

 <p style="text-align: center;">Norm for informasjonssikkerhet www.normen.no</p>	<p>Utgitt med støtte av:</p> 
<h2>Personvern og informasjonssikkerhet i helse- og sosialtjenesten - kortfattet oversikt for kommuneledelsen</h2>	<p><b>Støttedokument Faktaark nr. 44</b> Versjon: 1.1 Dato: 15.12.2010</p>

<p><b>Målgruppe</b></p> <p>Dette faktaarket er spesielt relevant for:</p>	<input type="checkbox"/> Leverandør <input type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input type="checkbox"/> Sikkerhetsleder/sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Øverste leder i kommunen (oftest rådmannen) er hovedansvarlig for personvern og informasjonssikkerhet.		
<b>Gjennomføring</b>	Kontinuerlig aktivitet.		
<b>Formål</b>	Bidra til at kommunenes øverste ledelse kan iverksette nødvendig styring innen personvern og informasjonssikkerhet.		
<b>Omfang</b>	Omfatter overordnede føringer for personvern og informasjonssikkerhet og gir en oversikt over sentrale sikkerhetstiltak kommunen må ivareta.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Personopplysningsloven §§ 8, 9, 11 og 13</li> <li>• Helsepersonelloven § 21</li> <li>• Pasientrettighetsloven §§ 3-6 og 4-1</li> <li>• Personopplysningsforskriften §§ 2-11, 2-12 og 2-13</li> <li>• Helseregisterloven § 16</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet (Normen) og faktaark</li> <li>• Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner</li> <li>• Veileder i informasjonssikkerhet ved tilknytning mellom kommuner, fylkeskommuner og helsenettet</li> </ul>		

I kommunen vil det være stort behov for å ivareta personvern og informasjonssikkerhet som en ledelsesoppgave, spesielt med utgangspunkt i at:

- en stadig større del av kommunens håndtering av helse- og personopplysninger innenfor helse- og sosialtjenesten skjer elektronisk
- stor dynamikk, høy endringstakt og høy grad av elektronisk registrering og bruk av fagsystemer og andre IT-systemer for tjenstedokumentasjon preger arbeidsdagen i kommunen, både på helseområdet og på sosialområdet
- tilsyn i kommunene har i enkelte tilfeller avdekket mangler og til dels store ulikheter ved håndteringen av helse- og personopplysninger
- alle kommuner som er tilknyttet helsenettet skal følge Normen
- kommunene har oppgaver knyttet til rapportering til IPLOS-registeret
- hensynet til den registrertes krav på personvern gjør det nødvendig å nå ut med informasjon til mottakere av kommunale helse- og sosialtjenester

I personvernsammenheng skal kommunen ivareta den registrertes rettsikkerhet gjennom:

- **Taushetsplikten:** Personellet som behandler helse- og personopplysninger i kommunen, vil være underlagt regler om taushetsplikt. Dette sikrer at den registrerte kan være trygg på at informasjonen ikke blir gitt videre til uvedkommende. Kommunens ledelse skal legge til rette for at det enkelte personell overholder den taushetsplikten som ligger til vedkommendes arbeidsoppgaver. Dette kan bl.a. skje gjennom etablering av prosedyrer, tilgangsstyring og hendelsesregistrering i forbindelse med valg og implementering av ulike fagsystemer for de ulike tjenestene kommunen tilbyr.
- **Informasjonsplikten:** Kommunen har plikt til å gi informasjon til den registrerte om hva kommunen registrerer om vedkommende. Unntak: Når det gjelder registrering av opplysninger i pasientjournal, er det ikke en slik informasjonsplikt om registreringen.

- **Informert samtykke:** Å behandle helse- og personopplysninger krever et rettslig grunnlag. Uten slikt grunnlag vil behandlingen av opplysningene ikke være lovlig. Et slikt grunnlag kan finnes i lov / forskrift eller ved at den registrerte samtykker i registreringen. Kommunens ledelse skal sikre at alle behandlinger av helse- og personopplysninger har korrekt og lovlig grunnlag.
- **Retten til reservasjon:** Den registrerte har rett til å reservere seg mot at diagnoser blir sendt til det sentrale IPLOS-registeret. For helseopplysninger har pasienten rett til å reservere seg mot at opplysninger gis til andre i forbindelse med at det ytes helsehjelp. Kommunens ledelse skal legge til rette for at den registrerte kjenner den reservasjonsretten som er aktuell for vedkommende. Det skal også legges til rette for at personellet behandler helse- og personopplysninger i samsvar med eventuelle reservasjoner.
- **Retten til innsyn:** En sentral rettighet er retten til innsyn i opplysningene som er lagret om en selv. Som hovedregel har den registrerte krav på et slikt innsyn. Det følger f.eks. av pasientrettighetsloven at pasienten vanligvis har innsyn i egen elektronisk pasientjournal. Kommunens ledelse skal sørge for at den registrerte får innsyn i samsvar med regelverket.
- **Retten til retting og sletting:** Den registrerte kan i en rekke sammenhenger kreve at feil i helse- og personopplysningene om en selv, blir rettet eller slettet. F.eks. følger det av pasientrettighetsloven at den registrerte kan kreve at mangelfulle, feilaktige eller utilbørlige helse- og personopplysninger eller utsagn blir rettet. Kommunens ledelse skal sørge for at krav om retting og sletting håndteres i samsvar med regelverket.

