1. Endringer siden forrige versjon

Opprettet som nytt dokument i Oslo universitetssykehus.

Erstatter tidligere tilsvarende dokumenter i hhv Aker, Rikshospitalet og Ullevål, inkludert databrukerkontrakt.

2. Hensikt og omfang

Formålet med denne instruksen er å etablere et felles sett med sikkerhetsregler for alle medarbeidere ved bruk av sykehusets IKT-løsninger og elektronisk produserte opplysninger.
Instruksen er en del av Oslo universitetssykehus' internkontrollsystem, slik som beskrevet i helseregisterloven (hlsregl) og personopplysningsloven (popplyl).

Denne sikkerhetsinstruks gjelder for alle ansatte, leverandører, konsulenter, vikarer og andre som gis tilgang til virksomhetens elektroniske tjenester. Dette omfatter all bruk av virksomhetens informasjonssystemer, inkludert stasjonært og bærbart utstyr, nettverk, pasientsystemer, programvare m.m.

3. Ansvar

Enhver leder er ansvarlig for å informere om denne instruks og gjøre den tilgjengelig for sine medarbeidere. Brukerne, ansatte, midlertidig ansatte, innleide og andre som skal gis tilgang til foretakets IKT-system, er selv ansvarlig for å gjøre seg kjent med og følge reglene i denne instruks. Foretaket forutsettes å ha nødvendig instruksjonsmyndighet på den som skal gis tilgang til foretakets IKT-system.

Ved ansettelse har foretaket nødvendig instruksjonsmyndighet. Tilsvarende må også sikres ved all innleie av personell som vil kunne komme i berøring med personopplysninger og foretakets IKT-system.

4. Fremgangsmåte

Fysisk adgang

Følgende gjelder:

- Alle ansatte skal bære gyldig ID-kort
- Den enkelte medarbeider skal, ved hjelp av fysiske sikringstiltak og/eller tilsyn, 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.
- Dersom ID-kort/nøkler mistes/blir stjålet, må dette straks meldes til
  - for Sinsen/Aker ved å ringe til ID-kortkontoret på nummer 70333
  - for Gaustad/Rikshospitalet ved å ringe til ID-kort/adgangskontrollkontoret på nummer 23070933
  - for Montebello/Radkiumhospitalet ved å ringe til ID-kortkontoret på nummer 22935896
  - for Kirkeveien, ID-kontoret på (221)18126, eller til portvakten på (221)18001.
- Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/nøkkelkort tilbake til avdelingsleder eller ID-kontoret dersom ikke annet er avtalt.
- Den som mottar besøkende, er ansvarlig for at disse ikke oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av en ansatt.
- Personer som oppholder seg i avlåste/avsperrede deler av virksomhetens lokaler uten følge av ansatt, uten ID-kort eller uten godkjennelse fra leder ansvarlig for området, skal kontaktes og eventuelt følges ut hvis de ikke skal være der.

Bruk av OUS informasjonssystemer

Logging
Bruk av foretakets informasjonssystemer blir logget. Loggene brukes til administrasjon og for å følge opp foretakets retningslinjer for informasjonssikkerhet. Loggføringen omfatter aktivitet i nettverket, bruk av tjenester og programmer, og spesielt bruk og aktivitet i

systemer som inneholder pasientopplysninger. Loggoppfølgingene kan spores tilbake til den enkelte bruker. Autorisert personell gjennomgår loggene og iverksetter tiltak om nødvendig. Brudd på foretakets retningslinjer for informasjonssikkerhet vil rapporteres til nærmeste overordnede.

System for digital informasjonsbeskyttelse
E-post som sendes til mottakere utenfor sykehuset og dokumenter som blir lastet opp på internett eller lagret på flyttbare lagringsmedier, blir skannet av systemet for digital informasjonsbeskyttelse. E-poster og dokumenter som inneholder personopplysninger blir loggført. Autorisert personell gjennomgår loggen, og tar kontakt med brukeren hvis det er nødvendig med ytterligere undersøkelser. Loggoppføringer som ikke fører til ytterligere undersøkelser blir slettet.

