NOF

Rutine

for

håndtering av personopplysninger – informasjonssikkerhet – internkontroll

For:

Signert av ansvarlig for virksomheten

Innhold

1. Innledning – virksomhetens policy

Hensikten med denne rutinen er å overholde nye lovpålagte krav til personvern og informasjonssikkerhet i ny personvernlov basert på EU-direktiv, populært kalt GDPR (General Data Protection Regulation) som vil tre i kraft i Norge i 2018. Vedlagt denne rutinen vil det ligge maler og standarder for de viktigste forhold som må dokumenteres i henhold til lovens krav.

Følgende prinsipper legges til grunn for vår behandling av personopplysninger i vår virksomhet:

- Behandlingen skal bare skje i den utstrekning det er nødvendig av hensyn til virksomhetens administrasjon og for vår behandling og oppfølging av pasienter
- Behandlingen skal alltid ha et lovlig grunnlag. Dette innebærer for oss, enten at det er en pasientavtale som gjør det nødvendig å behandle visse opplysninger, eller det er innhentet et skriftlig samtykke fra pasienten. I den grad det registreres og lagres sensitive personopplysninger om pasienten må det alltid innhentes et skriftlig samtykke.
- Virksomhetens behandling av personopplysninger vil alltid foretas innenfor rammene av god informasjonssikkerhet, herunder gode rutiner for håndteringen av personopplysninger.
- Det er et krav at det er et klart formål med den registreringen og lagringen av personopplysninger vår virksomhet foretar. Informasjonen som registreres skal kun anvendes i tråd med formålet med registeringen og på saklig måte i overensstemmelse med virksomhetens behov for opplysningene.

For vår virksomhet er formålet enten at det er nødvendig for å administrere pasientforholdet (altså at det trengs blant annet informasjon om navn og kontaktinformasjon til pasientene) eller at det er nødvendig for å kunne foreta en forsvarlig behandling og oppfølging av pasienten (at det er nødvendig å ha informasjon om helseforhold, medisinering og en del personlige forhold). De sistnevnte opplysninger registreres og lagres i pasientens journal i et fysisk arkiv eller på en datamaskin uten tilgang til nettverk. Vedlegg 1 viser en oversikt over virksomhetens behandling av personopplysninger slik loven krever.

Det er i vår virksomhet etablert en bevisst holdning til behandling av personopplysninger og til den enkeltes behov for tilgang til og håndteringen av slike opplysninger. Før registrering av personopplysninger, vurderes alltid følgende:

- Er det behov for å registrere/lagre personopplysninger om personen i det hele tatt?
- Hvilken informasjon skal og vil være nødvendig å legge inn om vedkommende?
- Hvilken kvalitet har informasjonen?
- Hvem har et «tjenstlig» behov tilgang til opplysningene?

De opplysningene vi registrerer og lagrer skal være korrekte og holdes oppdaterte.

All behandling av personopplysninger i vår virksomhet skal foregå på en slik måte at bare de som behandler vedkommende pasient eller har et annet «tjenstlig behov» for å få innsyn i personopplysningene kan få tilgang på informasjonen. Vår virksomhet skal tilstrebe, i hvert enkelt tilfelle, å gjøre et så lite inngrep i enkeltpersoners personvern som mulig.

Hvordan vi håndterer personopplysninger om pasienten skal beskrives i vår samtykkeerklæring og i vår personvernerklæring. Vår standard samtykkeerklæring følger som vedlegg 2 og vår personvernerklæring som vedlegg 3.

Dersom vår virksomhet inngår en avtale med en IT-leverandør eller andre personer/firma som medfører at vedkommende får tilgang til våre personopplysninger skal vi inngå en såkalt databehandleravtale med vedkommende. Denne avtalen skal blant annet inkludere den tilgang de skal ha til data, relevante sikkerhetskrav og de nødvendige kontroller vi må ha med bruken av data.

2. Informasjonssikkerhet

2.1 Innledning

Vår virksomhet må etter loven sørge for tilfredsstillende informasjonssikkerhet for arkiv og it-utstyr hvor det lagres personopplysninger. Vi skal dokumentere at rutiner og tiltak som sikrer personopplysningene er på plass og blir etterlevd i praksis. Denne rutinen skal ivareta krav til slik dokumentasjon.

Gjøres det endringer i måten vi behandler personopplysninger på, for eksempel dersom vi får ny datamaskin eller nytt saksbehandlingsprogram skal vi alltid først foreta en ny vurdering av hvordan informasjonssikkerheten for våre personopplysninger blir ivaretatt.

