NORMEN

Protokoll over behandlinger av helse- og personopplysninger i virksomheten (faktaark 13)

Versjon 3.0

20.11.2018

Utarbeidet med støtte fra direktoratet for e-helse

Vedtatt av styringsgruppen for Normen

Dette faktaarket er et støttedokument under Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen) som forvaltes av Styringsgruppen for Normen etter Normens forvaltningsmodell. Se mer på www.normen.no

Tema for faktaarket	Virksomhetens leder er ansvarlig for å ha oversikt over behandlinger av helse- og personopplysninger. I dette faktaarket jar vi utarbeidet en eksempel på protokoll for kommunal helse- og omsorgstjeneste. Eksemplene er ikke uttømmende og er utarbeidet som en inspirasjon og veiledning til kommunene. Eksemplene viser de mest sentrale lovpålagte tjenestene i den kommunale helse- og omsorgstjenesten. Det er dataansvarlig og databehandler skal føre protokoll over behandlingsaktiviteter. Dersom relevant, skal også den dataansvarliges representant også føre protokoll over behandlingsaktiviteter som utføres under deres ansvar. Protokollen skal vedlikeholdes kontinuerlig som en løpende aktivitet og skal inneholde detaljert informasjon om alle behandlingsaktiviteter i virksomheten.
Dette faktaarket er spesielt relevant for	Målgruppen for faktaarket er • IKT-ansvarlig • Sikkerhetsleder / sikkerhetskoordinator • Virksomhetens leder/ledelse • Databehandler • Personvernombud
Krav i Normen	Faktaarket gjelder følgende kapittel i Normen • Kapittel 3.3 Oversikt over teknologi og behandling av helse- og personopplysninger
Relevante lov- og forskriftsbestemmelser, standarder og andre rammeverk	Følgende lov- og forskriftsbestemmelser, standarder og andre rammeverk er spesielt relevante for faktaarket: • Personvernforordningen art. 30 Protokoller over behandlingsaktiviteter • Om personvernombud - fra Datatilsynet

Protokoll over behandlinger av helse- og personopplysninger i virksomheten

Alle virksomheter som behandler helse- og personopplysninger skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Den samme plikten gjelder virksomhetenes databehandlere. Denne behandlingsoversikten vil også være nyttig som en del av virksomhetens internkontrollplikt og dokumentasjon av denne.

1. Utforme en protokoll over behandlingsaktiviteter som utføres

Opprett et oversiktsskjema for de ulike behandlingene av helse- og personopplysninger. Protokollen skal være skriftlig, og kan være elektronisk. F.eks. kan vedlagte skjema benyttes som et utgangspunkt og videre tilpasses den enkelte behandlingen av helse- og personopplysninger.

2. Beskriv ytterligere detaljert informasjon for den aktuelle behandlingen av helse- og personopplysninger. For dataansvarlig er minimum følgende:

- Navnet på og kontaktopplysninger til den dataansvarlige og eventuelt felles dataansvarlig
- Databehandlere og databehandleravtaler (med referanse til arkivnr.)
- Evt. felles dataansvar (med tilhørende avtale)
- Navnet på og kontaktopplysninger til personvernombud
- Formålene med behandlingen
- Kategorier av registrerte (eksempelvis pasienter – barn og voksen, klient, bruker av tjenesten, ansatt, helsepersonell, bruker av informasjonssystem)
- Kategorier av personopplysninger (eksempelvis ansattopplysninger, helseopplysninger)
- Kategori av behandlinger (lagring, sammenstilling, utlevering mv)
- Hvorvidt det behandler personopplysninger av særlige kategorier og hjemmelsgrunnlaget for denne typen behandling.
- Mottakere av personopplysninger (eksempelvis NAV, HELFO, reseptregisteret, forsikringsselskap, o.l.)
- Kilder for innhenting av opplysninger (den registrerte selv, registre etc.)
- Eventuell overføring til tredjeland eller internasjonale organisasjoner og bekreftelse på at mottaker følger regulatoriske krav
- Planlagt lagringstid (Vil også omfatte journalføring og arkivering), og sletterutiner
- Beskrivelse av tekniske og organisatoriske sikkerhetstiltak, jf. styringssystemet
- Om det er utarbeidet personvernkonsekvensvurdering og begrunnelse for hvorfor ikke.

3. Beskriv ytterligere detaljert informasjon for den aktuelle behandlingen av helse- og personopplysninger. For databehandler er minimum følgende:

- Navn og kontaktopplysninger til dataansvarlig, eller dens representant som databehandler opptrer på vegne av

- Navn og kontaktopplysninger til personvernombudet hos dataansvarlig
- Kategorier av behandlinger utført på vegne av hver dataansvarlig
- Dersom relevant navn på tredjeland eller internasjonale organisasjoner som personopplysninger overføres til,
    - Dokumentasjon på nødvendige garantier ved overføringer til tredjeland eller internasjonale organisasjoner
- Dersom det er mulig, å gi en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak

4. Kontinuerlig forvaltning av helse- og personopplysningene som behandles

Som en løpende prosess må behandlingsoversikten oppdateres, enten det er en operativ/daglig dataansvarlig/databehandler eller et personvernombud.

- Se vedlegg 1 – Dataansvarliges protokoll over behandlinger av helse- og personopplysninger.
- Se vedlegg 2 – Databehandlers protokoll over behandlinger av helse- og personopplysninger.
- Eksempel på protokoll over behandlingsaktiviteter i kommunal helse- og omsorgstjeneste