Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:
Direktoratet for e-helse

Avviksbehandling

Støttedokument
Faktaark nr 8
Versjon: 5.1
Dato: 11.12.2018

Formål	Formålet med avviksbehandling er å: • Håndtere sikkerhetsbrudd på en systematisk måte • Gjenopprette normaltilstanden etter et sikkerhetsbrudd • Vurdere endringer i sikkerhetsarbeidet for å hindre fremtidige sikkerhetsbrudd • Sikre at Datatilsynet og den registrerte varsles ved brudd på personopplysningssikkerheten		
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 sikkerhetstiltak og rutiner.		
Omfang	Alle virksomheter som behandler helse- og personopplysninger skal ha rutine for håndtering av avvik.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Virksomhetens leder/ledelse ☒ Forskningsansvarlig ☒ Prosjektleder forskning ☒ Sikkerhetsleder	☒ Ansatt / medarbeider ☒ Forsker ☒ Personvernombud	☒ IKT-ansvarlig ☒ Databehandler ☐ Leverandør
Hjemmel	• Personvernforordningen artikkel 4 (12), 32, 33, 34 • Personopplysningsloven § 16		
Referanser	• Norm for informasjonssikkerhet, kap 5.8.1 og 5.8.2 • Datatilsynets veileder om når og hvordan melde avvik • Lenke til skjema til Datatilsynet for melding om brudd på personopplysningssikkerheten		

Innholdet i dokumentet er gjennomgått og oppdatert ut fra Normen 5.3, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning

Avvik er sikkerhetsbrudd og/eller når behandling av helse- og personopplysninger er utført i strid med gjeldende regelverk, retningslinjer eller rutiner. For å sikre at regelverket følges skal det etableres avviksrutiner slik at årsak til avviket, korrigerende tiltak og rapportering blir dokumentert. Avvikshåndtering kan også iverksettes ved tilfeller av manglende eller uhensiktsmessige rutiner.

En rutine for avvikshåndtering må spesielt:
- Definere en fast mottaker av avviksmeldinger, som kan være sikkerhetsleder, personvernombud e.l.
- Beskrive hvordan avviksmeldingen håndteres hos mottaker
- Beskrive hvem som er ansvarlig for håndteringen
- Beskriv at alle ansatte har plikt til å melde fra om avvik
- Gi veiledning i hva som er et avvik, for eksempel:
    - *Konfidensialitet*: Utskrift med personopplysninger eller bedrift sensitiv informasjon kommer på feil skriver, bærbart utstyr blir stjålet eller mistet papirjournal ligger åpent tilgjengelig, bruker går fra arbeidsstasjon usikret, bruker låner ut brukernavn og passord til andre, brukers tilgang ikke fjernet ved fratredelse, helse- og personopplysninger blir sendt i usikret e-post, uautoriserte får tilgang til helse- og personopplysninger (hacking), brukernavn/passord kommer på avveier, urettmessig tilegnelse av taushetsbelagte opplysninger (snoking), urettmessig bruk av nødrettstilgang eller elektroniske meldinger fra virksomheter feilsendes til andre virksomheter
    - *Integritet*: helse- og personopplysninger blir registrert i feil pasientjournal, uautoriserte endringer av helseopplysninger, autorisert personell endrer informasjon ved uhell/ overlegg,

    - *Tilgjengelighet*: autorisert bruker får ikke tilgang, systemer blir utsatt for skadelig programvare som forårsaker nedetid, personopplysninger blir slettet ved uhell, og det er mangel på backup, systemet blir utsatt for tjenestenektangrep som fører til at informasjon blir utilgjengelig.
- Gi eksempler på hva som ikke er et avvik; bruker får ikke logget på PC, planlagt nedetid for systemet, planlagt oppdatering av systemet
- Avvik som skyldes ekstern kommunikasjonspart, meldes til ansvarlig part, samt sørge for at denne gir tilbakemelding om oppfølging av avviket.

Rutinen bør inneholde:
- Hvordan og til hvem avvik skal rapporteres
- Identifisere årsaken til avviket
- Planlegge og gjennomføre tiltak for å hindre gjentagelse
- Samle inn og sikre hendelsesregistre og eventuelle andre bevis
- Kommunikasjon med brukere som berøres av eller er involvert i gjenopprettingen
- Plassere ansvar for å lukke avviket
    - Dersom det foreligger et databehandlerforhold hvor avviket oppstår hos databehandler, har databehandleren plikt til å informere dataansvarlig så raskt som mulig uten ugrunnet opphold. Databehandler kan melde avviket direkte til Datatilsynet dersom de har fullmakter til dette gitt av dataansvarlig, og det er spesifisert i databehandleravtalen. Dersom det foreligger felles behandlingsansvar, bør det reguleres i avtale hvem som har ansvar for å melde avviket, følge opp og lukke det.