Om privat bruk
Sykehusets informasjonssystemer er beregnet og skal primært benyttes for jobbrelaterte formål. Eventuell privat bruk skal ikke gå ut over virksomhetsrelaterte oppgaver og funksjoner, og skal ikke gjøres dersom det krever stor lagringsplass. 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.
- Mindre mengder private filer kan lagres i egen katalog på personlig område på sykehusnettet forutsatt at katalogen er merket "privat". Av plass og kapasitetshensyn skal ikke private bilder, video, musikkfiler eller tilsvarende lagres på sykehusnettet.
- Ansatte skal ikke bruke sin stillingstittel eller e-postadresse ved sykehuset når de opptrer som privatpersoner på internett. For eksempel på sosiale nettsteder (Facebook, Twitter og lignende), i debatter eller på underskriftslister.

Eierskap og ansvar
All maskinvare, programvare, nettverksinfrastruktur og annet utstyr i informasjonssystemet er Sykehuspartner eiendom. Foretaket benytter utstyret som eget, og har via avtaler den fulle beslutningsmyndighet og ansvar. All informasjon lagret i informasjonssystemet, uavhengig av lagringsmedium, er helseforetakets ansvar. Alle personopplysninger lagret er foretakets databehandlingsansvar..

Innsynsrett
Foretaket har ved behov rett til innsyn i all informasjon lagret i informasjonssystemet. Dette inkluderer, men er ikke begrenset til:

- Innsyn ved fravær

Ved uforutsett eller langvarig fravær kan nærmeste leder få innsyn i e-postboks, privat hjemmeområde og andre lagringsområder. Den ansatte vil så langt som mulig bli varslet før innsynet, og har rett til å la seg bistå av tillitsvalgt eller annen representant. Det blir ført en protokoll for innsyn.

- Innsyn ved brudd på sykehusets retningslinjer for informasjonssikkerhet

Ved begrunnet mistanke om brudd på sykehusets retningslinjer for informasjonssikkerhet kan en representant for sykehuset få innsyn i e-postboks, privat hjemmeområde og andre lagringsområder. Den ansatte vil så langt som mulig bli varslet og få anledning til å uttale seg før innsynet, og har rett til å la seg bistå av tillitsvalgt eller annen representant. Det blir ført en protokoll for innsyn.

De øvrige reglene for arbeidsgivers rett til innsyn finnes i personopplysningsforskriftens kapittel 9.

IKT-utstyr
Det er kun tillatt å bruke **godkjent maskinvare, programvare, nettverksutstyr, lagringsmedier og annet utstyr** i sykehusnettet med mindre annet er eksplisitt avtalt:

- Alt utstyr skal være levert av Sykehuspartner IKT
- Installasjon av alt utstyr og programvare skal gjøres av Sykehuspanrters IKT-ansatte eller av de som er utpekt til å gjøre denne jobben.
- Bruk av annen programvare eller maskinvare utenom det som sykehuset tilbyr som standard programvare, må godkjennes av autorisert personell.

Det er ikke tillatt å koble til privat utstyr av noe slag i sykehusets nett. Dette inkluderer PDA, mobiltelefon kamera og minnepenn. Eksterne konsulenter og vikarer skal ikke koble til egne PC'er i sykehusets nett, men få tildelt maskin av sykehuset. Særskilte behov for egne PC'er skal avklares med IKT-sikkerhetssjef. Det skal ikke tilkobles separate eksterne forbindelser til sykehusets nett (for eksempel via ekstra nettverkskort, trådløst forbindelse/aksesspunkt, modem, ISDN og lignende) uten godkjennelse fra IKT-sikkerhetssef. Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

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

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

Pålogging og avlogging, brukernavn, passord og skjermsparer

- Passordet (og eventuelt brikke/kort for fjerntilgang/passordkalkulator) er den ansattes personlige nøkkel til sykehusets 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, passordkalkulator og pålogget tilgang.
- Det er ikke tillatt å bruke en annens brukertilgang/passord
- Passord skal *ikke* skrives ned uten godkjennelse fra IKT-sikkerhetssjef.
- Velg et passord som er lett å huske. Passordet skal ikke inneholde navn på familiemedlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.
- Passordet skal bestå minst åtte tegn, hvorav

- minst et av tegnene skal være et tall
- minst et av tegnene skal være en stor bokstav (ikke Æ, Ø eller Å)
- minst et av tegnene skal være en liten bokstav (ikkeæ, ø eller å)

- Siste 5 passord skal ikke gjenbrukes. Passord skal endres hver 180 dag. Du vil få en påminnelse når det er på tide å bytte passord (enkelte gamle systemer kan avvike fra dette)
- Ved mistanke om at passordet er blitt kjent av andre, skal passordet byttes.
- 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. Hurtigpålogging fra Pasdoc benyttes for å sikre rask innlogging igjen
-
-