Vår virksomhet skal gjennomføre en årlig risikovurdering av om vår informasjonssikkerhet er god nok. Dette for å identifisere risiko for uønskede hendelser som kan ha betydning for personvernet. Med «risiko» menes sannsynligheten for og konsekvensen av at noe uønsket skal hende. Typisk vil vi måtte vurdere risikoen for at de opplysningene vi har lagret kommer på avveier. I risikovurderingen gis en overordnet konklusjon av risikoen. Dersom vår vurdering er at det er en for høy risiko for slike uønskede hendelser, må vi iverksette tiltak for å redusere denne risikoen til et akseptabelt nivå. Dette skal dokumenteres i risikovurderingen. Som vedlegg 4 følger vår risikovurdering.

2.2 Sikkerhetsmål og sikkerhetsstrategi

Våre sikkerhetsmål beskriver hva som ønskes oppnådd sikkerhetsmessig, mens sikkerhetstiltakene beskriver hva som skal gjennomføres for å oppnå sikkerhetsmålene. Våre sikkerhetsmål er styrende for alt arbeid med informasjonssikkerhet. Vi skal kontrollere jevnlig at målene etterleves, herunder at de krav som stilles i lov- og regelverk oppfylles.

Våre mål er følgende:

- Vi har nulltoleranse for brudd på lovverk tilknyttet personvern
- Vi har taushetsplikt for behandling av helseopplysninger og andre personlige opplysninger
- Uautoriserte skal ikke får kjennskap til personopplysninger lagret hos oss
- Vår informasjonsbehandling skal beskyttes mot utenforstående innsyn
- De opplysningene vi lagrer skal være oppdaterte og korrekte
- Opplysninger som ikke lengre er nødvendig for behandling av pasienten skal slettes
- For å sikre mot tap av data skal det tas sikkerhetskopier av lagrede personopplysninger
- Alle som bruker IT-system/utstyr skal ha kompetanse for å ivareta sikkerhetsbehov/krav

For å nå målene skal vår sikkerhetsstrategi inkludere følgende konkrete tiltak:

- Alle dokumenter og lagringsmedia som inneholder personopplysninger, skal behandles, oppbevares og destrueres på en slik måte at det ikke kommer uvedkommende i hender
- Alle elektroniske lagringsmedia som inneholder personopplysninger skal være passord-beskyttet og låse seg ved inaktivitet
- Arkiv eller IT-utstyr som inneholder sensitive personopplysninger skal være innelåst når de er uten tilsyn
- Tilgang til personopplysninger skal kun gis dem med tjenstlig behov
- Alle som skal ha tilgang må ha egen bruker og passord på datamaskin/server
- Sensitive opplysninger skal ikke lagres på ukryptert it-utstyr som tas ut av lokalet
- All tilgang og forsøk på uautorisert tilgang til personopplysninger skal loggføres
- Personopplysninger skal ikke lagres på IT-utstyr med tilgang til nettverk, uten at det er installert nødvendig informasjonssikkerhetstiltak på utstyret
- Alle som får tilgang til sensitive personopplysninger skal signere taushetserklæring

2.3 Nærmere om IT-sikkerhet i vår virksomhet

I vår virksomhet skal lagring av personopplysninger på datamaskin/harddisk eller på annet medium som er koblet til et nettverk, som hovedregel ikke forekomme, med mindre spesielle hensyn tilsier slik lagring og nødvendige sikkerhetstiltak er på plass. Sensitive opplysninger skal lagres på en slik måte at de kun er tilgjengelig for personer som har behov for å behandle slike opplysninger.

Virksomhetens tekniske løsning må sikres på en slik måte at uautorisert personell ikke får adgang til IT-utstyr eller arkiv med personopplysninger, eller på andre måter vil kunne få tilgang til personopplysninger. Dersom en ikke selv har den tekniske kompetansen til å være trygg på at de tekniske løsningene en benytter er sikker nok mot uautorisert tilgang, skal medlemmet sørge for at dette kontrolleres, og at IT-sikkerheten styrkes, av teknisk kyndig personell.

Registreres og lagres sensitive personopplysninger på datamaskin/server, så skal denne tilgangsbeskyttes i form av passord, samt oppbevaring under tilsyn eller i låst rom. Eventuelt mobilt utstyr som bærbare datamaskiner, IPads og smarttelefoner, må også sikres med autentisering (for eksempel passord) for å hindre uautorisert tilgang mv. på samme måte som stasjonært utstyr. Fysiske arkiv med sensitive personopplysninger skal lagres i låste rom når de ikke er under tilsyn. Skal datamaskin/server tilkobles nettverk/internett/e-post, kreves det at særskilte tekniske sikkerhetstiltak er installert på maskinen/utstyret i tillegg (se under).

