Regional Sikkerhetspolicy

Dokumentadministrator: Åsmund Ahlmann Nyre | Gyldig fra: 31.10.2016 | Revisjon: 2.3
Godkjent av: Paul Gundersen | Revisjonsfrist: 11.04.2018 | ID: 1987

HELSE MIDT-NORGE

Informasjonssikkerhet

Overordnet IKT-policy for Helse Midt-Norge 2016 - 2018

Godkjent av adm.direktør Helse Midt-Norge RHF

den xx.xx.2016

INNHOLDSFORTEGNELSE

2 MÅL OG PRINSIPPER

2.1 GENERELT

Personopplysningsloven med forskrift, Pasientjournalloven med forskrift og helseregisterloven stiller krav om at foretaket gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

Personopplysningsloven er forkortet til Pol.

Helseregisterloven er forkortet til Hrl.

I tillegg er foretakets forvaltning av person- og helseopplysninger regulert i div. annen lovgivning:

- Spesialisthelsetjenesteloven
- Pasientrettighetsloven
- Helsepersonelloven
- Helseforskningsloven
- Internkontrollforskriften
- Arkivloven
- Forvaltningsloven

Dokumentet er forankret i ”Norm for informasjonssikkerhet for helse- og omsorgstjenesten”, se www.normen.no med faktaark og veiledere samt Helse Midt-Norges (HMN) eierstrategi gjennom IKT-strategien.

Sikkerhetspolicien legger føringer for den enkelte HF-direktør for realisering.

På grunnlag av denne sikkerhetspolicyen er det utarbeidet en regional sikkerhetsplan, SP.

2.2 MÅLSETTING

Målsettinger med Regional IKT Policy omfatter:

- Formål med informasjonsbehandlingen
- Definerte mål og strategier for informasjonssikkerhet med hensyn til konfidensialitet, integritet, tilgjengelighet og sporbarhet
- Akseptkriterier for informasjonssikkerhet

2.3 OMFANG

Overordnede mål for informasjonsbehandling og informasjonssikkerhet i forhold til informasjonens tilgjengelighet, konfidensialitet, integritet og sporbarhet er beskrevet nedenfor.

Akseptkriteriene er målbare størrelser på informasjonssikkerheten hvor overskridelse skal medføre tiltak (i forhold til faktisk sårbarhet eller i forbindelse med risikovurderinger).

Sikkerhetspolicyen gjelder for alle brukere av IT-systemer i Helse Midt-Norge.

2.4 GRUNNLAGSINFORMASJON

Databehandlingsansvarlig er helseforetaket ved administrerende direktør.

Databehandler for helseforetakene i Helse Midt-Norge er Helse Midt-Norge IT (HEMIT) eller annen organisasjon eller person som behandler data på vegne av **Databehandlingsansvarlig**.

Personopplysninger kan kun brukes til uttrykkelige angitte formål som er saklig begrunnet i foretakets virksomhet. Et formål er saklig begrunnet når målet med behandlingen er forankret i det daglige virket til foretaket (Pol §§ 8, 9 og 11, Hrl § 11, PJL § 6).

