

Styringsystem for informasjonssikkerhet

Versjon 1.0 23/6-2006

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 1 av 25

Innholdsfortegnelse

1.	Innledning.....	3
1.1.	Målgrupper for dokumentet	3
1.2.	Relasjon mellom dokumenter.....	3
1.3.	Styringssystemets omfang.....	4
2.	Sikkerhetsmål	5
2.1.	Akseptabel risiko.....	5
3.	Sikkerhetsstrategi	7
4.	Den registrertes rettigheter	10
4.1.	Generelle rettigheter	10
4.2.	Journalspesifikke rettigheter	10
5.	Sikkerhetsorganisering og ansvar.....	12
5.1.	Oversikt over funksjoner	12
5.2.	Funksjonsbeskrivelser	12
6.	Gjennomføring av risikovurdering og beskrivelse av tiltak.....	15
6.1.	Forberedelsesfasen	15
6.2.	Gjennomføring	15
7.	Sikkerhetsinstruks	18
Vedlegg 1.	Definisjoner	19
Vedlegg 2.	Forklaring på tabellene i Vedlegg 3 og Vedlegg 4.....	20
Vedlegg 3.	Vurdering av sannsynlighet.....	21
Vedlegg 4.	Vurdering av konsekvens	22
Vedlegg 5.	Minimum innhold i sikkerhetsinstruks.....	23

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 2 av 25

1. Innledning

Dette dokumentet gir et felles grunnlag for informasjonssikkerhet innen spesialisthelsetjenesten. Styringssystemet bidrar til å sikre et felles nivå på informasjonssikkerhet på tvers av virksomheter, og gir felles føringer for alle helseforetak, regionale helseforetak, Norsk Helsenett samt øvrige driftsenheter eid av disse. Dette styringssystemet, sammen med bransjenorm for informasjonssikkerhet, er en erstatning for bilaterale avtaler mellom de virksomhetene som benytter styringssystemet.

1.1. Målgrupper for dokumentet

Dokumentet gir føringer for alle virksomheter som håndterer informasjon med krav til sikring for spesialisthelsetjenesten.

Dette felles styringssystemet skal benyttes i egen organisasjon. Styringssystemet gir et minimum av sikkerhetskrav som må oppfylles og etterlevs for å behandle helse-/personopplysninger og for å kunne samhandle. Styringssystemet gir føringer for informasjonsbehandlingen, men er ikke alene tilstrekkelig som sikkerhetsdokumentasjon for virksomhetene. Virksomhetene er selv ansvarlig for å etablere det totale sikkerhetsregime i organisasjonen.

1.2. Relasjon mellom dokumenter

Det er flere lover og forskrifter som regulerer krav til informasjonsbehandling i helsesektoren. De mest sentrale myndighetskravene som regulerer informasjonssikkerhet i helsesektoren er helse-registerloven med forskrifter, helsepersonelloven, pasientrettighetsloven og personopplysningsloven med forskrift. Sosial- og helsedirektoratet har i samarbeid med helsesektoren utarbeidet en bransjenorm¹ for informasjonssikkerhet.

Bransjenormen for informasjonssikkerhet er et rammeverk som ved å følges, sikrer etablering av alle relevante informasjonssikkerhetsaspekter i lovgivningen. Dette felles styringssystem er etablert for å etterkomme bransjenormens forutsetning om etablering av styringssystem og å gi nødvendige detaljer for felles akseptanskriterier.

Den enkelte virksomhets styringssystem skal ha følgende oppbygning:

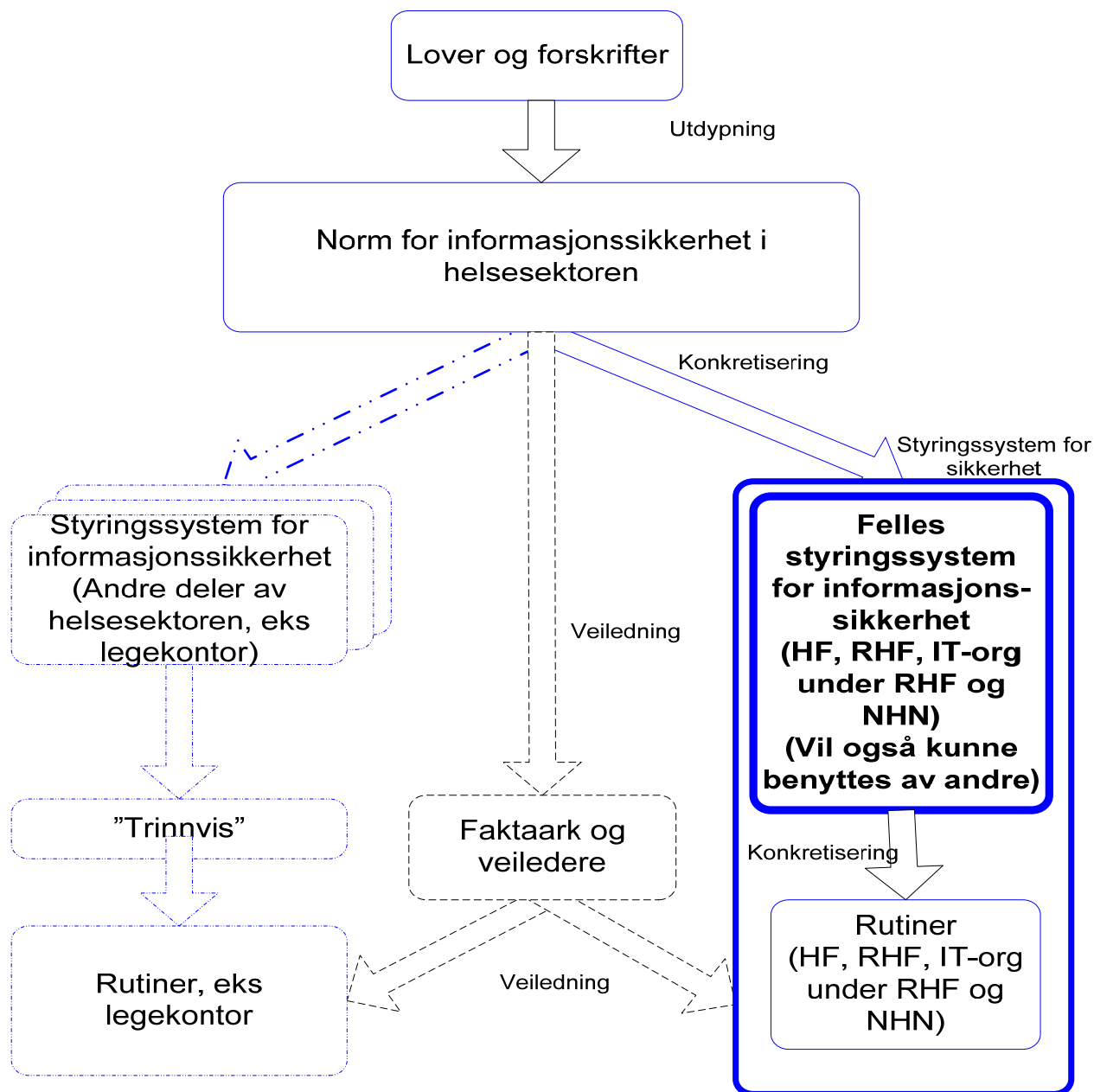
- Felles styringssystem for informasjonssikkerhet
- Eventuelle virksomhetsspesifikke tilpasninger
- Virksomhetsspesifikke rutiner

Bransjenormen ligger til grunn for utformingen av det felles styringssystem. Faktaarkene knyttet til bransjenormen er ment som en praktisk veiledning for utarbeiding av de virksomhetsspesifikke tilpasninger og rutiner.