Når det gjelder tilgangsbeskyttelse kreves det at ingen andre enn den personen hos oss som behandler pasienten, skal ha tilgang til sensitive personopplysninger om helse mv. Unntak kan tillates dersom det må gis tilgang til en annen medarbeider begrunnet i at det er nødvendig for behandlingen («tjenstlig behov»). I så fall skal det opprettes en egen bruker og et eget passord for denne brukertilgangen. Uansett er det bare vår virksomhets medarbeidere, som har underskrevet en taushetserklæring, som kan få tilgang til personopplysningene. Under behandles det særlige tilfellet at en IT-leverandør har tilgang til personopplysninger.

Sensitive personopplysninger skal ikke lagres på bærbar datamaskin eller andre portable/mobile løsninger, uten at dataene på utstyret er kryptert og tilstrekkelig sikret. Det mobile utstyret skal sikres med tilgangskontroll (for eksempel passord) for å hindre uautorisert tilgang mv. på samme måte som på stasjonært utstyr.

Skrivere/kopimaskiner som benyttes til å skrive ut sensitive personopplysninger skal være plassert på steder som er avlåst eller under tilsyn. Alle utskrifter/kopier må hentes med én gang av den personen som skrev ut opplysningene.

Det skal ikke brukes SMS eller e-post til overføring av sensitive personopplysninger eller 11-siffret fødselsnummer.

Særskilte tiltak for lagring på IT-utstyr tilkoblet nettverk

Dersom vi må lagre personopplysninger på en datamaskin/server/mobilt utstyr med tilgang til nettverk/internett eller til eksterne lagringsmedium, skal utstyret sikres mot «hacking» og annen tilgang fra uvedkommende, herunder ha installert virus-/«malware» programmer mv. Dette på grunn av at slikt IT-utstyr kan rammes av ondsinnet programvare som inneholder virus e.l. Det kreves blant annet at tilkobling til eksterne nettverk må sikres med to uavhengige «tekniske tiltak» fra pc/server/utstyr hvor det er lagret sensitive opplysninger. Det vises også til særskilte krav til konfigurasjonskontroll i vedlegg 7. Benyttes trådløse nettverk kreves det også at trådløst nettverk er sikret mot påkobling fra andre.

Sikkerhetskopiering

Virksomheten skal påse at personopplysninger sikkerhetskopieres fortløpende etter en fastsatt prosedyre. Sikkerhetskopiene skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret som er sikkerhetskopiert. Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte.

Sletting ved utfasing av utstyr

Ved utfasing av utstyr (for eksempel kopimaskin, telefaks, multifunksjonsskriver, PC, server mv.) skal virksomheten påse at personopplysninger slettes slik at opplysningene ikke kan gjenskapes. Vanlig sletting av datafiler og formatering er ikke tilstrekkelig. Et godkjent sletteprogram skal benyttes, alternativt kan lagringsmediene ødelegges fysisk.

2.4 Rutiner for uønskede hendelser og håndtering av avvik

Brudd på vår informasjonssikkerhet beskrevet i dette dokumentet og eventuelle andre uønskede hendelser knyttet til lagring av personopplysninger, skal loggføres i avviksskjema (vedlegg 5). Eksempler på situasjoner som skal meldes som avvik:

- Utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Brudd på taushetsplikt
- Når noen benytter informasjonssystemet uten autorisasjon
- Ved feil på utstyr eller program som kan ha innvirkning på informasjonssikkerheten
- Ved behandling av personopplysninger i strid med regelverket, for eksempel når:
    - Samtykke til behandling ikke foreligger
    - Hacking
    - Tap av data
- Personopplysninger blir lagret på IT-utstyr som ikke oppfyller krav til IT-sikkerhet

Sikkerhetshendelser krever ofte en rask reaksjon og må følges opp omgående. Dersom personopplysninger kommer på avveie må en vurdere om Datatilsynet og den registrerte skal varsles.

3. Internkontroll med etterlevelsen

All elektronisk behandling av personopplysninger skal skje på en kontrollerbar måte, slik at det er mulig på ethvert trinn av behandlingen, og i ettertid, å se hva som er behandlet og resultatet av behandlingen.