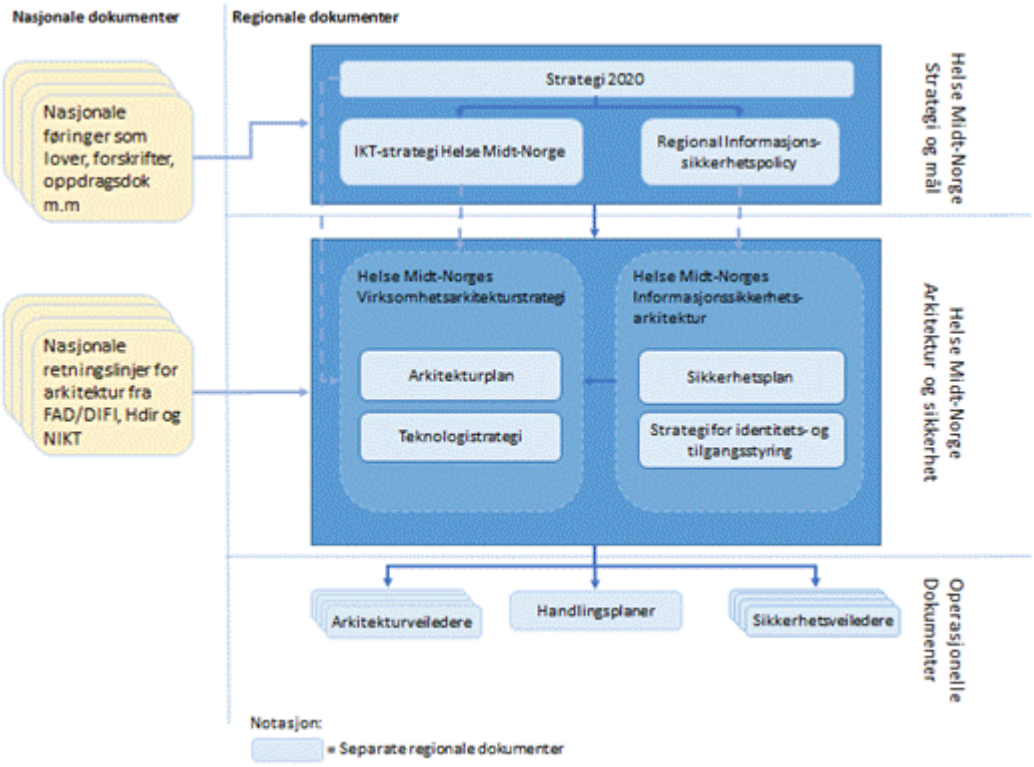
Foretakets oppgaver er definert i lov om spesialisthelsetjenesten og omfatter:

- Behandling av pasienter herunder kvalitetssikring
- Opplæring av pasienter og pårørende
- Forskning
- Utdanning av helsepersonell

I tillegg benyttes personaladministrative registre over ansatte.

2.5 STRUKTUR I PLANVERKET

Helse Midt-Norges regionale sikkerhetspolicy er bygget opp rundt et rolleorientert rammeverk. Policydokumentet er strukturert med et overordnet styrende dokument som beskriver struktur og rutiner (dette dokumentet). Dette dokumentet er ment å gi en relativt statisk beskrivelse av etablerte informasjonssikkerhetskrav i Helse Midt-Norge.



Figur 1Regional informasjonsikkerhetspolicy i Helse Midt-Norge

3 FORMÅLET

Informasjonsbehandlingen i foretaket skal gjennomføres på en sikker og kvalitetsbevisst måte for å opprettholde og styrke befolkningens tillit til foretaket. Dette skjer gjennom u
nderstøttelse av:

- Pasientrettede tjenester
- Undervisning av pasienter og pårørende

- Helseforetakets forskningsaktivitet
- Kompetanseoppbygging og utdanning av helsepersonell ved sykehuset
- Ledelse og administrative tjenester (bl.a. personalsystem)
- Krav til helhetlig og koordinert ytelse av pasientrettede tjenester
- Leveranse av tjenester (sykehusets laboratorier, røntgen, apotek osv.) til eksterne rekvirenter (andre helsepersoner og helseinstitusjoner)
- Ivaretakelse av lovmessige krav (innsyn, arkivering, journalføring, rapportering til sentrale helseregistre, gjennomføring av risikovurderinger ved endringer som har betydning for informasjonssikkerheten og liknende)

4 MÅL OG STRATEGI FOR INFORMASJONSSIKKERHET

4.1 KONFIDENSIALITET

4.1.1 HOVEDMÅL

Personopplysninger ved helseforetaket skal ikke være tilgjengelig for, eller bli kjent for uautorisert personell eller uvedkommende internt eller eksternt. Ved konflikt mellom konfidensialitet og tilgjengelighet skal konfidensialitet vike hvis det påvirker pasientens sikkerhet.

4.1.2 DELMÅL BEHANDLING AV PERSONOPPLYSNINGER

- Personopplysninger som HF er databehandlingsansvarlig for skal kun være tilgjengelig for autorisert personell med tjenestelig behov.
- Utlevering eller overføring av sensitive personopplysninger som HF er databehandlingsansvarlig for, til andre HF eller førstelinjetjenesten, skal kun gjøres på spesifisert forespørsel og med mindre pasienten motsetter seg det, i henhold til relevante lovkrav.
- HF skal sikre at meldinger blir sendt til riktig mottaker.
- Behandling av personopplysninger i pasientjournal og i helseregistre som HF er databehandlingsansvarlig for, skal godkjennes av databehandlingsansvarlig og hjemmel skal foreligge.
- Behandling av personopplysninger som angår ansatte og som HF er databehandlingsansvarlig for, skal godkjennes av databehandlingsansvarlig.
- Databehandlingsansvarlig skal ha kontroll med databehandlers tilgang til sensitive personopplysninger.