Informasjonshåndtering

Personopplysningsloven og personopplysningsforskriften omfatter personvern og informasjonssikkerhet, og gir 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 flere persondata enn fødselsår og initialer.
- Før et register opprettes, skal det meldes til personvernombudet ved foretaket, som skal ha oversikt over all behandling av personopplysninger. Registre med personopplysninger kan ikke opprettes før de er meldt til personvernombudet og personvernombudet har gitt nødvendig tilrådning til opprettelse av registeret. Meldeskjema for melding til personvernombud og styrende dokumenter finnes i sykehusets e-håndbok, på Intranett og Internett. Ved formål og bruk ifm medisinsk og helsefaglig forskning, skal det også søkes om godkjenning hos De regionale komiteer for helsefaglig og medisinsk forskningsetikk (REK).
- Ved lagring av personopplysninger, skal teknisk sikring vurderes av personvernombudet. Det gjelder strengere krav til sensitive personopplysninger, hvor både tilgangskonstroll skal kunne reguleres og tilgang logges ved bruk. Personopplysninger som foretaket er databehandlingsansvarlig for, kan ikke lagres på privat utstyr eller lagringsmedium. Sensitive personopplysninger kan heller ikke lagres i universitets- eller høyskolenett. Alle lagring av personopplysninger utenfor foretakets nettverk/utstyr krever gjennomført risikovurdering, som må godkjennes av foretakets IKT-sikkerhetssjef, før lagring kan gjøres. All lagring utenfor foretakets nettverk/utstyr krever også inngått databehandleravtale før slik lagring kan gjøres.
- For all annen bruk av sensitive personopplysninger og personregistre enn direkte helsehjelp og pålagte meldinger, skal det som hovedregel innhentes samtykke fra de inkluderte.
-
- Helse- og personopplysninger ved sykehuset skal ikke gjøres tilgjengelig for uautorisert personell eller andre uvedkommende, herunder også egne ansatte.
- Det skal ikke søkes etter pasientinformasjon eller andre opplysninger den ansatte ikke har bruk for i det daglige arbeidet.
- Utskrifter skal hentes umiddelbart.

Lagring
Det er som hovedregel kun tillatt å lagre sensitive personopplysninger i godkjente fagapplikasjoner på sykehusnettet. Unntak fra dette er:

- Bruk av ikke-fagapplikasjoner (som Word) for skriving av journaler, sakkyndigrapporter og tilsvarende er *kun* tillatt dersom dette er tiltenkt som midlertidig lagring. Navn, personnummer og andre direkte identifiserbare kjennetegn skal skrives inn så sent som mulig og slettes straks de er skrevet ut, slik at disse opplysninger elektronisk kun er tilgjengelig i minimalt tidsrom. Denne midlertidige lagring skal bare skje på avdelingens fellesområde / hjemmeområde på serveren. Notatene *skal* slettes etter de er godkjent, eventuelt lagt inn i fagapplikasjoner og skrevet ut.
- Helse- og personopplysninger skal bare lagres lokalt på PC eller på portabelt utstyr som bærbar PC, minnepinner eller lignende dersom det er innhentet godkjenning fra personvernombudet og forutsatt at lagring skjer med løsninger godkjent av IKT-sikkerhetssjef. Dette gjelder også kodede (avidentifiserte) opplysninger.
- Helse- og personopplysninger skal ikke lagres på PDA, mobiltelefon, MP3 spillere eller tilsvarende og aldri på privat utstyr. Bruk av kamera må sikres med egne rutiner og skal ikke være privat kamera.
- Sensitive personopplysninger, inkludert kodede (avidentifiserte personopplysninger) skal aldri lagres i det ordinære UiO-nettet eller på privat utstyr.
- Forskningsstudier skal som hovedregel lagres på dedikerte forskningsservere i samsvar med hva som er meldt. Unntak skal være registrert og avtalt i melding til sykehusets personvernombud.
- Kvalitetsregistre skal som hovedregel lagres på dedikerte kvalitetssikringsservere i samsvar med hva som er meldt. Unntak skal være registrert og avtalt i melding til sykehusets personvernombud.Når lagringsmedia eller dokumenter med registre eller sensitive personopplysninger ikke er under direkte oppsyn, skal de oppbevares nedlåst.

