 siffer) eller andre identifiserende opplysninger.

Spesielt viktig: Du skal utvise aktsomhet ved åpning av e-post. Vedlegg eller lenker kan inneholde virus eller annen skadelig kode. Ved tvil skal avsender eller Sykehuspartner HF kontaktes og e-postmeldingen slettes. Du bør melde til avsender hvis du mottar en åpenbart feil adressert e-post og deretter slette e-posten.

Utlevering av helseopplysninger og andre personopplysninger fra SSHF til eksterne parter krever eget rettslig grunnlag, se mer informasjon her: Utlevering av helseopplysninger.

Internett

Internett skal kun benyttes til lovlig aktivitet og i samsvar med vanlige etiske normer, slik at virksomhetsrelaterte oppgaver og funksjoner, samt opplysninger SSHF behandler, ikke blir skadelidende. Dine oppslag på internett kan spores tilbake til SSHF og den PC/brukeridentitet du brukte da oppslaget ble gjort.

Bruk av fildelingstjenester er ikke tillatt.

Bruk av mobiltelefon

Mobiltelefon med synkronisering krever at mobiltelefonen er kjøpt og eies av helseforetaket, samt at godkjent løsning for dette benyttes. Oppsett av mobiltelefonen følger egne rutiner.

Det er ikke tillatt å ta bilder av pasienter eller pårørende eller å lagre andre sensitive opplysninger på mobiltelefon. Bildedokumentasjon av pasienter må skje i henhold til retningslinjer for dette.

Mer informasjon om bruk av mobiltelefon finnes her: Telefonreglement SSHF - mobiltelefoner og i dokumentet Bruk av mobiltelefoner og annet IKT-utstyr som ikke fullt ut administreres av foretaket.

Videokommunikasjon om eller med pasienter

Det skal kun benyttes godkjente løsninger for ytelse av helsehjelp med lyd og videooverføring og hvor pasienten enten er til stede eller omtales med identifiserende opplysninger.

Når videokommunikasjon brukes i ytelse av helsehjelp skal brukerveiledningen for den aktuelle løsningen følges, herunder:

- Sørge for at de som deltar er entydig identifisert slik det er beskrevet i brukerveiledningen
- Sørge for at ingen uvedkommende ser eller lytter til videosamtalen
- Sikre at videosamtalen er lukket ved avslutning av samtale

Pasientens deltakelse i videokommunikasjonen anses som samtykke. Videokonsultasjoner med pasienter skal foregå fra sykehusets lokaler. Mer informasjon finnes i dokumentet Videokonsultasjon mellom behandler og pasient ved hjelp av Norsk Helsenett

Hjemmekontor og andre former for fjerntilkobling

Utstyret som brukes til hjemmekontor og ved fjerntilkobling skal følge beskrivelsene under neste avsnitt «IKT-utstyr og medisinsk teknisk utstyr».

Brukere av hjemmekontor skal:

- Benytte skjermfilter/innsynsfilter eller påse at plassering av skjerm forhindrer uautorisert innsyn
- Hindre innsyn til personopplysninger eller virksomhetskritisk informasjon
- Påse at PC'en er låst eller avlogget når den forlates
- Sørge for at PC'en ikke brukes av uautoriserte personer (familiemedlemmer eller andre)

IKT-utstyr og medisinsk teknisk utstyr

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

Det er ikke tillatt å benytte privat utstyr til å behandle personopplysninger man får kjennskap til gjennom SSHF. Det er kun tillatt å benytte utstyr og programvare levert og installert av SSHF eller Sykehuspartner. Arbeid via ekstern arbeidsflate er tillatt, fordi man da arbeider på SSHF sin IKT-plattform.

Bruker skal ikke omgå logiske eller tekniske sikringstiltak. Handlinger i strid med dette vil kunne påtales av arbeidsgiver. Sykehuspartner kan fjerne programvare hvis denne påvirker drift av IKT.

Ved mistanke om svakheter, sårbarheter, feil eller mangler i informasjonssystemer, skal dette meldes i Kvalitetsportalen (modul Uønsket hendelse).

Brukere som slutter skal levere tilbake IKT-utstyr som er stilt til personlig disposisjon.