4.1.3 DELMÅL FORSKNING

- Alle forsknings- og studentprosjekter som innebærer behandling av person- og sensitive personopplysninger skal godkjennes av personvernombudet og/eller REK[1], eller gis konsesjon fra Datatilsynet.
- Utlevering av person- og sensitive personopplysninger for bruk i forsknings- og studentprosjekter både internt og utenfor foretaket skal godkjennes av databehandlingsansvarlig.
- Juridisk selvstendige parter er selv ansvarlig for å avklare om krav til konsesjon er gjeldende for sin behandling av opplysningene.

4.1.4 STRATEGI FOR BEHANDLING AV PERSONOPPLYSNINGER

- Alle ansatte som gis tilgang til IT-systemer der det behandles personopplysninger skal autoriseres etter gjeldende rutiner. Autorisasjon skal skje på bakgrunn av dokumentert kompetanse i informasjonssikkerhet (signert databrukerkontrakt eller bestått e-læring).
- Endringer og innsyn i behandlingsrettede registre skal kunne følges tilbake til den som utførte endringen og innsynet (logging).
- Helse- og personopplysninger skal prinsipielt lagres på sentrale servere.
  - Lagringsenhet for medisinteknisk som behandler helse- og personopplysninger og ikke lagrer på sentrale servere, skal plasseres i rom med adgangskontroll. Det skal i hvert enkelt tilfelle gjennomføres risikovurderinger.
  - Lagringsenheter tilknyttet videoutstyr som behandler helse- og personopplysninger og ikke lagrer på sentrale servere, skal plasseres i rom med adgangskontroll. Det skal i hvert enkelt tilfelle gjennomføres risikovurderinger. Alle nye fillager på lokalt utstyr skal krypteres, og eksisterende lager skal en vurdere sikker sletting og overføre resten til ett format som kan krypteres.

- Utstyr til avhending skal slettes for personopplysninger ellers bestilles sletting for hos HEMIT.
- Automatisk avlogging tas i bruk som virkemiddel for å ivareta krav til konfidensialitet. Dette kan gå på bekostning av tilgjengelighetskrav. Tid for automatisk avlogging skal nedfelles i avtaleverket for hver enkelt applikasjon og arbeidsstasjon.
- Behandling av personopplysninger skal sikres mot uautorisert innsyn. Kravet må ivaretas også ved tilgang til personopplysninger via hjemmekontorløsning.
- Det skal finnes autorisasjonskontroll til systemer som inneholder personopplysninger.
- Personell, både interne og eksterne, som skal ha adgang til områder hvor det behandles personopplysninger, skal signere taushetserklæring.
- Det skal etableres skriftlige prosedyrer for:
  - tildeling av autorisasjon
  - sletting og kontroll av tildelt autorisasjon
  - tilgang til sensitive personopplysninger for databehandler
  - innsyn i journal og journallogg
  - anonymisering
  - rapportering av avvik
  - behandling av avvik
  - utlevering eller overføring av sensitive personopplysninger
  - bruk av eksterne tjenesteleverandører
  - gjennomgang og oppfølging av logger
  - utfylling og signering av taushetserklæring
- Logging av innsyn i sensitive personopplysninger skal gjennomføres. Det skal etableres prosedyrer for regelmessig gjennomgang av logger, samt for utlevering av logger.
- Logging av bruk av pasientjournalsystemene som helseforetaket er databehandlingsansvarlig for, skal oppbevares like lenge som pasientjournalen. Øvrige logger oppbevares i minst 2 år. Se Normens faktaark 15.
- Ekstern datakommunikasjon av sensitive personopplysninger skal krypteres ihht Normens krav.
- Data lagret på mobile enheter (for eksempel laptop, USB-lager, mobile disker, nettbrett, mobiltelefoner m.m.), skal sikres etter Normens krav (kryptering).
- Dersom det skal etableres fjerntilgang for drift og service av systemer skal alt drifts- og servicepersonell autentiseres ved hjelp av minimum nivå 3 autentisering, før det gis tilgang.
- Alle leverandører som skal gis tilgang til personopplysninger via fjernaksessløsning, må dokumentere tilfredsstillende informasjonssikkerhet i egen organisasjon.
- Tilgang via fjernaksessløsninger til systemer med personopplysninger skal logges, og kommunikasjonen skal være kryptert.
- Ansatte som gis fjerntilgang til IT-systemer skal autentiseres ved hjelp av minimum nivå 3 autentisering.
- Utstyr (for eksempel skjermer eller annet mobilt utstyr) som benyttes ved tilgang til personopplysninger, skal beskyttes mot innsyn fra uautoriserte.

