

 <p>Norm for informasjonssikkerhet www.normen.no</p>	Utgitt med støtte av: 
<h2>Skadereparasjon når data har blitt utilsiktet utlevert</h2>	<b>Støttedokument</b> <b>Faktaark nr. 41</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 checked="" type="checkbox"/> Forsker <input checked="" type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder / sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input checked="" type="checkbox"/> Forskningsansvarlig	<input checked="" type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	Virksomhetens leder er ansvarlig for at utilsiktet utlevering av helse- og personopplysninger blir håndtert på en korrekt måte.		
<b>Gjennomføring</b>	Virksomheten skal etablere prosedyrer for å håndtere utilsiktet utlevering av helse- og personopplysninger. Faktaarket kan danne grunnlag for en slik prosedyre.		
<b>Formål</b>	Håndtere utilsiktet utlevering av helse- og personopplysninger på en korrekt måte samt gi ansatte opplæring i håndtering av utilsiktet utlevering.		
<b>Omfang</b>	All utilsiktet utlevering av helse- og personopplysninger		
<b>Hjemmel</b>	Personopplysningsforskriften § 2-6		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Helseregisterloven § 33</li> <li>• Helseregisterloven § 34</li> <li>• Helseregisterloven § 35</li> <li>• Personopplysninger på avveier (22.11.2007), Datatilsynet, En handlingsplan for virksomheter: <a href="http://www.datatilsynet.no/templates/article_2071.aspx">http://www.datatilsynet.no/templates/article_2071.aspx</a></li> <li>• Faktaark 7 – Risikovurdering</li> <li>• Faktaark 8 – Avviksbehandling</li> <li>• Faktaark 15 – Hendelsesregistrering og oppfølging</li> <li>• Faktaark 17 – Fysisk sikring av områder og utstyr</li> <li>• Faktaark 19 – Tiltak for å hindre ondsinnet program</li> <li>• Faktaark 22 – Kontroll og sikring av ekstern tilgang</li> <li>• Faktaark 30 – Mobilt utstyr</li> <li>• Faktaark 34 – Håndtering av lagringsmedia</li> <li>• Faktaark 36 – Fjernaksess for vedlikehold og oppdatering</li> <li>• Faktaark 42 – Bruk av SMS i pasientkontakt</li> </ul>		

Med utilsiktet utlevering menes hendelser som har medført utilsiktet utlevering av helse- og personopplysninger.

Nr	Handling
1.	<b>Stanse og begrense utlevering av helse- og personopplysninger</b> <ol style="list-style-type: none"> <li>a) Varsle internt om hendelsen</li> <li>b) Plassere ansvar på en person som leder og organiserer skadebegrensningen</li> <li>c) Kartlegge og dokumentere overordnet hva som har skjedd. Bruk etablerte prosedyrer og skjemaer for avviksbehandling</li> <li>d) Etablere nødvendige strakstiltak for å stanse og begrense utleveringen:           <ul style="list-style-type: none"> <li>- dersom helse- og personopplysninger ved feil er utlevert, be om at disse slettes</li> <li>- dersom helse- og personopplysninger ved feil er publisert få disse slettet</li> <li>- tekniske tiltak slik at sikker løsning gjenoprettes. Teknisk løsning er spesielt sårbar ifm oppdateringer som endrer konfigurasjon og oppsett av sikkerhetsbarrierer</li> <li>- fysiske tiltak for å begrense adgang til helse- og personopplysninger</li> <li>- administrative tiltak</li> </ul> </li> <li>e) Ved behov sikre bevis uten å fjerne eller å skade lagrete data. Her kan det være nødvendig å kontakte ekspertise på sikring av databevis</li> <li>f) Vurdere om det er nødvendig å kontakte politiet. Dette avhenger av hva som har skjedd og hvordan det har skjedd. Databehandlingsansvarlig avgjør om dette skal gjøres</li> </ol>