Se skissen i Figur 1 som viser en skjematisk sammenheng.

¹ Foreløpig ennå ikke formalisert.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 3 av 25



Figur 1 – Lover og forskrifter – Sikkerhetsnorm – Styringssystem for sikkerhet

1.3. Styringssystemets omfang

For å utføre oppgaver innen spesialisthelsetjenesten, behandler virksomheten personopplysninger om medarbeidere, pasienter og om andre personer som er i kontakt med virksomheten. Disse opplysningene behandles i overveiende grad elektronisk og omfatter også bruk av medisinskteknisk utstyr (MTU), og annet tilsvarende utstyr.

Dette styringssystemet gjelder for all informasjonsbehandling av personopplysninger. Styringssystemet dekker også metoder for sikring av virksomhetens øvrige informasjon (eksempelvis økonomiske og strategiske opplysninger).

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 4 av 25

2. Sikkerhetsmål

Virksomheten skal behandle personopplysninger i samsvar med kravene i helseregisterloven og personopplysningsloven med tilhørende forskrifter. Ingen helse- og personopplysninger skal samles inn, bearbejdes, lagres eller slettes uten at den opplysningene omhandler har gitt sitt samtykke, eller det er fastsatt i lov at det er adgang til slik behandling.

Følgende sikkerhetsmål skal oppnås:

- at kun personell med autorisert tilgang kan benytte informasjonssystemene² (konfidensialitet)
- at autorisert personell har korrekt tilgang til tjenester og informasjon til rett tid og riktig sted (tilgjengelighet)
- at informasjonen til enhver tid er et resultat av rettmessige registreringer og kontrollerte aktiviteter (integritet)
- at informasjonen til enhver tid er fullstendig, oppdatert og korrekt³. (kvalitet)
- at den registrertes rettigheter ivaretas
- at alle som ber om det, skal få generell informasjon om virksomhetens behandlinger av personopplysninger.

Internkontroll knyttet til informasjonssikkerhet har som formål å sikre at medarbeidere med autorisert tilgang benytter informasjonssystemet i tråd med nedfelte rutiner. Videre skal internkontrollen sikre at den registrertes rettigheter blir ivaretatt. Når det forekommer avvik på nedfelte databehandlingsrutiner, skal dette registreres som avvik og avviksbehandles.

2.1. Akseptabel risiko

Sikkerhetsbrudd aksepteres ikke. Virksomhetene erkjenner like fullt at det eksisterer sannsynlighet for at sikkerhetsbrudd kan forekomme. For å begrense sannsynlighet for uønskede hendelser, etableres akseptkriterier knyttet til risiko.

Sikkerhetstiltak skal etableres slik at:

- tiltakene omfatter både rutiner medarbeiderne forutsettes å følge, og tiltak som ikke kan påvirkes eller omgås av medarbeiderne med uaktsomhet.
- tiltakene ikke kan omgås av eksterne, selv om disse opptrer med forsett.
- der er liten sannsynlighet for at sensitive personopplysninger/helseopplysninger kompromitteres.
- øvrige personopplysninger skal minimum sikres med tiltak som gir moderat grad av sannsynlighet for kompromittering, forutsatt at dette ikke øker sannsynligheten for kompromittering av sensitive personopplysninger.
- det går flere år mellom hendelser med moderat konsekvens for helsehjelpen⁴, forholdet til pasienten⁵, helseforetaket/-personellet⁶ og for øvrige medarbeidere⁷.
- hendelser med alvorlig konsekvens er enda vanskeligere å forårsake og inntreffer enda sjeldnere

For å forebygge vesentlig fare for liv eller alvorlig skade på noens helse, vil kravet til konfidensialitet kunne settes til side for å sikre nødvendig tilgjengelighet på opplysninger. Et slikt brudd på konfidensialiteten skal behandles som sikkerhetsavvik i etterkant og loggføres.

² Tilgang til opplysninger vil også reguleres av taushetsplikten i lover.

³ Ansvar i fm faglig innhold og forsvarlighet i dokumentasjon tilligger ikke dette styringssystemet.

⁴ Eksempelvis hendelser som kan medføre helseopplysninger med utilstrekkelig kvalitet

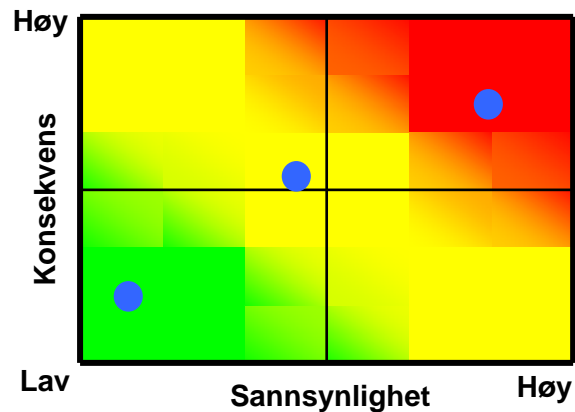
⁵ Eksempelvis hendelser som kan medføre at personlig integritet og privatlivets fred ikke ivaretas

⁶ Eksempelvis hendelser som kan medføre bøtStraff eller suspensjon av autorisasjon, lisens eller spesialistgodkjenning

⁷ Eksempelvis hendelser som kan medføre betydelig – men gjenopprettelig – økonomisk tap

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 5 av 25

Risikomatrise



● Markering av en hendelse i forhold til sannsynlighet og konsekvens

Figur 2 – Visualisering av akseptabelt risikonivå for helseopplysninger

Figur 2 gir en visualisering av risikonivå ved behandling av helseopplysninger. Hver hendelse som kan påvirke sikkerheten ved databehandlingen av personopplysninger, og dermed gi et uakseptabelt risikonivå, må vurderes. Vurderingen gjøres i forhold til sannsynlighet for at hendelsen vil inntre og hvilken konsekvens dette vil få dersom den inntre. Graden av sannsynlighet og konsekvens er angitt i skala fra lav til høy, og må begrunnes i risikovurderingen. Det grønne område viser der risikonivå for at hendelse inntre og konsekvenser ved dette er akseptabel. Det røde området viser der risikonivå for at hendelse inntre og konsekvens ikke er akseptabelt, og hvor nye/endrede sikkerhetstiltak må etableres. Det gule feltet, og overgangen mellom gult/grønt og gult/rødt må gis en argumentasjon i risikovurderingen for å konkludere om sannsynlighet for at den enkelte hendelse inntre og konsekvenser ved denne er akseptabel, eller om tilleggstiltak må etableres for å oppnå akseptabelt risikonivå.

Som vedlegg ligger detaljer for felles førende krav til akseptansenivå, se Vedlegg 3 og Vedlegg 4. Vedleggene viser tabeller for gradering av sannsynlighet og konsekvens som skal benyttes i risikovurderinger.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 6 av 25

3. Sikkerhetsstrategi

Sikkerhetsstrategien utgjør føringer som virksomheten setter for å oppnå det definerte sikkerhetsmålet. De strategiske føringene underbygges av rutiner og tekniske tiltak.