4.1.5 STRATEGI FORSKNING

Forsknings- og/eller studentprosjekter

- skal behandle personopplysninger på bestemte filområder
- som involverer personopplysninger skal ikke igangsettes før godkjennelse av personvernombudet og REK foreligger
- skal oppbevare navnelister med referansenummer nedlåst eller på et annet elektronisk filområde enn de avidentifiserte personopplysningene
- skal foreta anonymisering / sletting av data innen gitt frist i godkjent melding / konsesjon
- skal sikre personopplysninger og avidentifiserte personopplysninger mot uautorisert innsyn

4.2 INTEGRITET

4.2.1 HOVEDMÅL

Alle personopplysninger ved helseforetaket skal til enhver tid være relevante, korrekte, oppdaterte og et resultat av autoriserte og kontrollerte aktiviteter.

4.2.2 DELMÅL PASIENTBEHANDLING

- Det skal være samsvar mellom informasjonen ved informasjonskilden og gjengivelsen av denne informasjonen i helseforetakets behandlingsrettede systemer.
- Alle registreringer, endringer og slettinger i behandlingsrettede systemer skal være et resultat av

autoriserte og kontrollerte handlinger.
- Alle personopplysninger benyttet ved pasientrettede tjenester skal lagres i journalsystem.
- Alle registreringer og endringer i behandlingsrettede registre skal kunne spores til opprinnelse.

4.2.3 DELMÅL FORSKNING

Forsknings- og/eller studentprosjekter
- som oppretter registre skal lagre disse på sentrale filområder for forskning
- skal rette eller slette uriktige eller ufullstendige opplysninger
- skal slette opplysninger som det ikke er gitt formell godkjenning til å behandle

4.2.4 STRATEGI PASIENTBEHANDLING

- Registre med personopplysninger skal lagres på sentrale servere.
- Det skal være etablert prosedyrer for:
  - Dokumentasjon av pasientrettede tjenester.
  - Behandling av avvik.
  - Logging og oppfølging av logger ved behandlingsrettede registre.
- Helse- og personopplysninger som oppstår ved anvendelse av medisinteknisk utstyr (MU) skal lagres på sentrale servere eller utstyrets lager med tilstrekkelig sikring.
  - MU som ikke lagrer personopplysninger på sentrale servere, skal plasseres i rom med adgangskontroll. Det skal i hvert enkelt tilfelle gjennomføres risikovurderinger.
  - MU tilknyttet videoutstyr som behandler helse- og personopplysninger og ikke lagrer på sentrale servere, skal plasseres i rom med adgangskontroll. Det skal i hvert enkelt tilfelle gjennomføres risikovurderinger. Data skal krypteres.
  - MU som HMN ikke har kontroll over, og som knyttes opp mot sentrale servere og/eller felles lagringsmedier, skal plasseres i nettsegment beregnet for dette.
- Endringer ved behandlingstrettede tjenester skal kunne følges tilbake til rett bruker gjennom logging og regelmessig gjennomgang av logger.
- Historikk skal alltid bevares ved endring av informasjon i behandlingsrettede systemer.
- Sletting av informasjon i behandlingsrettede systemer skal skje i tråd med gjeldende lover og forskrifter og i henhold til foretakets prosedyrer.

4.2.5 STRATEGI FORSKNING

- Det skal etableres prosedyrer for retting og sletting av opplysninger registrert i forsknings- eller studentprosjekter.
- Det skal etableres sentrale filområder for forskning med tilgangsstyring i henhold til konsesjonsvilkår.

4.3 TILGJENGELIGHET

4.3.1 HOVEDMÅL

Personopplysninger skal være tilgjengelig og anvendelig for autorisert personell slik at oppgaver kan utføres til planlagt tid. Det skal ikke oppstå personskade pga. svikt i tilgangen på person- og helseopplysninger.

4.3.2 DELMÅL PASIENTBEHANDLING

Kritiske systemer for pasientrettede tjenester skal som hovedregel[2] være kontinuerlig tilgjengelig for sluttbruker.

