

 	Utgitt med støtte av:  HelseDirektoratet
Norm for informasjonssikkerhet <a href="http://www.normen.no">www.normen.no</a>	
<h2>Oversikt over behandlinger av helse- og personopplysninger i virksomheten</h2>	<b>Støttedokument</b> <b>Faktaark nr 13</b> Versjon: 2.1 Dato: 15.12.2010

<b>Målgruppe</b>  Dette faktaarket er spesielt relevant for:	<input type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" 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 checked="" type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens leder er ansvarlig for å ha oversikt over behandlinger av helse- og personopplysninger.		
<b>Gjennomføring</b>	Kontinuerlig som en løpende aktivitet.		
<b>Formål</b>	Ha oversikt over behandlingene virksomheten utfører.		
<b>Omfang</b>	Skal inneholde informasjon om alle behandlinger i virksomheten.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Personopplysningsloven § 11 og § 13</li> <li>• Personopplysningsforskriften kap 2</li> <li>• Helseregisterloven § 11</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet, kapittel 4.5</li> <li>• Om personvernombud, se: <a href="http://www.datatilsynet.no">www.datatilsynet.no</a></li> <li>• Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner</li> </ul>		

For mange virksomheter kan det være en utfordring å ha oversikt over hvilke behandlinger av helse- og personopplysninger som gjøres med tanke på formål, hjemmel, informasjonssystemer, etc. En slik samlet og oppdatert oversikt over alle behandlinger av helse- og personopplysninger i virksomheten, er et viktig styringsdokument for informasjonssikkerhet, og et praktisk redskap i det gjennomførende arbeidet. Dette vil også kunne være et viktig bidrag til den generelle internkontrollen i virksomheten på dette området.

Nr.	Aktivitet/Beskrivelse
1	<b>Utforme oversikt over behandlinger og tilhørende formål</b> Opprett et oversiktsskjema for de ulike behandlingene av helse- og personopplysninger. F.eks. kan vedlagte skjema benyttes som et utgangspunkt og videre tilpasses den enkelte behandlingen av helse- og personopplysninger.
2	<b>Beskriv ytterligere detaljert informasjon for den aktuelle behandlingen av helse- og personopplysninger</b> <ul style="list-style-type: none"> <li>- Beskrivelse av formålet med behandlingen av helse- og personopplysninger</li> <li>- Juridisk hjemmelsgrunnlag for behandlingen</li> <li>- Angivelse av system/register/utstyr, og om det er elektronisk eller manuelt</li> <li>- Om opplysningene er sensitive eller ikke sensitive personopplysninger</li> <li>- Konesjonsplikt/meldeplikt/hjemmel for unntak</li> <li>- Evt. partnere, databehandlere eller leverandører</li> <li>- Internt ansvarlig for det enkelte system/register/utstyr</li> </ul> <p>På et mer detaljert nivå kan oversikten inneholde nærmere opplysninger og kommentarer relatert til punktene ovenfor, samt informasjon om hvilke sikkerhetstiltak som er iverksatt for det enkelte system, register eller utstyr og dato for siste gjennomførte risikovurdering</p>
3	<b>Kontinuerlig forvaltning av helse- og personopplysningene som behandles</b> Som en løpende prosess må de ulike oversiktene oppdateres av den ansvarlige, enten det er en operativ databehandlingsansvarlig eller et personvernombud.

## Eksempel på tabell

VIRKSOMHETSNAVN	<helseforetaket, institusjon, etc.>
KONTAKTINFORMASJON	<telefon, e-postadresse>

Behandling	Formål med behandlingen av opplysningene	Hjemmel og behandling Angi om det er flere behandlinger under den enkelte behandling	Navn på fagsystemet opplysningene er registrert i (EPJ-leverandør, systemnavn mv.)	Kategorier av opplysninger Sensitive personopplysninger, ikke sensitive personopplysninger eller administrative opplysninger, evt. kombinasjon av disse.	Er behandlingen(e) i fagsystemet meldepliktig eller konsesjonspliktig? Dato for meldingen / konsesjon noteres. <u>Meldingen skal fornyes hvert 3 år.</u> Flere behandlinger kan inngå i den samme meldingen.	Data-behandlings-ansvarlig / delegert	Data-behandler (Evt. informasjon om databehandleravtale (dato for inngåelse, varighet mv.))
				<input type="checkbox"/> Sensitive <input type="checkbox"/> Ikke sensitive <input type="checkbox"/> Administrative	<input type="checkbox"/> Meldeplikt: _____ <input type="checkbox"/> Konsesjon: _____		<input type="checkbox"/> Ja <input type="checkbox"/> Nei