Organisasjon – ansvar

- Databehandlingsansvarlig er virksomhetens administrerende direktør/daglig leder
- Sikkerheten ved virksomheten skal ha forankring i ledelsen.
- Sikkerheten skal ivaretas som en integrert del av organisasjonen med klare ansvars- og myndighetsforhold
- Sikkerhetsorganiseringen skal sikre et utøvende og et kontrollerende ansvar
- Utnevnelse av personvernombud (PVO) kan benyttes for å sikre oppfylging av lovverk⁸

Ansatte/medarbeidere og bruk av informasjonssystemet

- Informasjonssystem skal benyttes for virksomhetsrelaterte oppgaver og virksomhetens medarbeidere skal ha tilstrekkelige kunnskaper for slik bruk.
- Privat bruk av informasjonssystemet kan i begrenset grad tillates, forutsatt at slik bruk ikke utsetter behandling av helseopplysninger for ytterligere risiko.
- Alle medarbeidere plikter å etterleve føringer gitt i dette sikkerhetsregelverket. Misbruk av informasjonssystemet og/eller brudd på sikkerhetsbestemmelsene, kan medføre disiplinære reaksjoner.
- Det skal sikres at medarbeidere har tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov/krav.

Avtale med eksterne

- Eksterne partnere og leverandører skal forplikte seg gjennom avtale til å følge relevante krav i lovgivningen (helselovgivning og personopplysningsloven med forskrift) og bransjenorm for sikkerhet. Videre vil kravene i styringssystem for sikkerhet være gjeldende. Eksterne kan omfatte:
 - Virksomheter som følger dette styringssystem og er tilsluttet bruk av bransjenorm. Disse er underlagt samme sikkerhetsregimet og det er dermed ikke behov for annet enn bekreftelse og tilslutning til styringssystem og bransjenorm.
 - Databehandlere, som har egne styringssystem for sikkerhet, og hvor det ved databehandleravtaler må settes krav til leverandør om å oppfylle sikkerhetskrav i dette styringssystem for sikkerhet og bransjenorm.
 - Online-service leverandører, som har egne styringssystem for sikkerhet, og hvor det ved avtaler må settes krav til leverandør om å oppfylle relevante deler av sikkerhetskrav i dette styringssystem for sikkerhet og bransjenorm.
- Formål og håndtering av personopplysninger inkludert krav til sikkerhetsnivå og sletting ved avslutning av formålet må alltid sikres ved bruk av eksterne parter.

Konfidensialitet – tilgjengelighet – integritet – kvalitet

- Tilgang til systemer og informasjon gis kun til medarbeidere etter tjenstlig behov.
- All tilgang til personopplysninger gis på individuell basis.
- Det skal forhindres at uvedkommende får tilgang til systemer og informasjon.
- Det skal forhindres at personer bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller privatpersoner.

⁸ Utnevnelse av PVO er valgfritt, og kan gjøres med intern eller ekstern utnevnelse.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 7 av 25

- Det skal sikres at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
- Det skal sikres at nødvendig tilgjengelighet til systemer/tjenester og informasjon til rett tid for de personer som er autorisert til dette.
- Det skal etableres et entydig ansvar for å sikre at medarbeidere ikke lenger har tilgang til systemet når behovet opphører.
- Autentiseringsmekanismer, som bruk av passord, skal utformes på en slik måte at man kan ha tilfredsstillende tillit til at kun rett person får tilgang.
- Ekstern kommunikasjon av sensitive personopplysninger skal sikres med kryptering eller tilsvarende mekanismer.
- Dersom man befinner seg utenfor virksomheten og skal gis tilgang til sensitive personopplysninger, skal tilkoblingen sikres med tilstrekkelig 2-nivå autentisering.
- Det skal utarbeides rutiner for kassering, transport og service av IKT-utstyr inneholdende minne, slik at ikke uvedkommende får tilgang og innsyn.
- IKT-løsningene må ha viruskontroll og sikres mot øvrig ondsinnet kode
- Det skal gjennomføres adgangskontroll på områder som ikke er åpent for publikum. Medarbeidere som oppholder seg i slike områder, skal bære synlig adgangskort.
- Sensitive personopplysninger og øvrige sikringsverdige opplysninger skrevet ut på papir eller lagret elektronisk på flyttbare media, skal sikres mot uautorisert innsyn.

Sikkerhetsnivå for sensitive personopplysninger

- Sikkerhetsnivå for virksomhetens IKT-løsning etableres ved bruk av risikovurdering hvor akseptansekriterier (se Vedlegg 3 og Vedlegg 4) legges til grunn. Videre kreves det at sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og skal ikke være begrenset til handlinger som den enkelte forutsettes å utføre.

Forvaltning – oppfølging – forbedring

- Det skal være mulig å spore relevante sikkerhetshendelser.
- Det skal være etablert rutiner og løsninger for å håndtere uønskede, inkludert virksomhetskritiske, hendelser (et avviksrapporingssystem).
- Det skal være etablert systematiske lærings- og forbedringsprosesser ved uønskede hendelser, slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres.
- For å sikre at endringer og nyinstallasjoner ikke uønsket påvirker sikkerheten, skal det alltid gjennomføres og dokumenteres konsekvens og risikovurdering før realisering. Avdekkede nødvendige sikkerhetstiltak skal inkluderes i gjennomføringsplan.
- For å sikre at forutsatt sikkerhetsnivå virkelig er etablert og følges, skal det jevnlig foretas revisjoner. Avvik skal følges opp og lukkes iht rasjonell fremdriftsplan. Det må sørges for at revisjonsteamet har tilstrekkelig kompetanse, og uavhengighet til revisjonsobjektet.
- Ledelsen skal ved minimum årlig gjennomgang av kritiske avvik funnet ved revisjoner, risikovurderinger og tilsyn, samt rapporterte alvorlige sikkerhetshendelser, vurdere behov for tiltak og endringer i sikkerhetsmål og –strategi, samt budsjettere for utvikling og iverksetting av nye sikkerhetstiltak. Behov for endring av sikkerhetsmål og –strategi som krever endring i dette styringssystemet, må sikres gjennomført hos alle virksomheter.
- Det skal være etablert beredskaps og krisehåndtering som sikrer nødvendig oppetid og tilgjengelighet av kritiske systemer.
- Rutiner for bruk av informasjonssystemet og annen informasjon av betydning for informasjonssikkerheten, skal dokumenteres. Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny utgave. Registrering av autorisert bruk av

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 8 av 25

informasjonssystemet, samt forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten.

Sikre relevant hjemmelsgrunnlag ved databehandling av personopplysninger

Det skal føres oversikt over alle databehandlinger som omfatter personopplysninger, inkludert oversikt over hjemmelsgrunnlaget for slik behandling. Behandling av sensitive personopplysninger skal være gitt i medhold av lov (melding), i konsesjon eller tilråd fra personvernombud der dette er oppnevnt.

Ivareta den registrertes rettigheter

Dersom ikke hjemmelsgrunnlaget for å behandle personopplysninger er gitt i lov eller forskrift, skal slik behandling som hovedregel være basert på samtykke, alternativt dispensasjon. Ved dispensasjon skal det vurderes om den registrerte likevel skal informeres.

Den registrerte skal informeres om sine rettigheter til innsyn, retting og sletting av personopplysningene. For retten til sletting må dette vurderes om annet er grunnlagt i lov.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 9 av 25

4. Den registrertes rettigheter

Den registrertes rettigheter til innsyn, retting, sletting og sperring skal sikres, slik at de etterkommes i samsvar med rettigheter som følger av pasientrettighetsloven samt personopplysningsloven.

Følgende rettigheter skal sikres med tilhørende rutiner og ansvar.