4.3.3 DELMÅL FORSKNING

Systemer brukt i forskning skal være tilgjengelige på samme nivå som ikke-kritiske systemer.

4.3.4 STRATEGI PASIENTBEHANDLING

- Tekniske løsninger for komponenter som understøtter kritiske systemer for pasientrettede tjenester skal som hovedregel[3] være dupliserte. Ved avvik fra hovedregel skal risikovurderinger legges til grunn.
- Kritiske IKT-system skal være dimensjonert for å ivareta kontinuerlig tilgjengelighet, målt hos sluttbruker.

- Det skal etableres beredskapstiltak for bortfall av kritiske systemer.
- Det skal etableres prosedyrer for sikkerhetskopiering og sikker oppbevaring av disse.

4.3.5 STRATEGI FORSKNING

- Systemer brukt i forskning blir ivaretatt av tjenesteavtaler mellom helseforetak og databehandler.

5 NIVÅ FOR AKSEPTABEL RISIKO

	Indikator	Akseptkriterium
Konfidensialitet	Antall avvik hvor person- og/eller helseopplysninger tilsiktet eller utilsiktet er blitt tilgjengeliggjort for uautoriserte. Antall personer som tilsiktet eller utilsiktet har fått uautorisert tilgang til opplysningene.	Informasjon om pasient eller ansatt skal alltid gis til rett person – null toleranse.
	Forskning Antall avvik hvor forsknings- og studentprosjekter som involverer personopplysninger er igangsatt før godkjennelse av REK foreligger.	**Forskning** Alle forsknings- og studentprosjekter som involverer personopplysninger, skal ikke igangsettes før hjemmel for utlevering er vurdert av klinikk og personvernombud og forhåndsgodkjenning fra REK foreligger – nulltoleranse Navneliste med referansenummer i forsknings- eller studentprosjekter skal oppbevares fysisk atskilt fra de avidentifiserte personopplysningene – nulltoleranse. Anonymisering/sletting av data og backup av data i forsknings- eller studentprosjekter skal foretas innen gitt frist i godkjent melding/konsesjon – nullvisjon.
Integritet / Datakvalitet	**Pasientbehandling** Antall feilbehandlinger av pasienter som følge av feil i pasientdata som har opphav i feil eller mangler ved informasjonssystemer eller i menneskelige feil. Antall awik der det er oppdaget brudd på integritet som har opphav i feil eller mangler ved informasjonssystemer eller i menneskelige feil.	**Pasientbehandling** Feilbehandling av pasienter som følge av feil i helse- og personopplysninger (ikke korrekte eller ufullstendige) skal ikke forekomme - nullvisjon.
	Forskning Antall awik der det oppdages registre i forsknings- eller studentprosjekter som inneholder opplysninger det ikke er adgang til å behandle. Antall awik der det oppdages registre i forsknings- eller studentprosjekter som inneholder opplysninger som er ukorrekte eller ufullstendige.	**Forskning** Uriktige eller ufullstendige opplysninger som er registrert i forsknings- eller studentprosjekter skal alltid rettes eller slettes – nulltoleranse. Opplysninger som er registrert i forsknings- eller studentprosjekter som det ikke er adgang til å behandle skal alltid slettes – nulltoleranse.