Leverandører

Alt arbeid som skal utføres av eksternt personell på SSHF sine systemer og utstyr skal bestilles gjennom Sykehuspartner HF, Medisinsk teknologisk avdeling eller Teknisk avdeling iht gjeldende rutiner.

Leverandører skal skrive seg inn hos oppdragsansvarlig og få oppdragsbeskrivelse før arbeid på SSHF utstyr startes. Det skal kun benyttes IKT-utstyr som er forhåndsgodkjent av informasjonssikkerhetsleder.

Tilkobling av ikke-godkjent IKT-utstyr, utkopiering av loggfiler som ikke er godkjent og avtalt på forhånd eller andre uautoriserte handlinger skal avviksmeldes i Kvalitetsportalen (modul Uønsket hendelse).

Opphør av arbeidsforhold

Medarbeidere som slutter, skal rydde i egne filområder og e-post.

Medarbeidere som slutter, skal makulere eller avlevere egne dokumenter i henhold til rutinene over.

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

Avvikshåndtering

Brukere skal ved mistenkelige hendelser og observerte sikkerhetsbrudd registrere i Kvalitetsportalen (modul Uønsket hendelse).

Brudd på sikkerhetsinstruks

Brudd på reglene i sikkerhetsinstruksen, herunder taushetsplikt og urettmessig tilegnelse av taushetsbelagte opplysninger, kan få konsekvenser for arbeidsforholdet. Anmeldelse til politiet og melding til tilsynsmyndighetene vil bli vurdert, sistnevnt med tanke på vurdering av autorisasjon.

Informasjonssikkerhetsleder/personvernombud kan benyttes for rådføring.

Spørsmål om innholdet i denne instruksen

Dersom du har spørsmål om innholdet i denne instruksen, eller hvordan du kan eller skal forholde deg til regelverket kan du kontakte din leder, evt foretakets

Informasjonssikkerhetsleder, e-post informasjonssikkerhet@sshf.no

eller Personvernombudet (PVO), e-post personvernombud@sshf.no

SIGNATURDEL

Dette sikkerhetsinstruksen skal signeres av personell som ikke leser/signerer via SSHF sin Kompetanseportal
Leder sender signert kopi til Dokumentsenteret. Merk forsendelsen «for innscanning i personal-/samlemappe».

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

For- og etternavn + f.dato (blokkbokstaver): _____ / f.dato _____

Brukernavn: _____

Stilling: _____

Virksomhet: _____

_____ _____

Sted/dato **Signatur**

_____ **Sted/dato**	_____ **Mottatt av ansvarlig leder / ansvarssted SSHF**

Kryssreferanser

I.2.1.4-4	Videokonsultasjon, registrere (brukerveiledning)
I.6.2.6.2.1.8-1	Avfallsrutiner
I.6.3..-1	Taushetsplikten - informasjon og lover SSHF
I.6.3..-2	Taushetsplikten - informasjon og signatur SSHF
I.6.9.2-2	Bruk av e-post, chat, telefaks og SMS for kommunikasjon med og om pasienter
I.6.9.2-5	Bruk av mobiltelefoner og annet IKT-utstyr som ikke fullt ut administreres av foretaket
I.6.9.2-7	Innsyn i en ansatts hjemmeområde og e-postkonto
I.6.9.2-8	Grunnlag for oppslag i journal
I.6.9.2-9	Lagring, arkivering og sletting av helse- og personopplysninger
I.6.9.2-10	Lagring av data utenfor fagsystemer
I.6.9.2-12	Utlevering av helseopplysninger
I.6.9.3-2	Loggføring av aktivitet og kontroll av logger
I.6.9.4-2	HSØ Sikkerhetsinstruks
I.6.9.4-3	Kilder og definisjoner for styrende dokumenter for informasjonssikkerhet og personvern
I.6.10.3.MTA.2.2-2	Retningslinjer for bruk av mobiltelefoner og annet trådløst utstyr på SSHF
I.6.10.7-2	Telefonreglement SSHF - mobiltelefoner

Eksterne referanser

168 Regionalt ledelsessystem for informasjonssikkerhet

1.16 Forvaltningsloven

1.22 Helsepersonelloven

1.41 Spesialisthelsetjenesteloven