4.1. Generelle rettigheter

Rett til innsyn i opplysninger som er registrert om den enkelte

Den registrerte har rett til å be om innsyn i de opplysninger som er registrert om vedkommende. Dette gjelder både om opplysningene er registrert som direkte identifiserbare ved navn eller fødselsnummer, eller om de er indirekte identifiserbare under en kode. En slik forespørsel skal etterkommes. For innsyn i journal, se eget punkt.

Rett til å få rettet og til å få slettet opplysninger som er registrert om den enkelte

Dersom de opplysninger som er registrert om den enkelte er ukorrekte eller feilaktige, har den registrerte rett til å be om at opplysningene korrigeres, slik at de blir riktige. En slik forespørsel skal etterkommes. Videre skal også krav om sletting etterkommes dersom det ikke annet er lovhjemlet. For retting og sletting i journal, se eget punkt.

4.2. Journalspesifikke rettigheter

Rett til innsyn i egen journal

Pasienten har som hovedregel rett til innsyn i journalen med bilag, og har også rett til å få kopi. Med bilag menes røntgenbilder, pleieplaner, kardex, modeller og annet som ikke føres direkte i journalen. Ved bruk av elektronisk journal, gis det papirutskrift av journalopplysningene.

Pasienter har etter forespørsel krav på en enkel og kortfattet forklaring av faguttrykk og lignende som er brukt i journalen. I flg. Pasientrettighetsloven § 3-5 skal informasjon som gis pasient og pårørende være tilpasset deres individuelle forutsetninger. Blinde og døvblinde personer trenger bistand for å kunne utøve innsynsretten, andre kan ha behov for tolk. Kostnadene ved dette skal dekkes som en del av det ordinære tjenestetilbudet.

Det skal noteres i journalen at det er gitt innsyn eller sendt kopi av journal. Innsyn i journal omfatter også innsyn i logg over hvem som har vært inne i journalen.

Rett til å få rettet og til å få slettet journalopplysninger

Etter pasientrettighetsloven § 5-2 har pasienten eller den opplysningene gjelder rett til å kreve at opplysninger i journalen rettes eller slettes etter reglene i helsepersonelloven §§ 42,43, 44.

- **Retting** (helsepersonelloven § 42): Feilaktige, mangelfulle eller utilbørlige opplysninger eller utsagn i en journal kan rettes ved at journalen føres på nytt eller ved at det gjøres en datert tilføyelse i journal.
- **Sletting** (helsepersonelloven § 43): Hvis det er ubetenkelig ut fra allmenne hensyn, kan feilaktige eller misvisende opplysninger som føles belastende for den de gjelder, slettes. Det samme gjelder opplysninger som åpenbart ikke er nødvendige for å gi pasienten helsehjelp.

Hvis journal er ført på feil person, kan den journalansvarlige av eget tiltak eller etter krav fra den opplysningene gjelder, iflg helsepersonelloven § 44 slette journal eller opplysninger/utsagn i en journal, hvis ikke allmenne hensyn tilsier at sletting ikke kan foretas (for eksempel hvis opplysningene trengs i en tilsynssak).

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 10 av 25

Rett til å få sperret journalopplysninger

Enkelte pasienter krever/ønsker at enkeltpersoner/avdelinger/andre helseinstitusjoner ikke skal ha tilgang til hele eller deler av deres journal. Dette kalles å sperre journalen, og pasienten har rett til dette, selv om det kan gå på tvers av hensynet til faglig forsvarlighet. Vurdering av om journal skal sperres er en oppgave for den journalansvarlige.

Pasienten må selv ta ansvar for risikoen forbundet med at helsepersonell ikke får tilgang til relevante opplysninger. Dette forutsetter at pasienten informeres om konsekvensene det kan få ved å sperre hele eller deler av journalen. Vedkommende må ha nådd helserettslig myndighetsalder på 16 år og ha sine åndsevner i behold for å kunne kreve sperring. Det må journalføres hvilken informasjon pasienten har fått, og hvilket standpunkt pasienten har tatt, slik at det klart fremgår om hele eller deler av journalen skal sperres, evt. hvilke enkeltpersoner/avdelinger/andre helseinstitusjoner som ikke skal få tilgang.

Opplysninger kan unntaksvis utleveres, selv om pasienten har fått sperret hele eller deler av sin journal.

At en journal er sperret betyr at pasienten selv har lagt begrensninger på bruk av taushetsbelagte opplysninger om seg for helsepersonell som yter helsehjelp, men journalen/ journalopplysninger kan brukes til andre formål uten pasientens samtykke:

- Iflg.hpl § 23 nr. 5 kan taushetsbelagte opplysninger gis videre hvis det er fastsatt i lov eller i medhold av lov at taushetsplikt ikke skal gjelde.
- Opplysninger til virksomhetens ledelse og til administrative systemer, hpl. § 26
- Opplysninger om en avdød kan gis videre hvis vektige grunner taler for dette, og nærmeste pårørende har rett til innsyn i journal etter en persons død hvis ikke tungtveiende grunner taler mot det (hpl. § 24).

Andre unntak fra sperringen omfatter opplysninger underlagt opplysningsplikt og meldeplikt, idet utlevering skjer uavhengig av pasientens samtykke. Disse omfatter:

- Tilsynsmyndighet, nødetater, sosialtjenesten, barneverntjenesten og offentlige myndigheter i forbindelse med førerkort og sertifikat har iflg helsepersonelloven kap. 6 krav på visse opplysninger. I slike tilfeller er det ikke opp til helsepersonell å foreta avveininger.
- Helsepersonell har plikt til å gi melding om fødsler og dødsfall, og plikter iflg helsepersonelloven kap 7 å gi opplysninger til helseregistre opprettet og godkjent av Kongen.
- Betydelig personskade voldt på pasient i helseinstitusjon skal iflg lov om spesialisthelsetjenesten § 3-3 rapporteres til Helsetilsynet i fylket.

Utlevering til forskning vil som hovedprinsipp kreve samtykke, men kan også i tilfeller ved dispensasjon og egne instruksjoner kunne utleveres til forskning uten samtykke.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 11 av 25

5. Sikkerhetsorganisering og ansvar

En viktig del av sikkerhetsarbeidet er å avklare ansvars- og myndighetsforhold knyttet til bruk av informasjonssystemet, dokumentere disse og gjøre dem kjent. Særlig viktig er det å avklare operativt ansvar for drift av informasjonssystemet og operativt ansvar for å følge opp sikkerhetsarbeidet. Operativt ansvar for drift er en utøvende funksjon som omfatter å sikre at informasjonssystemet fungerer som besluttet. Operativt ansvar for å følge opp sikkerhetsarbeidet er en kontrollerende funksjon som omfatter etterprøving av at informasjonssystemet benyttes som besluttet.

Sikkerhetsorganisasjonen skal forvalte og styre organiseringen av sikkerhetsarbeidet, og bør baseres på tverrfaglig samarbeid.

5.1. Oversikt over funksjoner

Med dette som utgangspunkt skal foretakene etablere en sikkerhetsorganisering som minimum består av følgende funksjoner:

- Administrerende direktør/daglig leder
- Systemeier
- Informasjonssikkerhetsleder
- Personvernombud⁹
- Leder med personalansvar
- Bruker/medarbeider
- IKT-drift/databehandler

Med sikkerhetsorganisering menes oppgaver og ansvar med betydning for informasjonssikkerheten og er ikke en egen organisasjon. Nevnte funksjoner skal ivareta sikkerhetsansvaret som en del av sitt totale ansvar.