Virksomheten foreta hvert år en kontroll av at sikkerheten ivaretas og er tilstrekkelig. Kontrollen dokumenteres og vil innebære å:

- kontrollere at det er gjennomført nødvendige sikkerhetstiltak
- verifisere at sikkerhetstiltakene fungerer
- kontrollere at regelverk, inkludert denne retningslinje og rutine, følges i praksis

Inkludert i en slik kontroll vil vi også vurdere om de sikkerhetsmål og –strategier vi har er i varetatt.

Denne rutinen med vedlegg gjennomgås hvert år for å sikre at rutinene er

- oppdaterte i henhold til interne og eksterne forhold,
- hensiktsmessige og
- tilstrekkelige.

Kontroll av etterlevelse av reglene for behandling av personopplysninger innebærer også å:

- Kartlegge omfanget av personopplysninger
- Foreta og oppdatere risikovurdering
- Utføre internkontroll

4. Ivaretakelse av den registrertes rettigheter

Vår virksomhet skal sørge for at de rettigheter som den registrerte har etter den nye loven til å få informasjon om behandlingen av opplysninger og til at opplysningene er korrekte sikres.

Sletting
Vi skal på eget tiltak slette personopplysninger når formålet med behandlingen er oppnådd. Det vil si når opplysningene ikke lenger er nødvendige for formålet de ble samlet inn til.

Personopplysninger om inaktive pasienter skal slettes etter 1 år etter siste behandling/konsultasjon. Dette med mindre pasienten har eksplisitt uttalt at vedkommende vil fortsette behandlingen, eller at det er konkrete grunner for å beholde opplysningene lengre, og det finnes et rettslig grunnlag.

De personer vi har registrert personopplysninger har rett til å kreve at personopplysninger om seg selv slettes, dersom opplysningene ikke lenger er nødvendige for formålet de ble samlet inn for.

Dersom opplysningene som behandles utelukkende er basert på et samtykke fra vår pasient og samtykket trekkes tilbake vil vi normalt måtte slette opplysningene umiddelbart.

Rett til korrigering
De registrerte har, på forespørsel, rett til å få uriktige personopplysninger om seg selv korrigert. I så fall krever vi at det fremmes en skriftlig anmodning med beskrivelse av de opplysningene som hevdes å være feil og med en begrunnelse for hvorfor de er feil.

Informasjon til den registrerte
Som et utgangspunkt vil de privatpersoner som vi har registrert personopplysninger om rett til å bli informert om behandlingen. Det er i utgangspunktet krav til å gi informasjon når opplysningene innhentes fra den registrerte selv og/eller fra andre kilder. Dette gjør vi og i samtykkeerklæringen.

De registrerte skal også ha rett til, på forespørsel, å få mer informasjon om hvordan deres personopplysninger behandles og til å få kopi av de personopplysninger som er lagret.

Informasjonen gir vi i forbindelse med den samtykkeerklæringen som vi ber pasienten signere på ved første konsultasjon, samt i vår personvernerklæring. Vår informasjon til pasienter omfatter følgende:

- Hva slags personopplysninger virksomheten behandler
- Hvilke formål virksomheten bruker personopplysningene
- Hva er det rettslige grunnlaget for virksomhetens behandling av personopplysninger
- Hvem utleverer virksomheten eventuelt personopplysninger til
- Hvor lenge lagres personopplysningene eller kriteriene for å fastsette lagringstid
- Hvilke rettigheter har den registrerte (innsyn, korrigering, sletting, begrensning, protestere, rett til å klage til Datatilsynet).

I vedlegg 6 beskrives nærmere hvilken type informasjon som skal gis innsyn i ved en anmodning.

Svar på henvendelser om innsyn skal gis uten ugrunnet opphold og senest innen 30 dager. Vil det ta lengre tid enn dette skal det gis et foreløpig svar med opplysninger om grunnen til forsinkelsen og sannsynlig tidspunkt for når svar kan forventes.

Vedlegg til dokumentet

Vedlegg 1 – Oversikt over behandling av personopplysninger

Vedlegg 2 – Standard samtykkeerklæring

Vedlegg 3 – Mal personvernerklæring

Vedlegg 4 – Risikovurdering

Vedlegg 5 – Avviksskjema

Vedlegg 6 – Hvilken informasjon vi skal gi til våre pasienter

Vedlegg 7 – Beskrivelse av IT-konfigurasjonskontroll

Vedlegg 8 – Taushetserklæring medarbeidere/brukere