Tilgjengelighet	**Pasientbehandling** Antall tilgjengelighetsbrudd på systemer som behandler personopplysninger. Tilgjengelighetsbrudd omfatter også responstid ut over angitt krav. Varighet av nedetid på systemer hvor det behandles personopplysninger. Det skilles mellom planlagt og ikke-planlagt nedetid. Antall tilfeller hvor det har oppstått personskader eller fare for personskade grunnet tilgjengelighetsbrudd.	**Pasientbehandling** Ikke-planlagte avbrudd: Antall ikke-planlagte avbrudd i kritiske systemer skal ikke overstige nivået satt i vedlegg 2 ”SLA krav”, tjenestenivå 1. Planlagte avbrudd: Antall ikke-planlagte avbrudd i kritiske systemer skal ikke overstige nivået satt i vedlegg 2 ”SLA krav”, tjenestenivå 1. Responstid: Ved pålogging: Summen av påloggingstid nettverk og kritiske applikasjoner skal ikke overstige 2,5 minutter[4]. Når pålogget: Krav til responstid for definerte enkeltfunksjoner i kritiske applikasjoner skal nedfelles i avtaleverket for hver enkelt applikasjon. Responstid som overskrider definerte krav, defineres som uplanlagt nedetid. Feilbehandling: Feilbehandling av pasienter som følge av utilgjengelige kritiske IKT-systemer skal ikke forekomme - nullvisjon.
	Forskning Antall tilgjengelighetsbrudd på systemer som benyttes i forskning. Varighet av nedetid på systemer som benyttes i forskning.	**Forskning** Ikke-planlagte avbrudd: Antall ikke-planlagte avbrudd skal ikke overstige nivået satt i vedlegg 2 ”SLA krav”, tjenestenivå 3. Planlagte avbrudd: Antall ikke-planlagte avbrudd skal ikke overstige nivået satt i vedlegg 2 ”SLA krav”, tjenestenivå 3. Responstid: Når pålogget: Krav til responstid for definerte enkeltfunksjoner i applikasjoner skal nedfelles i avtaleverket for hver enkelt applikasjon.
Sporbarhet	**Pasientbehandling** Antall avvik hvor registreringer og endringer av sensitive personopplysninger ikke kan følges tilbake til rett bruker.	**Pasientbehandling** Lesing, oppslag registreringer og endringer av sensitive personopplysninger i behandlingsrettede registre skal alltid kunne følges tilbake til rett bruker – nulltoleranse. Historikk skal alltid bevares ved endring av sensitive personopplysninger i behandlingsrettede systemer – nulltoleranse.

6 SYSTEMATISK FORBEDRINGSARBEID

6.1.1 VEDLIKEHOLD AV POLICY

- Ansvarlig for vedlikehold/revisjon av denne planen er **Regionalt InformasjonssikkerhetsForum, RIF**.
- Planen revideres i forbindelse med sikkerhetsrevisjoner eller reelle hendelser og ved organisatoriske endringer. Årlig gjennomgåelse i RIF-møte i januar.

6.1.2 INTERNREVISJONER

- Regionalt og lokalt planverk skal gjennomgås ved internrevisjoner på lik linje med resten av internkontrollsystemene i HF/RHF.
- RIF kan sette opp revisjonsteam som gjennomfører slike internrevisjoner.
- RIF kan på vegne av helseforetakene gjennomføre 2. partsrevisjon hos databehandler.
- Resultatet av internrevisjonene behandles i RIF.

6.1.3 EVALUERING AV REELLE HENDELSER

- Brudd på denne policy skal behandles i RIF.
- Eventuelle læringspunkter skal tilflyte resten av organisasjonen.

7 VEDLEGG 1 DEFINISJONER

7.1 DEFINISJONER

7.1.1 AUTORISERT PERSONELL

Personell i bestemte roller som er gitt bestemte rettigheter (=autorisasjon) til lesing, registrering, redigering, retting, sletting og/eller sperring av helse- og personopplysninger. Autorisasjon kan bare gis i den grad det er nødvendig for vedkommende sitt arbeid, er begrunnet ut fra tjenstlig behov og er i henhold til bestemmelser om taushetsplikt.

7.1.2 BEHANDLINGSRETTET HELSEREGISTER

Journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger.

7.1.3 DATABEHANDLINGSANSVARLIG / BEHANDLINGSANSVARLIG

Den som bestemmer formålet med personopplysningene og hvilke hjelpemidler som skal benyttes,

7.1.4 DATABEHANDLER

Den som behandler personopplysninger på vegne av databehandlingsansvarlige. Pol §2. Hrl § 2.

7.1.5 MU (TIDLIGERE BENEVNT SOM MTU)

Medisinteknisk utstyr.

7.1.6 LEVERANDØR

Den som, gjennom avtale med databehandler og/eller databehandlingsansvarlig, leverer EMU-/ IKT-løsninger og/eller drift av

løsningene.

7.1.7 FJERNAKSESS

Avtalefestet og styrt tilgang til databehandlingsansvarlig og databehandlers EMU-/IKT-løsninger via eksterne linjer[5].