Nr	Handling
2.	<p><b>Dokumentere type og omfang av helse- og personopplysninger som er utlevert</b></p> <p>a) Beskriv type og omfang av helse og personopplysningene som er utlevert. Kan opplysningene brukes (er de kryptert eller ikke)?</p> <p>b) Dokumenter hendelsesforløp og årsaken for utleveringen. Årsakene kan være tekniske, fysiske eller administrative. Bruk hendelsesregistrering, der dette er relevant, for å kartlegge hendelsen detaljert. Eksempler på utilsiktet utlevering kan være</p> <ul style="list-style-type: none"> <li>- Uhell ved at utskrift av pasientjournaler er forlagt, bærbar PC med helseopplysninger mistes, lagringsmedia som forsendes via rekommandert post kommer på avveie</li> <li>- Bevisst handling som "kikking" i elektroniske journaler, utskrift av journaler (for kjente personer) som man ikke er behandlende helsepersonell for eller forsendelse av helseopplysninger via e-post</li> <li>- Kriminell handling ved tyveri av sentral server fra legekantoret som inneholdt det elektroniske journalsystemet, tyveri av arbeidsstasjoner og bærbart utstyr, avlytting av trådløst nettverk</li> <li>- Feil i systemer (funksjonsfeil eller feil ved konfigurasjon) slik at utskrifter har blitt sendt til feil skriver, bruker får tilgang til elektroniske pasientjournaler tilhørende en annen virksomhet ved bruk av ekstern driftsleverandør (databehandler), meldinger fra et laboratorium er feilsendt til virksomheten, andre meldinger (elektroniske) er feilsendt til/fra virksomheten</li> </ul> <p>c) Beskriv hvem som er berørt av hendelsen. For eksempel:</p> <ul style="list-style-type: none"> <li>- Pasient(er)</li> <li>- Helsepersonell</li> <li>- Pårørende / foresatte</li> <li>- Virksomheten</li> <li>- Leverandør</li> <li>- Ansatte</li> </ul> <p>d) Beskriv skader som følge av hendelsen. Som for eksempel:</p> <ul style="list-style-type: none"> <li>- Blottstilling av helseopplysninger</li> <li>- Tap av helseopplysninger</li> <li>- Medieomtale</li> <li>- Søksmål mot virksomheten eller berørte parter</li> <li>- Har hendelsen inntruffet før eller er det en engangshendelse</li> </ul>
3.	<p><b>Varsle om hendelsen</b></p> <p>a) Ved tilfeller hvor politiet er inne i bildet skal all varsling avklares med politiet</p> <p>b) Varsle berørte parter ift pkt 2 c) over. Databehandlingsansvarlig må vurdere om berørte parter skal varsles og hvilke hensyn som bør vektlegges ved selve varslingen. Ved at berørte varsles kan vedkommende selv bidra til skadebegrensning og hindre at ytterligere skade inntreffer. Måten og innholdet i varslingen avpasses ift hendelsen og hvilken informasjon som er utlevert. Jo mer alvorlig utleveringen er ovenfor den enkelte, desto mer direkte bør varslingen være</p> <p>c) Varsle Datatilsynet for å ivareta virksomhetens varslingsplikt iht Personopplysningsforskriftens § 2-6. Rapporteringen vil normalt inneholde</p> <ul style="list-style-type: none"> <li>- Ivaretagelse av varslingsplikten</li> <li>- Beskrivelse av hendelsen som har inntruffet</li> <li>- Beskrivelse av type informasjon som er utlevert og i hvilket omfang</li> <li>- Årsak til hendelsen</li> <li>- Tiltak som er gjennomført eller som vil bli gjennomført</li> <li>- Hvem som er varslet om hendelsen</li> <li>- Kontaktperson i virksomheten for ytterligere informasjon</li> </ul> <p>d) Rapportere internt i virksomheten hvem de berørte partene er og hvordan varslingen er gjennomført</p> <p>e) Avhengig av omfang og type utilsiktet utlevering kan det medføre en mediasak som berører både virksomheten og de berørte parter. Virksomheten må i så fall planlegge hvordan media skal håndteres</p>

Nr	Handling
4.	<p><b>Skadeopprettende tiltak</b></p> <ul style="list-style-type: none"> <li>a) Avklare hvordan helse- og personopplysninger har blitt spredd (for eksempel e-post, minnepinne på avveie, svikt i teknisk løsning, bærbar PC, nettsted med feil, utskrift)</li> <li>b) Gjennomføre sikkerhetsrevisjon av eksisterende tiltak og løsninger som skulle ha forhindret hendelsen for å avdekke om eksisterende sikkerhetsløsninger og prosedyrer må endres og nye tiltak etableres</li> <li>c) Gi råd til berørte parter hvordan de kan eller skal forholde seg for å begrense skade</li> <li>d) I tilfeller helse- og personopplysninger er spredd på Internett skal søkemotorer, nasjonalbiblioteket, Internett-bibliotek generelt og andre parter på Internett kontaktes og pålegges å slette informasjonen. Årsaken er at flere av disse indekserer og tar kopi av eventuell publisering</li> <li>e) Datatilsynet vil kunne gi råd i skadeopprettende tiltak</li> </ul>
5.	<p><b>Forhindre gjentakelse</b></p> <ul style="list-style-type: none"> <li>a) Detaljert gjennomgang av årsaker og kartlegge om dette er et enkeltstående tilfelle eller om utleveringen kan oppstå på nytt</li> <li>b) Gjennomføre risikovurdering av nye løsninger for å avdekke mulige svakheter</li> <li>c) Utarbeide tiltaksplan</li> <li>d) Gjennomføre foreslåtte tiltak for å hindre gjentakelse</li> <li>e) Vurdere behovet for en intern eller ekstern granskning av hendelsen</li> </ul>