

   		Utgitt med støtte av:  Helsedirektoratet
Norm for informasjonssikkerhet www.normen.no		
<h1>Avviksbehandling</h1>		Støttedokument Faktaark nr 8 Versjon: 2.1 Dato: 15.12.2010

Målgruppe 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
Ansvar	Den enkelte medarbeider er ansvarlig for å rapportere avvik. Virksomhetens ledelse er ansvarlig for å behandle avvik og iverksette tiltak.		
Gjennomføring	Ved avvik fra etablerte prosedyrer		
Formål	Formålet med avviksbehandling er å: <ul style="list-style-type: none"> • Håndtere sikkerhetsbrudd på en systematisk måte • Gjenopprette normaltstanden etter et sikkerhetsbrudd • Vurdere endringer i sikkerhetsarbeidet for å hindre fremtidige sikkerhetsbrudd • Sikre at Datatilsynet varsles ved uautorisert utlevering av helse- og personopplysninger 		
Omfang	Alle virksomheter som behandler helse- og personopplysninger skal ha prosedyrer for håndtering av avvik. Med avvik menes enhver behandling av helse- og personopplysninger som ikke er iht gjeldende regelverk og prosedyrer.		
Hjemmel	<ul style="list-style-type: none"> • Personopplysningsforskriften § 2-6 • Internkontrollforskriften av 20. des. 2002 nr. 1731, jf. helsepersonelloven § 16, 2. ledd. 		
Referanser	<ul style="list-style-type: none"> • Norm for informasjonssikkerhet, kap 6. 3 Avvikshåndtering • Faktaark 41 - Skadereparasjon når data har blitt utilsiktet utlevert 		

Avvik er brudd på regelverk og etablerte prosedyrer som skal sikre konfidensialitet, integritet, tilgjengelighet og kvalitet.

En prosedyre for avvikshåndtering må spesielt:

- Definere en fast mottaker av avviksmeldinger
- Beskrive hvordan avviksmeldingen håndteres hos mottaker
- Beskrive hvem som er ansvarlig for håndteringen
- Gi veiledning i hva som er et avvik (f.eks.: utskift kommer på feil skiver, bærbart utstyr blir stjålet, papirjournal ligger åpent tilgjengelig, bruker går fra arbeidsstasjonen usikret, bruker låner ut brukernavn og passord til andre, brukers tilgang blir ikke fjernet ved fratredelse, helse- og personopplysninger blir sendt i usikret e-post, autorisert bruker får ikke tilgang, urettmessig tilegnelse av taushetsbelagte opplysninger {snoking}, bruk av nødrettstilgang)
- Melde avvik som skyldes eksterne kommunikasjonsparter til eksternt part, samt sørge for at eksternt part gir tilbakemelding om oppfølging av avviket

Prosedyren bør inneholde:

- Identifisering av årsaken til avviket
- Planlegging og gjennomføring av tiltak for å forhindre gjentakelse
- Innsamling og sikring av hendelsesregistre og eventuelle andre bevis
- Kommunikasjon med brukere som berøres av eller er involvert i gjenopprettingen
- Ansvarlig for lukking av avvik

Oppdagelse og rapportering av avvik

Avvik kan avdekkes på ulike måter: Ansatte oppdager at informasjon er kommet på avveie, IKT-driftspersonalet avdekker sikkerhetsbrudd som manglende tilgang, uautorisert tilgang osv. Melding om avvik kan også komme fra databehandler eller gjennom automatiske varslingsfunksjoner. Alle ansatte har plikt til å melde fra om avvik. Avvik rapporteres iht prosedyre. I større virksomheter kan det være

naturlig at en sikkerhetskoordinator eller lignende rolle utpekes som mottaker av avviksrapporten og som ansvarlig for å iverksette strakstiltak. I forbindelse med elektronisk samhandling er det viktig at store virksomheter klargjør for kommunikasjonsparter hvem som skal varsles og hvem som har ansvar for å følge opp avvik som er relatert til samhandlingen. Eksempel på rapporteringsskjema er vist nedenfor.

Iverksetting av strakstiltak

Nødvendige strakstiltak, dvs. tiltak for å stoppe avviket og begrense skadeomfanget må iverksettes så raskt som mulig. Strakstiltakene bør besluttes av den som er ansvarlig for å håndtere avviket i samarbeid med eventuelt berørte parter og annen nødvendig kompetanse, f.eks. IKT-driftsavdeling. Opplysninger om hva som er besluttet og av hvem, hva som er utført og av hvem skal dokumenteres på avviksskjema. Eksempler på strakstiltak er å stenge tjenester i nettverket og stenge brukerkontoer.

Tekniske spor, hendelsesregistre o.l. som kan bidra til å klargjøre årsakssammenheng for avviket bør samles inn så raskt som mulig. Hvis avviket kan medføre politianmeldelse bør relevante komponenter (IKT-systemer, hendelsesregistre, osv.) beskyttes mot endringer (frakobles nettverk, speilkopieres, mv.) for å kunne benyttes som evt. bevismateriale.

Korrigerende tiltak

Korrigerende tiltak er de mer langsiktige endringene som gjennomføres som konsekvens av avviket. De korrigerende tiltakene skal fjerne/reducere årsaken til avvikene og kan innebære mer omfattende endringer i IKT-systemer, organisasjonen og prosedyrer.

Iverksetting av korrigerende tiltak bør også innebære en vurdering av strakstiltakene som er innført og hvorvidt disse skal opprettholdes eller endres.

Vurdering av tiltak

Tiltakene som er innført bør vurderes etter en tid. Det bør vurderes om tiltakene har vært hensiktsmessige, hvorvidt de er effektive for å hindre sikkerhetsbrudd og om de har hatt utilsiktede konsekvenser som eksempelvis mangelfull tilgang til systemer, redusert funksjonalitet i IKT-systemene, mv. Denne vurderingen bør være en del av ledelsenes årlige gjennomgang av informasjonssikkerheten.

Har avviket vært omfattende bør det gjennomføres en risikovurdering for å avklare om etablerte tiltak er tilstrekkelige.

Ved uautorisert utlevering av helse- og personopplysninger skal Datatilsynet varsles. Videre kan virksomhetens ledelse vurdere om den registrerte (pasient, pårørende, osv) skal informeres.

Eksempel på skjema for avviksrapportering

Område	Innhold	Kommentarer
Avvik registrert av:		Hvem som har registrert avviket – inkl. kontaktinformasjon
Tidspunkt:		Når avviket inntraff
Hendelse:		Beskrivelse av avviket
Strakstiltak:		Eventuelle strakstiltak som er innført

I tillegg bør den som mottar avviksrapporten fylle ut informasjon om:

Område	Innhold	Kommentarer
Korrigerende tiltak:		Hvilke korrigerende tiltak som er besluttet innført
Evaluering av tiltak:		Hvem som er ansvarlig for å evaluere tiltakene, og når.

Område	Innhold	Kommentarer
Varsling:		Interne og eksterne (for eksempel legekantor) som er varslet om avviket. Hvis avviket innebærer uautorisert utlevering av helse- og personopplysninger skal Datatilsynet varsles.
Ansvarlig for å lukke avviket:		Navn på den som skal påse at avviket lukkes.
Tilbakerapportering til melder av avviket:		Ekstern melder skal også ha tilbakerapportering.