5.2. Funksjonsbeskrivelser¹⁰

Administrerende direktør (AD)/daglig leder

- er databehandlingsansvarlig for all behandling av personopplysninger herunder ansvarlig for å bestemme formålet med databehandlingene og ha dokumentert oversikt over disse
- har det overordnede ansvar for informasjonssikkerheten og skal sikre at tjenester er tilgjengelig for å gjennomføre tiltak
- har ansvar for at dette styringssystemet for informasjonssikkerhet blir implementert og vedlikeholdt
- er ansvarlig for organiseringen av sikkerhetsarbeidet
- har ansvar for at det fastsettes akseptabelt risikonivå som minimum tilfredsstillende kravene i dette styringssystemet
- har ansvaret for at det finnes et definert regime for tilgang til helse- og personopplysninger.

⁹ Dersom virksomheter velger å etablere personvernombud, vil vedkommende være en del av virksomhetens sikkerhetsorganisering.

¹⁰ Funksjonsbeskrivelsene er begrenset til sikkerhetsmessige aspekter.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 12 av 25

Systemeier

- har ansvar for å stille krav til tilgjengelighet, konfidensialitet, integritet og kvalitet for det system vedkommende er systemeier for, slik at det oppfyller lovbestemte og andre krav
- definerer tilgangsroller for sitt system innenfor rammene gitt av AD og gjøre disse kjent
- skal sørge for at det inngås skriftlige avtaler med IKT-leverandør/databehandler med krav til tjenestenivå og forvaltning
- er ansvarlig for formalia i forhold til konsesjon/meldeplikt
- skal sørge for at nødvendig opplæring blir gitt
- overvåker risiko forbundet med informasjonsbehandling og forestå risikovurdering ved behov

Informasjonssikkerhetsleder

- Har det utøvende ansvar for virksomhetens sikkerhetsarbeid bl.a. gjennom å
 - forberede ledelsens årlige gjennomgang av bruk av informasjonssystemet og følge opp iverksetting av tiltak som er besluttet etter gjennomganger
 - lage årlig revisjonsplaner og forestå gjennomføring av sikkerhetsrevisjoner i virksomheten
 - vurdere rapporterte avvik og meddele avvik til virksomhetens ledelse i samsvar med rutine for avviksbehandling
 - forestå gjennomføring av risikovurderinger
- drive opplysningsvirksomhet i foretaket mhp informasjonssikkerhet
- være rådgiver i sikkerhetsspørsmål
- utvikle og vedlikeholde overordnede styrende dokumenter innen ansvarsområde
- ansvarlig for å påse utvikling og vedlikehold av beredskaps-/varslingsplaner (katastrofeplan), samt kontinuitetsplaner relatert til IKT
- iverksette og delta i revisjoner, risikovurderinger og egenkontroll
- avgjøre om nye løsninger eller endringer er innenfor akseptabelt risikonivå
- stille krav til nye/endrede sikkerhetsløsninger ved IT drift, både for etablerte og nye behov som oppstår ved at nye IKT-løsninger innføres
- påse at avvikhåndtering, forbedringsprosesser og vedlikehold av informasjonssikkerheten gjøres i alle ledd, heri om nødvendig å gi pålegg
- iverksette korrektive og andre sikkerhetsrelaterte tiltak
- bistå og tilrettelegge i relevante tilsynssaker

Personvernombud

Med hjemmel i personopplysningsforskriften § 7-12 kan virksomheten utpeke et personvernombud (PVO). PVO må være uavhengig, dvs ha en selvstendig rolle, som ikke begrenses i organisasjonen med hensyn på sine oppgaver. Dersom Datatilsynet samtykker i utnevnelsen av PVO ved et vedtak, gjøres det unntak fra meldeplikt etter personopplysningsloven § 31 første ledd.

PVO har i oppgave å sikre at den behandlingsansvarlige følger personopplysningsloven med forskrift. Personvernombudet skal også føre en oversikt over opplysningene som nevnt i personopplysningsloven § 32, se Datatilsynets web-sider for detaljer om oppgaver.

Det er viktig å være klar over at opprettelse av personvernombud ikke fritar databehandlingsansvarlig for sitt ansvar for at reglene i personopplysningsloven overholdes.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 13 av 25

Leder med personalansvar

Enhver leder er ansvarlig for informasjonssikkerhet innen egen organisasjonsenhet. Ledere skal sørge for at underlagte enheter og ansatte der det er relevant:

- er kjent med og etterlever sitt ansvar, virksomhetens styringssystem for informasjonssikkerhet og sikkerhetsbestemmelser som er relevante
- gjennomfører tilstrekkelig sikkerhetsopplæring av eget og innleid personell, slik at disse har en forståelse av hva som er forventet av dem
- innhenter taushetserklæringer for alle ansatte og innleid personell og påser at disse er kjent med og etterlever styrende dokumenter som regulerer brukeratferd
- tildeler og kontrollerer personellens tilgang til informasjon etter fastsatt tilgangsregime
- rapporterer og formaliserer registre, prosjekter og øvrige databehandlinger inneholdende person- og helseopplysninger i ht virksomhetens rutiner
- følger opp det daglige sikkerhetsarbeidet gjennom et etablert system for avviksbehandling, nødvendige kontroller og iverksette relevante tiltak
- er ansvarlig for resultater, fremdrift og rapportering av sikkerhetsarbeidet innen eget ansvarsområde
- er ansvarlig for at beredskapsplaner ved bortfall av informasjonssystemer finnes

Bruker/medarbeider:

Den enkelte medarbeider er ansvarlig for å:

- følge virksomhetens sikkerhetsbestemmelser inkludert sikkerhetsinstruks
- ha en forståelse av hva som er forventet av dem (adferd)
- søke informasjon ved usikkerhet eller tvil
- forhindre eller rapportere hendelser som kan innebære avvik
- rapportere avvik når disse oppstår til nærmeste leder eventuelt sikkerhetsleder

Enhver ansatt oppfordres til å bidra aktivt med synspunkter og komme med forslag til forbedringer knyttet til sikkerhet.

IKT-drift/databehandler

IKT-drift/databehandler har ansvar for at virksomhetens informasjonssystem er tilgjengelig og at det oppfyller lovbestemte og andre krav samt fungerer som besluttet. Dette inkluderer å

- overvåke risiko forbundet med informasjonsbehandling og forestå risikovurderinger ved behov
- utarbeide beredskapsplan for IKT-området
- følge opp partnere, leverandører og andre databehandlere som har betydning for informasjonssikkerheten
- håndtere meldte avvik
- å sørge for at bruk av personopplysninger begrenses til det som er avtalt
- sørge for å utvikle og etterleve driftsdokumentasjon
- sørge for å utvikle og etterleve dokumentasjon for konfigurasjons- og endringskontroll
- å etablere tiltak for å hindre uautorisert bruk og adgang til informasjonssystemene
- å etablere tiltak for å registrere sikkerhetsavvik, hindre forsøk på uautorisert bruk og tilhørende avvikshåndtering
- å etablere tiltak for å motstå angrep fra ondsinnet programvare

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 14 av 25

6. Gjennomføring av risikovurdering og beskrivelse av tiltak

Risikovurdering skal gjennomføres ved alle endringer som kan ha betydning for informasjonssikkerheten. Risikovurderingen gjennomføres som en stegvis prosess. I det følgende beskrives disse.