#### Ved bruk av private tjenesteytere (tjenesteutsetting):

- har kommunen det overordnede ansvaret for at tjenester ytes
- bør kommunen nøye påse at tjenesteyteren følger gjeldende regler innen personvern og informasjonssikkerhet. Det anbefales at kommunen ivaretar dette ved utforming av kravspesifikasjoner og kontrakter
- har kommunen ikke noe direkte ansvar for personvernet og informasjonssikkerheten internt hos den private tjenesteyteren. Databehandlingsansvaret ligger hos den private tjenesteyteren.

#### Mer veiledning

I ”Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner” er det gitt en nærmere bakgrunn for personvernet og informasjonssikkerheten, og anbefalinger for sikkerhetstiltak er utførlig beskrevet. Øvrige faktaark og veiledere under Normen gir utdypende råd og veiledning på ulike områder. Dokumentene kan lases ned på: <http://www.normen.no>

Tabellen nedenfor gir en oversikt over tiltak kommunen må iverksette og følge opp før behandling, under behandling og ved sletting/avvikling av helse- og personopplysninger:

Nr.	Handling
1.	<p><b>Før behandling av helse- og personopplysninger:</b></p> <ul style="list-style-type: none"> <li>a) Utarbeide eller oppdatere styringssystemet for informasjonssikkerhet</li> <li>b) Utarbeide eller påse at sikkerhetsmål og -strategi er ivarettatt</li> <li>c) Definere ansvar og roller for ivaretagelsen av personvernet og informasjonssikkerheten</li> <li>d) Identifisere og beskrive formålet med behandling av helse- og personopplysninger. (Enkelte behandlinger kan være melde- eller konsesjonspliktige overfor Datatilsynet. I så fall må melding inngis/konsesjon søkes før behandlingen tar til.)</li> <li>e) Fastsette akseptkriterier og gjennomføre risikovurdering av fagsystemet</li> <li>f) Etablere tekniske løsninger</li> <li>g) Oppdatere konfigurasjonskontroll og dokumentasjon</li> <li>h) Etablere prinsipper og prosedyrer for tilgangsstyring</li> <li>i) Etablere prosedyrer for elektronisk samhandling med eksterne</li> <li>j) Etablere prosedyrer for intern samhandling med helse- og personopplysninger</li> <li>k) Etablere hendelsesregistrering</li> <li>l) Etablere prosedyrer for håndtering av utskrifter</li> <li>m) Etablere prosedyrer for å ivareta sentrale rettigheter for den registrerte</li> <li>n) Gjennomføre opplæring for etterlevelse av personvernet og informasjonssikkerheten</li> </ul>

Nr.	Handling
	o) Etablere prosedyrer for avviksbehandling p) Håndtere kommunesamarbeid i forbindelse med felles fagsystem eller systemer for tjenstedokumentasjon q) Etablere evt. databehandleravtale (ved bruk av ekstern driftsenhet)
2.	<b>Under behandling av helse- og personopplysninger:</b> a) Følge opp prosedyrene for sentrale rettigheter for den registrerte b) Følge opp autorisasjon og tilgangsstyring c) Revidere risikovurderinger d) Gjennomføre sikkerhetsrevisjoner e) Identifisere og håndtere sikkerhetshendelser (avvik) f) Følge opp konfigurasjon og dokumentasjon g) Følge opp hendelsesregistrering h) Ivareta bruk av mobilt utstyr i) Ivareta utsendelse av elektroniske meldinger til den registrerte j) Oppdatere løsninger mot ondsinnet programvare k) Etterleve prosedyrene for samhandling med interne og eksterne parter l) Sørge for nødvendig opplæring
3.	<b>Ved avvikling eller sletting av helse- og personopplysninger:</b> a) Følge opp konfigurasjonsstyring b) Følge opp autorisasjon og tilgangsstyring c) Vurdere å slette, overføre eller deponere helse- og personopplysninger