7.1.8 PERSONVERNOMBUD OG PERSONVERNOMBUD FOR FORSKNINGS- OG STUDENTPROSJEKT

Den som skal vurdere om foreslått behandling av personopplysninger er lovlig. Det betyr i praksis at meldeplikten til Datatilsynet ved behandling av personopplysninger er erstattet med meldeplikt til personvernombudet. For prosjekter som vurderes som konsesjonspliktig sender personvernombudet søknad til Datatilsynet[6].
Personvernombud kan være internt eller eksternt etter avtale med Datatilsynet.
Personvernombud for forsknings- og studentprosjekt kan være internt eller ivaretatt av NSD (Norsk Samfunnsvitenskapelig Datatjeneste).

7.1.9 KRITISKE SYSTEMER

Tilsvarer prioritet 1 i normen (Norm for informasjonssikkerhet i Helsesektoren).

Tilsvarer tjenestenivå 1 i SLA (Service Level Agreement).
Systemer som anvendes i diagnostikk, behandling eller pleie og hvor tapt tilgang gir økt risiko for at tjenesten enten ikke ytes eller må ytes med redusert kvalitet, førende til økt risiko for feil behandling.

7.1.10 IKKE KRITISKE SYSTEMER

Tilsvarer prioritet 5 i normen.

Tilsvarer tjenestenivå 3 i SLA (Service Level Agreement).
Typiske systemer her er systemer for forskning, dvs. systemer som ikke er direkte pasientbehandlingsrelatert.

7.1.11 PRIORITERTE SYSTEMER

Tilsvarer prioritet 2, 3 og 4 i normen.

Tilsvarer tjenestenivå 2 i SLA (Service Level Agreement).
Tjenester hvor stopp i systemet kan få alvorlige konsekvenser f.eks.:

- Betydelig merarbeid for personell.
- Tapt effektivitet.

7.1.12 RESPONSTID

Tiden det tar - målt hos bruker - fra en ”kommando” er gitt til svar på ”kommandoen” er mottatt.

7.1.13 SENTRAL SERVER

Server og lagringsenhet som er plassert innenfor godkjent sikkerhetsregime.

7.1.14 SENSITIVE PERSONOPPLYSNINGER (POL. §2 PKT8)

Personopplysninger som inneholder opplysninger om:

- 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

Pol. §2 pkt. 8

7.1.15 HELSEOPPLYSNINGER

Taushetsbelagte opplysninger i henhold til Helsepersonellovens § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold som kan knyttes til en enkeltperson, Helseregisterlovens § 2 pkt 1.

7.1.16 PERSONOPPLYSNINGER

Opplysninger og vurderinger som kan knyttes til en enkeltperson. Pol. §2 pkt. 2.

7.1.17 AUTENTISERING

Det er definert fire sikkerhetsnivåer, hvor nivå 4 er kvalifiserte sertifikater, for eksempel Bankid. Nivå 3 er HMNs smartkort for pålogging og SMS-autentisering. Nivå 2 er brukernavn og passord, nivå 1 har ingen. For mer info, se: http://www.regjeringen.no/nb/dep/fad/dok/lover-og-regler/retningslinjer/2008/rammeverk-for-autentisering-og-uawiseli/4.html?id=505929
.

7.1.18 SIKKER SONE

De deler av et informasjonssystem som inneholder komponenter hvor det lagres og/eller behandles sensitive personopplysninger. Sikre soner skal være sikkerhetsmessig atskilt fra det øvrige interne nettverket og evt. andre sikre soner samt fra eksterne nettverk.

7.1.19 TILFREDSSTILLENDE INFORMASJONSSIKKERHET

Informasjonssikkerheten er tilfredsstillende når den oppfyller kravene i helseforetakets sikkerhetspolicy, norm for informasjonssikkerhet og norsk lov.

---

[1] De regionale komiteer for medisinsk og helsefaglig forskningsetikk.

[2] Avvik fra hovedregel kan være aktuelt i forbindelse med mindre lokale enheter, slik som distriktsmedisinske sentre, distriktspsykiatriske sentre, små lokale kontor med åpningstid 1 – 2 dager i uken.

[3] Avvik fra hovedregel kan være aktuelt ved mindre lokale enheter som ikke driver akuttbehandling, slik som distriktsmedisinske sentre, distriktspsykiatriske sentre, små lokale kontor med åpningstid 1 – 2 dager i uken.

[4] Forutsetter at klient tilfredsstiller krav fra Hemit.

[5] Se Norm for informasjonssikkerhet i Helsesektoren faktaark 36.

[6] Se også Datatilsynets veileder for personvernombud: http://www.datatilsynet.no/upload/Personvernombud/Veileder%20for%20personvernombud_m_skjema.pdf