6.1. Forberedelsesfasen

Beskrivelse av informasjonens og/eller funksjonens sikkerhetsbehov

Kort beskrivelse av informasjonens og/eller funksjonens sikkerhetsbehov. Hvilket formål og eventuell hjemmel for behandlingen. Det må komme frem om, hvor og hvilke type (sensitive/ikke sensitive) personopplysninger som behandles. I hvilken grad og hvordan informasjonen er kritisk for virksomheten. Videre må det tydeliggjøres hvilke sikkerhetsbehov som er relevant, dvs konfidensialitet, integritet og tilgjengelighet.

Beskrivelse av aktører og informasjonsflyt

Beskriv hvilke aktører som vil behandle informasjonen, inkludert bruk av databehandler. Beskriv eventuelt hvordan informasjonen vil bli overført mellom disse.

Beskrivelse av informasjonssystemet

Angi hva systemet heter og hvilke funksjoner det dekker. Beskriv (hvis relevant) hvilke roller som er etablert for å forvalte systemet, eks systemeier, fagansvarlig, systemforvalter, driftsansvarlig, opplæringsansvarlig og superbrukere. Beskriv kortfattet system som brukes i databehandlingen. Hvor er system(ene) plassert, hvor sitter brukerne, angi størrelse på system. Beskriv eksisterende sikkerhetsmekanismer.

Beskrivelse av, og begrunnelse for endring av informasjonssystemet

Beskriv kortfattet hvorfor opprettelsen eller endringen må gjennomføres, hvordan utførelsen eller utformingen av informasjonssystem er foreslått endret/opprettet. Hvem som har ansvar for utførelse. Angi tidsperspektiv.

Avgrensning av risikovurdering

Risikovurderingen skal omfatte de databehandlinger av helse- og personopplysninger som er berørt. Ved avgrensningen skal grenseflater mot andre databehandlinger, systemer og risikovurderinger beskrives.

6.2. Gjennomføring

Gjennomføring av selve risikovurderingen skal gi en vurdering av om uønskede hendelser kan inntre, hvilken sannsynlighet for at dette skjer med påfølgende konsekvens, og om dette er innenfor eller utenfor akseptabelt risikonivå. Dette vil danne grunnlaget for å avklare om det er behov for nye eller endrede sikkerhetstiltak.

Hendelser er tilstander eller handlinger med en **årsak** og med **virkning** i forhold til behovet for konfidensialitet, tilgjengelighet eller integritet. Hendelser beskrives ved å angi årsak og virkning. Det er viktig å skille klart mellom årsak og virkning – bla. for å sikre at alle sentrale virkninger blir vurdert, og ikke kun en lang rekke årsaker knyttet til den samme virkningen.

Årsak beskrives gjennom å angi situasjoner som forårsaker hendelsen. Årsak er således et spørsmål om hvordan, og – i forlengelsen av dette – et spørsmål om hvem. Beskrivelser av årsaker er grunnlaget for vurdering av sannsynlighet for sikkerhetsbrudd.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 15 av 25

Virkning beskrives i forhold til behovet for sikring av konfidensialitet, tilgjengelighet og integritet. En naturlig inndeling for beskrivelse av virkning er:

- **utlevering/oppdaget** – som er påvirkning av behovet for konfidensialitet gjennom utilsiktet utlevering av opplysninger. Utleveringen oppdages tidsnok til at det kan iverksettes tiltak for å begrense skade.
- **utlevering/uoppdaget** – som er påvirkning av behovet for konfidensialitet gjennom utilsiktet utlevering av opplysninger. Utleveringen oppdages ikke tidsnok til at tiltak kan iverksettes.
- **utilgjengelig/tidsbegrenset** – som er påvirkning av behovet for tilgjengelighet ved at opplysninger er utilgjengelig innenfor et tidsrom.
- **utilgjengelig/permanent** – som er påvirkning av behovet for tilgjengelighet ved at opplysninger er utilgjengelige for alltid.
- **feil/gjenopprettelig** – som er påvirkning av behovet for integritet ved at opplysninger er feil, men hvor feilen kan gjenopprettes.
- **feil/uopprettelig** – som er påvirkning av behovet for integritet ved at opplysninger er feil, og hvor feilen ikke kan gjenopprettes.

Beskrivelser av virkninger er grunnlaget for vurdering av konsekvens av sikkerhetsbrudd.

En virkning kan ha flere årsaker, og en årsak kan gi opphav til flere virkninger. Spesielt, når en hendelse har flere årsaker, skal det beskrives de forskjellige årsakene, siden disse vil inntreffe med forskjellige sannsynligheter. Årsakene skal være beskrevet med relevans i den konkrete situasjon.

Bestem sannsynligheten for at hendelsene kan oppstå og klassifiser i følge tabellene Vedlegg 3 og Vedlegg 4. Under "Konsekvens" og "Sannsynlighet" må det skrives en begrunnende tekst, slik at det er mulig for andre å forstå og følge begrunnelsen og eventuelle forutsetninger i ettertid. Angi spesielt systemtekniske og/eller organisatoriske sikkerhetsmekanismer som underbygger konklusjonen for angitt "Konsekvens" og "Sannsynlighet". I de tilfeller hvor kriteriene for frekvens og/eller tiltak er like for sannsynlighet, må valget av verdi begrunnes eksplisitt, se Vedlegg 3.

Avgjør til slutt om risikoen ligger utenfor akseptkriteriene. I så fall må det iverksettes tiltak. Det kan være ønskelig å iverksette tiltak også for hendelser som ligger innenfor akseptkriteriene.

Hendelser		Konsekvens Beskrivelse og klassifisering K1, K2, K3, K4)	Sannsynlighet Beskrivelse og klassifisering (S1, S2, S3, S4)	Utenfor akseptkri- terier (Ja/Nei)
Årsak	Virkning			
1.				
2.				
3.				
4.				

Figur 3: Enkel oversikt over detaljer i risikovurdering

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 16 av 25

Der risikoen ligger utenfor akseptkriteriene, skal forslag til tiltak som vil gjøre risiko akseptabel angis. Gi en forklaring for hvorfor de foreslåtte tiltak vil være dekkende. Disse kan bestå av både systemtekniske og organisatoriske tiltak.

Tiltakene må gjennomføres for at løsningen oppnår et akseptabelt risikonivå og er i samsvar med styringssystem for sikkerhet.

Bestem tiltak for å redusere risikoen til, i første omgang, de uønskede hendelser som ligger utenfor akseptkriteriene. Lag plan for gjennomføring av tiltak. Angi ansvar for utførelsen.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 17 av 25

7. Sikkerhetsinstruks

Det er etablert et minimum av hva som må legges inn i virksomhetens sikkerhetsinstruks. Denne vil måtte detaljeres og tilpasses den enkelte virksomhet avhengig av tjenester og funksjoner som tilbys og tillates, samt organisatoriske og tekniske løsninger.