Forsendelse
Sensitive personopplysninger skal ikke sendes på ukryptert epost, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger. Risikovurdering skal gjennomføres og godkjennes av IKT-sikkerhetssjef før slike forsendelsesmetoder benyttes. Dokumenter og lagringsmedia med sensitive personopplysninger skal alltid forsendes i gjenlimt konvolutt/forseglet innpakning.

Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for opplysningene.

Sensitive personopplysninger kan kun utleveres dersom det foreligger nødvendig hjemmel. Utlevering uten slik hjemmel vil være et **lovbrudd og et alvorlig brudd på retningslinjene for informasjonssikkerhet**.

Makulering/sletting av dokumenter

Dokumenter med person og helseopplysninger 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.

Ansatte som slutter, skal rydde i egne filområder og e-post og sikre at all relevant informasjon blir lagret på **avdelingens filområde**. Gjenværende informasjon på brukerens område slettes når ansettelsesforholdet er avsluttet.

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

Kassering/Håndtering av utstyr og lagringsmedier
Harddisker, minnepinner, utstyr som inneholder harddisker og andre elektroniske lagringsmedier, skal leveres til Sykehuspartner IKT for forsvarlig destruksjon. Lagringsmedia som CD, DVD, floppy-disker osv som inneholder sensitive person- og helseopplysninger (inkluderte kodede), skal leveres til Sykehuspartner IKT for destruksjon, mens media med andre opplysninger klippes/brekkes i biter og kastes som avfall. Alternativt kan tilsvarende løsninger selv etableres og benyttes etter godkjenning av IKT-sikkerhetssjef. Ansatte som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutinene over.

Sikkerhetskopiering
Det tas regelmessige sikkerhetskopier av all informasjon lagret i sykehusets fagapplikasjoner og på sykehusets filservere. For å sikre at det blir tatt sikkerhetskopier, skal all jobbrelatert informasjon lagres på eller eventuelt systematisk kopieres til sykehusets fagapplikasjoner eller filservere. Det blir ikke tatt sikkerhetskopier av informasjon lagret på lokale lagringsmedier som for eksempel minnepinner, eksterne harddisker eller **lokal harddisk på PC-er i sykehusnettet.**

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

Internett
Den ansattes oppslag på Internett kan spores tilbake til virksomheten og den PC/brukeridentiet som var i bruk da oppslaget ble gjort. Internett skal benyttes med varsomhet 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 surfe på sider eller laste ned og lagre filer som inneholder pornografi, opphavsrettslig beskyttet materiale (f.eks. musikk, filmer og programvare), eller informasjon som er støtende, trakasserende, obskøne, truende eller rasistiske. Slike filer kan bli slettet automatisk uten varsel
- Det er ikke tillatt å laste ned og installere programvare på OUS IKT-utstyr uten spesiell godkjenning i forkant
- Fildelingstjenester er ikke tillatt
- Ressurskrevende ikke-jobbrelaterte tjenester/applikasjoner, f.eks. radiolytting og TV/video-streaming, er ikke tillatt.

E-post og viruskontroll
Det skal skilles på intern og ekstern e-post. Merking eller annen tilsvarende funksjonalitet skal bekrefte at det som sendes ut ikke inneholder sensitive personopplysninger. Ekstern e-post som ikke er merket slik, blir blokkert av sikkerhetssystemet.

E-post er ikke sikkert nok til å kommunisere sensitive personopplysninger/journalopplysninger eller personnummer med. Dersom pasienter likevel skulle sende forespørsel om egen eller andre navngitte personers helse via e-post, skal dette besvares med at e-post ikke kan benyttes for slik kommunikasjon. Vær nøye med å ikke returnere mottatt e-post i besvarelsen. Henvendelsen fra pasient må ivaretas på annen måte, slik at forespørsel blir tilstrekkelig besvart.

Eventuell privat e-post skal lagres i en egen mappe merket "privat".

Massedistribusjon av informasjon skal være jobbrelatert og ansvarlig for distribusjon 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 Sykehuspartner IKT kontaktes eller e-post-meldingen slettes. Mottaker av e-post bør melde til avsender hvis mottaker åpenbart er feil adressat. Slike e-poster skal slettes.

Reparasjon, service, vedlikehold og brukerstøtte

- Ta kontakt med Sykehuspartner IKT dersom du har mistanke om feil eller problemer med tilgang til systemer, tjenester eller informasjon
- All reparasjon av IKT-utstyr skal bestilles gjennom Sykehuspartner IKT slik at nødvendige sikkerhetstiltak kan iverksettes før utstyret videresendes til reparasjon.
- Eventuelle feilmeldinger til utstyrsleverandører skal sendes til Sykehuspartner. Dette gjelder også utstyr som skal til service.
- Alt arbeid som skal utføres av eksternt personell på sykehusets systemer og utstyr skal bestilles gjennom Sykehuspartner IK

Kartlegging og utnyttelse av systemsvakheter
Den ansatte 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.