Minimumskrav til innhold i instruks er gitt i Vedlegg 5.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 18 av 25

Vedlegg 1. Definisjoner

Emne	Definisjon
Autorisert tilgang	(Innen IKT) Godkjent og tildelt tilgang til et eller flere informasjonssystemer.
Behandling av helseopplysninger	Enhver formålsbestemt bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter.
Databehandler	En juridisk enhet som behandler personopplysninger på vegne av den behandlingsansvarlige.
Databehandlingsansvarlig	Den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes.
Forsettlig, ref Vedlegg 3	Hendelsen skjer ved en bevisst handling hvor en har kunnskap om at det som gjøres kan forårsake et sikkerhetsbrudd.
Helseopplysninger	taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson.
Helseregisterloven	Lov om helseregistre og behandling av helseopplysninger, LOV 2001-05-18 nr 24.
Informasjonssystemet	Samlebetegnelse på alt PC-utstyr, systemer og nettverkskomponenter som inngår i virksomhetens elektroniske databehandling.
Integritet	Å sikre at informasjonen og behandlingsmetodene er nøyaktige og fullstendige.
Kompromittering	Brudd på konfidensialitet, tilgjengelighet eller integritet.
Konfidensialitet	Å sikre at informasjonen er tilgjengelig bare for dem som har autorisert tilgang.
Overlegg, ref Vedlegg 3	Systematisk eller planlagt aktivitet som kan medføre et sikkerhetsbrudd.
Personopplysninger	Opplysninger og vurderinger som kan knyttes til en enkeltperson.
Personopplysningsforskriften	Forskrift til personopplysningsloven, 15. desember 2000 nr. 1265.
Personopplysningsloven	Lov om behandling av personopplysninger, 14. april 2000 nr. 31.
Sensitive personopplysninger	Opplysninger om: <ul style="list-style-type: none"> - rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning. - at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling. - helseforhold. - seksuelle forhold. - medlemskap i fagforeninger.
Sikkerhetshendelse	En hendelse som får konsekvenser for informasjonssikkerheten i virksomheten.
Tilgjengelighet	Å sikre autoriserte brukeres tilgang til informasjon og tilhørende ressurser ved behov.
Uaktsomhet, ref Vedlegg 3	Hendelsen skjer ved uhell, feil, tilfeldighet, ukyndighet eller tilsvarende som kan medføre et sikkerhetsbrudd.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 19 av 25

Vedlegg 2. Forklaring på tabellene i Vedlegg 3 og Vedlegg 4

1. Tabell for vurdering og tallfesting av sannsynlighet, med følgende kolonner:
 - a. Angivelse av konklusjon på vurdering angitt ved
 - i. verdier fra 1 til 4
 - ii. tekstlig beskrivelse av hva hver verdi gir av sannsynlighet
 - b. Alternativ 1 – *Frekvens* – for vurdering av sannsynlighet. Denne baseres på erfaringsgrunnlag og vil i stor grad benyttes i fm vurdering av tilgjengelighet og eventuell sannsynlighet for tap.
 - c. Alternativ 2 – *Letthetsvurdering* – for vurdering av sannsynlighet. Denne baseres på for hhv eksterne, interne uautoriserte og autoriserte en kombinasjon av vurdering av:
 - i. Hvilke motivering som skulle resultere i hendelsen
 - ii. Hvilke ressurser som skal til for at hendelsen skal inntre
 - iii. Vurdering av eksisterende tiltak

2. Tabell for vurdering og tallfesting av akseptabel risiko for konsekvens, med følgende kolonner:
 - a. Angivelse av konklusjon på vurdering angitt ved
 - i. verdier fra 1 til 4
 - ii. tekstlig beskrivelse av hva hver verdi gir av konsekvens
 - b. Beskrivelse av konsekvensen for de ulike aspekter som må vurderes. Dette omfatter vurdering av konsekvens:
 - i. for helsehjelpen
 - ii. i forholdet til individet
 1. pasienten
 2. personvernet
 - iii. for helsevesenet
 - iv. for virksomheten/personellet

Dette vil danne felles grunnlag for vurdering av sannsynlighet og konsekvens ved gjennomføring av risikovurderinger.

Instruks: Gjennomføring av konsesjon/melding ved behandling av personopplysninger				
Dato: 15/9-2003	Utarbeidet av:	Dato: 1/10-2003	Godkjent av: ?????	Side 20 av 25

Vedlegg 3. Vurdering av sannsynlighet

Akseptabel Risiko – Sannsynlighet						
Vurdering:	Frekvens	Letthet (motivering, ressurser og kunnskap)			Eksisterende tiltak	
		Ekstern	Uautorisert intern	Autorisert intern		
4	Svært høy sannsynlighet	Hendelsen inntreffer flere ganger årlig	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes små ressurser uten kjennskap til sikkerhetstiltak uaktsomt 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes små ressurser uten kjennskap til sikkerhetstiltak uaktsomt 	Ikke relevant	Sikkerhetstiltak er ikke etablert eller fungerer ikke etter hensikten
3	Høy sannsynlighet	Hendelsen inntreffer årlig eller sjeldnere	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes kjennskap til sikkerhetstiltak forsettelig 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes uten kjennskap til sikkerhetstiltak uaktsomt 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes uten kjennskap til sikkerhetstiltak uaktsomt 	Sikkerhetstiltak er ikke etablert eller fungerer ikke etter hensikten
2	Moderat sannsynlighet	Hendelsen inntreffer sjeldnere enn årlig	<ul style="list-style-type: none"> god kompetanse evt benytte særskilt utstyr/ program inngående kjennskap til sikkerhetstiltak overlegg 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes kjennskap til sikkerhetstiltak forsettelig 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes uten kjennskap til sikkerhetstiltak forsettelig 	Sikkerhetstiltak er etablert og fungerer etter hensikten
1	Lav sannsynlighet	Hendelsen inntreffer sjeldnere enn årlig	<ul style="list-style-type: none"> god kompetanse evt benytte særskilt utstyr/ program inngående kjennskap til sikkerhetstiltak overlegg 	<ul style="list-style-type: none"> god kompetanse evt benytte særskilt utstyr/ program inngående kjennskap til sikkerhetstiltak overlegg 	<ul style="list-style-type: none"> normal kompetanse uten at særskilt utstyr/ program må benyttes uten kjennskap til sikkerhetstiltak forsettelig 	Sikkerhetstiltak er etablert og fungerer etter hensikten

Vedlegg 4. Vurdering av konsekvens

Akseptabel Risiko – Konsekvens						
FOKUS:		Helsehjelpen	Forholdet til individet		Helsevesenet	Helseforetaket og helsepersonellet
			Forholdet til pasienten	Personvernet		
4	Katastrofal konsekvens	Hendelsen medfører uforsvarlig helsehjelp og manglende sikkerhet (for å unngå personskade) for pasienten	Hendelsen medfører manglende respekt for den enkeltes liv, integritet eller menneskeverd	Hendelsen medfører tap av liv, vedvarende helsetap, betydelig og uopprettelig økonomisk tap eller alvorlig tap av anseelse /integritet.		
3	Stor konsekvens	Hendelsen medfører helsehjelp med utilstrekkelig kvalitet	Hendelsen medfører manglende tillit mellom pasient og helsevesen/-personell	Hendelsen medfører helsetap, uopprettelig økonomisk tap eller alvorlig tap av anseelse/integritet.	Hendelsen medfører helsetjeneste med utilstrekkelig kvalitet	Hendelsen medfører fengselsstraff, inndragning av autorisasjon, lisens eller spesialistgodkjenning eller stengning av helseinstitusjon.
2	Moderat konsekvens	Hendelsen medfører helseopplysninger med utilstrekkelig kvalitet.	Hendelsen medfører at personlig integritet og privatlivets fred ikke ivaretas	Hendelsen medfører betydelig økonomisk tap som kan gjenopprettes eller tap av anseelse/integritet gjennom kompromittering av krenkende opplysninger	Hendelsen medfører helsehjelp med utilstrekkelig kvalitet	Hendelsen medfører bøtestraff, suspensjon av autorisasjon, lisens eller spesialistgodkjenning, erstatningsansvar eller tvangsmulkt
1	Liten konsekvens			Hendelsen medfører økonomisk tap som kan gjenopprettes eller tap av anseelse gjennom kompromittering av følsomme opplysninger	Hendelsen medfører manglende informasjon / kunnskap om sykdomsforhold i befolkningen	Hendelsen medfører administrativ reaksjon, herunder advarsel fra helsetilsynet

Vedlegg 5. Minimum innhold i sikkerhetsinstruks

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. Brukerne er selv ansvarlig for å gjøre seg kjent med og følge reglene i denne instruks.

Fysisk adgang

- Den enkelte medarbeider skal, ved hjelp av fysiske sikringstiltak og/eller tilsyn, hindre at uvedkommende får adgang til dokumenter, flyttbare medier og annet utstyr som inneholder opplysninger det gjelder taushetsplikt for.
- Dersom ID kort/nøkler mistes/blir stjålet, må dette straks meldes til <...>.
- Ansatte som slutter eller går ut i permisjon, skal levere nøkkel/nøkkelkort tilbake til <...> dersom ikke annet er avtalt.
- Den som mottar besøkende, er ansvarlig for at disse ikke oppholder seg i avlåste/avspærrede deler av virksomhetens lokaler uten følge av en ansatt.
- Personer som oppholder seg i avlåste/avspærrede deler av virksomhetens lokaler uten følge av ansatt, uten ID-kort eller uten godkjennelse fra leder ansvarlig for området, skal bortvises.

Bruk av virksomhetens informasjonssystemer

Logging

Internett- og nettverkstrafikk blir logget for administrasjon og for å følge opp virksomhetens sikkerhetsretningslinjer. Det betyr at den ansattes aktiviteter på nettet og ved bruk av program blir registrert, og at det er mulig å spore tilbake om det oppdages brudd på virksomhetens retningslinjer. Loggføringen omfatter aktivitet i nettverket, bruk av tjenester og programmer, og spesielt bruk og aktivitet i systemer som inneholder pasientopplysninger. Autorisert personell gjennomgår loggene og iverksetter tiltak om nødvendig. Brudd på virksomhetens sikkerhetsretningslinjer vil rapporteres til nærmeste overordnede.

Om privat bruk (dersom tillatt)

Virksomhetens informasjonssystemer er beregnet og skal primært benyttes for jobbrelevante formål. Eventuell privat bruk skal ikke gå ut over virksomhetsrelaterte oppgaver og funksjoner.

<Eventuell privat bruk må detaljeres instruks for.>

Eierskap og ansvar

Informasjonssystemet og alt tilhørende utstyr, programvare og lagret informasjon (også på klienter), er virksomhetens eiendom og ansvar.

Virksomheten har innsynsrett i all informasjon lagret i informasjonssystemene begrunnet ut fra virksomhetens behov. Dette inkluderer gjennomgang for å avdekke brudd på virksomhetens sikkerhetsretningslinjer. Ved uforutsett fravær vil e-postkassen, personlig hjemmekatalog og lignende kunne åpnes for nærmeste leder sammen med en tillitsvalgt eller annen objektiv part for å hente ut tjenestemessige dokumenter. Det vil dersom mulig, innhentes samtykke fra den det gjelder, men dersom det ikke lar seg gjøre, vil personvernet ivaretas av tillitsvalgt eller annen objektiv part.

IKT-utstyr

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

- Installasjon av alt utstyr og programvare skal gjøres av autorisert personell.
- Bruk av annen programvare utenom det som virksomheten tilbyr som standard programvare, må godkjennes av autorisert personell.

Det skal ikke tilkobles privat utstyr i virksomhetens nett. Dette gjelder også privat PDA, mobiltelefon og fotoapparat.

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 autorisert personell.

Det skal ikke tilkobles separate eksterne forbindelser til virksomhetens nett (for eksempel via ekstra nettverkskort, trådløst forbindelse, modem, ISDN el) uten driftsenhetens godkjenning og medvirkning. Nettverkskort med direkte tilgang til eksterne nett/Internett skal aldri tilkobles.

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 osv) og programvarelisenser til driftsenheten, dersom ikke annet er avtalt.

Pålogging og avlogging, brukernavn, passord og skjermsparer

- Passordet (og eventuelt brikke/kort for fjerntilgang) er den ansattes nøkkel til virksomhetens datasystem og skal ikke oppgis til eller lånes ut til andre. 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 ikke inneholde navn på familiemedlemmer, fødselsnummer eller andre opplysninger som lett lar seg knytte til brukeren.
- Dersom det er 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 før maskinen overlates til andre.

Informasjonshåndtering

Personopplysningsloven (POL) omfatter personvern og gir krav til beskyttelse av Person- og helseopplysninger. Den gjelder helt fra det er registrert enkle opplysninger vedrørende én enkelt person.

- Et personregister er etablert dersom det registreres mer personidentifikasjon enn fødselsår og initialer. Register skal før det opprettes ha håndtert konsesjon eller melding. Behovet for dette sammen med behov for teknisk sikring vurderes av personvernombud/eller annen autorisert.
- For all annen bruk av sensitive personopplysninger og personregistre enn direkte helsehjelp og pålagte meldinger, skal det som hovedregel innhentes samtykke fra de inkluderte.
- Person- og helseopplysninger ved virksomheten 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 daglig arbeid.
- Utskrifter skal hentes umiddelbart.

Lagring (det må etableres rutiner for hvor sensitive personopplysninger kan lagres)

Forsendelse

- Sensitive personopplysninger skal ikke sendes på åpen epost, telefaks eller tilsvarende løsninger uten godkjente sikkerhetsløsninger.
- Dokumenter og lagringsmedia med sensitive personopplysninger skal alltid sendes i gjenlimt konvolutt/forseglet innpakning.
- Avsender er alltid ansvarlig for å forsikre seg om at mottaker er autorisert for opplysningene.

Makulering/sletting av dokumenter

- Dokumenter med person- og helseopplysninger skal makuleres ved avhending.
- Ansatte som slutter, skal rydde i egne filområder og e-post og sikre at all relevant virksomhetsinformasjon blir lagret på relevante kataloger. Driftsenheten vil når ansettelsesforholdet er avsluttet, slette gjenværende informasjon på brukerens områder.
- Ansatte som slutter, skal makulere eller avlevere egne dokumenter i henhold til rutine over.

Kassering/Håndtering av utstyr og lagringsmedier

- Harddisker, minnepinner eller utstyr som inneholder harddisker og andre elektroniske lagringsmedier, skal leveres til driftsenheten for forsvarlig destruksjon.
- Ansatte som slutter skal kassere/håndtere alle lagringsmedia i henhold til rutine over.

Internett

Den ansattes oppslag på Internett kan spores tilbake til virksomheten og den PC/brukerkode oppslaget er utført fra.

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.

<Styrt bruk må eventuelt detaljeres i instruksen.>

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.

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

Massedistribusjon av informasjon skal eventuelt være jobberelatert 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 driftsenheten 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.

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.

Personell og sikkerhet - Sikkerhetsbrudd

Mistenkelige hendelser og observerte sikkerhetsbrudd skal rapporteres til nærmeste leder eller <....>. Hendelser knyttet til at denne sikkerhetsinstruks ikke følges, vurderes som sikkerhetsbrudd. Brudd på sikkerhetsinstruks ses på som mislighold av arbeidsavtalen og virksomhetens styringssystem for sikkerhet, og vil bli behandlet som personalsak. Alvorlige brudd på reglene i sikkerhetsinstruks vil få konsekvenser for ansattes arbeidsforhold samt eventuelt resultere i strafferettslige reaksjoner.