5. Definisjoner

Se alle definisjoner i eget dokument som legges inn med peker når begge dokument er lagt inn i e-håndboken.

6. Avvik eller dissens

Mistenkelige hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste leder, eller til IKT-sikkerhetssjef. Avvikene skal registreres i foretakets avvikssystem.

Brudd på denne sikkerhetsinstruksen ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for sikkerhet, og vil bli behandlet som personalsak. Alvorlige brudd på reglene i sikkerhetsinstruksen vil få konsekvenser for ansattes arbeidsforhold samt eventuelt resultere i strafferettslige reaksjoner.

IKT-sikkerhetssjef/personvernombud kan benyttes for rådføring.

7. Referanser

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

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

Lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

Forskrift av 15. des. 2000 om behandling av personopplysninger (personopplysningsforskriften)

Norm for informasjonssikkerhet i helsesektoren

Oslo universitetssykehus

Notat

Fra: Heidi Thorstensen, IKT-sikkerhetssjef/Personvernombud

Behov for innskjerping av tilgang til journal – den enkeltes ansvar

MÅLGRUPPE: Alle som gis tilgang til sykehusets elektroniske journal

For å sikre forsvarlig helsehjelp og deri nødvendig tilgang til journalopplysninger, må sykehuset rent teknisk gi videre tilganger enn kun til de pasienter den enkelte deltar i helsehjelpen med. Teknisk tilgang gir imidlertid ikke grunnlag for å søke opp en pasient, men kun en nødvendig mulighet som kun skal benyttes når det er lovlig grunnlag for oppslag på konkret pasient. Det er derfor helt avgjørende at den enkelte som får disse tilganger, forstår og etterlever de føringer som gjelder for tilgang i de enkelte journaler. Brudd på dette medfører konsekvenser for vedkommendes ansettelsesforhold.

1. Lovlig bruk av tildelte tilganger

Aktualisering – rett til å beslutte tiltak, Denne myndigheten tilligger kun lege, selv om funksjonen også gis til sekretær der disse skriver for lege. Det påpekes at sekretær og eventuelt andre som gis denne funksjonen og som ikke er ansvarlig for behandlingen, ikke selv har myndighet til å beslutte tiltak. Deres bruk av aktualisering kan kun legitimeres når det er på legens beslutning aktualiseringsfunksjonen benyttes.

Følgende gjelder for bruk av tekniske tilganger i journal:

A. **Helsehjelp til aktuell pasient**, Den som yter selvstendig helsehjelp eller som deltar i behandlingen av en pasient, skal dokumentere egen helsehjelp og kan i denne sammenheng søke relevante opplysninger i journalen om den aktuelle pasient. For de fleste vil tilgang til de relevante journaler i denne sammenheng gjøres med normal tilgang. Aktualisering vil typisk kun være relevant ifm lege i vakt og funksjoner som går på tvers av hele sykehuset, eksempelvis anestesi. For pleiepersonell skal tilgangene til inneliggende pasienter på egen avdeling oppnås med ordinære tilgang. Telefonoppringning fra pasienten etter utskriving, vil typisk kreve funksjonen aktualisering for at tilgang til tidligere journalnotater, prøver og bilder, før pasienten igjen innlegges, skal oppnås. Alle legene vil ha denne muligheten, men normalt ikke pleiepersonellet. Kun de pasienter man deltar i helsehjelpen for, kan som hovedprinsipp slås opp i journalen for.

B. **Kvalitetssikring av gitt diagnostisering og behandling**, Medisinsk faglig ansvarlig for en gitt behandling kan på eget initiativ eller på leders initiativ gjennomgå relevante journaler ifm kvalitetssikring. Avdelingsleder og medisinsk faglig ansvarlig for gitt behandling kan i denne sammenheng også be annet personale som har tilgang i journalen, å gjøre slik gjennomgang. Det skal i så tilfelle foreligge dokumentasjon på at slik gjennomgang er spurt om av bemyndiget person. Siden dette oftest vil omfatte også utskrevne pasienter, vil bruken av aktualisering måtte benyttes, og forutsetter beslutning om bruk av slik tilgang av autoriserte. Etablering av registre for slik sammenligning må være meldt sykehusets personvernombud i forkant for etablering av slike registre.

C. **Faglig interesse og egenopplæring**, Faglig interesse og faglig oppfølging av pasient etter gitt behandling, krever samtykke fra den aktuelle pasient for slikt innsyn, når pasienten ikke lenger er under behandling av denne person. Det samme gjelder om pasienten ikke er gitt behandling av den som ønsker innsyn, men det søkes kunnskap om en gitt diagnose eller behandlingsform. Innsyn gitt denne årsak skal spesifikt dokumenteres i blindnotat, hvor det skal angis årsak til at man har gått inn i journalen og at samtykke er innhentet. Dette kommer i tillegg til at det må angis grunn når aktualisering benyttes dersom pasienten er utskrevet. Innsyn av denne årsak kan ikke forveksles med kvalitetssikring, punkt B, som krever at leder eller medisinsk faglig ansvarlig for gitt behandling

initierer en systematisk gjennomgang. Dersom samtykke fra pasient ikke er mulig, kan en annen som er autorisert for innsyn (pasientansvarlig eller journalansvarlig) ta ut relevante opplysninger og anonymisere dem før de overleveres til den som er faglig interessert. Dette punktet er svært relevant for studenter, hvor samme regler er gjeldende.

D. **Kodeveiledning og øvrige tilsvarende pålagte funksjoner,** Kodeveiledning og andre tilsvarende pålagte funksjoner gir grunnlag for begrenset innsyn i journal. Kodeveileder må imidlertid faktisk ha en aktiv funksjon for spesifikk pasient om innsyn kan legitimeres, eller revisjon kan initieres av ledelsen. Dette kan ikke initieres av den enkelte selv.

2. Konsekvens for den enkelte dersom pålagte føringer ikke følges

Tildeling av de funksjonelle rettighetene i journalen forutsetter at de brukes i samsvar med gjeldende regler. Det er den enkeltes ansvar å sette seg inn i og følge sykehusets instrukser og regler for tilgang og bruk av journaler.

Mistenkelige hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste leder, Sikkerhetssjef ved fysiske innbrudd eller IKT-sikkerhetssjef. Hendelser knyttet til at de styrende dokumenter for journal og Sikkerhetsinstruksen ikke følges, vurderes som sikkerhetsbrudd. Slike brudd ses på som mislighold av arbeidsavtalen og vil bli behandlet som personalsak. Alvorlige brudd på reglene i Sikkerhetsinstruksen vil få konsekvenser for ansattes arbeidsforhold samt eventuelt resultere i strafferettslige reaksjoner. Ved mistanke om mislighold av tillit, skal det gjennomføres en samtale hvor det avklares hva som har skjedd.

Følgende skal vurderes som reaksjoner ved sikkerhetsbrudd:

i. Skriftlig advarsel i personalmappen. Dette er minimum reaksjon.
ii. Rapportering av den enkeltes adferd til Helsetilsynet. Dette vil typisk være reaksjon om handlingen er alvorlig og det er grunn til å sette spørsmål ved vedkommendes forståelse av ansvar og plikter for helsepersonell.
iii. Ved gjentatte hendelser eller svært alvorlige hendelser må oppsigelse vurderes.
iv. Eventuell anmeldelser og strafferettslige reaksjoner om hendelsen er av slik karakter.

I noen tilfeller ved mistanke om misbruk, har den ansatte påstått at andre har vært inne og brukt vedkommendes tilgang. I en hektisk arbeidssituasjon, kan det være tilfellet, men den ansatte er uansett ansvarlig for bruken av sin pålogging, og skal logge seg ut av systemet som inneholder pasientopplysninger før arbeidsstasjonen forlates. Dette er tydeliggjort i gjeldende Sikkerhetsinstruks, og endrer ikke på at den ansatte vil være ansvarlig for de oppslag i journal som gjøres.

3. Sentrale styrende dokumenter ifm krav til sikkerhet, tilgang til journal og atferd for ansatte/innleide

Følgende styrende dokumenter er sentrale for krav til sikkerhet, tilgang til journal og atferd for ansatte, innleide og studenter, se e-håndboken nivå 1 (kun de mest sentrale er angitt):

- Sikkerhetsinstruks
- Pasientjournalen – Føring, tilgang, behandling, pasientens innsynsrett, forskning og oppbevaring
- Pasientjournalen – Tilgang til journalen, tilgangsmatrise og aktualiseringsrett