Brudd på personopplysningssikkerheten er alltid et brudd på sikkerheten, men et brudd på sikkerheten er ikke alltid et brudd på personopplysningssikkerheten. Virksomheten skal ha interne rutiner for å kunne oppdage og håndtere avvik, men det er ikke alltid nødvendig å melde inn dette til Datatilsynet. I rutinen må man vurdere risikoen for de registrerte, og om det er nødvendig å melde til datatilsynet innen 72 timer. Vurderingene som gjøres, må dokumenteres.
- Dersom det er ingen eller lav risiko, er det ikke behov for å melde fra til Datatilsynet, eller de berørte.
- Dersom det er middels risiko, er det nødvendig å melde fra til Datatilsynet, men ikke informere de berørte.
- Dersom det er høy risiko, er det nødvendig å melde fra til Datatilsynet, og informere de berørte.

Når man skal vurdere risiko av et brudd må man se på de konkrete omstendighetene rundt et brudd, herunder dens alvorlighetsgrad og potensielle innvirkning. For å avgjøre dette kan man se på følgende kriterier:
- Er det brudd på konfidensialitet, integritet, tilgjengelighet eller robustheten, og hva er konsekvensene av det?
- Hva slags kategorier av personopplysninger er det snakk om? Graden av sensitivitet vil ofte tilsi at jo mer sensitiv eller følsomme opplysningen er, jo større risiko er det for de berørte. Brudd som kombinerer ulike kategorier vil også ofte tilsvare større risiko for de berørte.
- Hvor lett er det å identifisere enkeltpersoner? Ut i fra data som er kompromittert, må virksomheten vurdere om hvor lett det er å identifisere enkeltpersonene som er berørte. Er dataene krypterte, og har man kontroll på krypteringsnøklene?
- Alvorlighetsgraden av konsekvenser for enkeltpersoner. Det må vurderes hva bruddet kan medføre av konsekvenser. F.eks. om bruddet kan føre til ID-tyveri, svindel, fysisk skade, psykisk påkjenning, ydmykelse eller skade av omdømme. Dersom det er feilaktig utlevert til tredjepart man har tillit til, hvor det er stor grad av tillit til opplysningene blir slettet/tilbakeført, kan dette ha påvirkning på risikoen for enkeltpersoner.
- Om det er spesielle egenskaper ved enkeltpersoner. Dersom det er snakk om barn, eller andre sårbare enkeltpersoner/ utsatte grupper kan det medføre større konsekvenser.

- Antall berørte enkeltpersoner kan variere fra en person, noen få, til mange tusen. Generelt vil det være større konsekvenser jo flere som er berørte.
- Spesielle egenskaper ved den behandlingsansvarlige. Et helseforetak vil behandle helseopplysninger som vil kunne medføre større skade ved et brudd, enn hvis det skjer en utlevering av en adresseliste over abonnenter av en avis.

Den registrerte skal varsles om avviket har medført sletting, endring eller uautorisert tilgjengeliggjøring/tilgang helse- og personopplysningene dersom bruddet medfører høy risiko for den registrertes rettigheter og friheter. Unntak til dette er dersom

- Det er gjennomført tekniske og organisatoriske sikkerhetstiltak for de personopplysningene som er berørt av avviket, f.eks. tiltak som gjør opplysningene uleselige.
- Det er truffet tiltaket i etterkant som gjør at det er lite trolig at avviket har ført til utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert tilgjengeliggjøring av eller tilgang til personopplysninger.
- Om varslingen innebærer en uforholdsmessig stor innsats (f.eks. ved at avviket berører et stort antall individer) skal allmennheten underrettes slik at den registrerte likevel underrettes på en effektiv måte.

Det anbefales å benytte et felles avvikssystem i virksomheten. Da er det er viktig å kunne skille avvik mellom ulike områder (for eksempel medisinsk sikkerhet, personellsikkerhet (HMS), informasjonssikkerhet). Eksempel på forløp av avviksbehandling kan være:

Nr	Aktivitet	Beskrivelse
1.	Oppdage og rapportere avviket	Avvik kan avdekkes på ulike måter: - Ansatte oppdager at informasjon er kommet på avveie, IKT-driftspersonell 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. rutiner. 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
2.	Iverksette strakstiltak	- Nødvendige strakstiltak, dvs. tiltak for å stoppe avviket og begrense skadeomfanget må iverksettes så raskt som mulig, f.eks.: o Dersom helse- og personopplysninger ved feil er utlevert, be om at disse slettes, dersom helse- og personopplysninger ved feil er publisert, få disse slettet, tekniske tiltak slik at sikker løsning gjenopprettes. Teknisk løsning er spesielt sårbar ifm. oppdateringer som endrer konfigurasjon og oppsett av sikkerhetsbarrierer, dersom helse- og personopplysninger endres av personell med feiltakelse, eller med overlegg, endre disse, fysiske tiltak for å begrense adgang til helse- og personopplysninger - 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

Nr	Aktivitet	Beskrivelse
3.	Melding til Datatilsynet	- Når det oppstår et brudd på personopplysningssikkerheten som har medført middels eller høy risiko for den registrerte, skal dataansvarlig rapportere inn avviket til Datatilsynet snarest mulig, og senest innen 72 timer. https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/ - Meldingen skal inneholde en beskrivelse av avviket: o Hovedårsaken til at avviket oppstod, o Tidsrommet, o Når avviket ble oppdaget, o Antall personer som er berørt, o Beskrivelse av hva som har skjedd, o Hvordan avviket oppstod, o Beskrivelse av hva slags personopplysninger som ble berørt o Hvilken relasjon virksomheten har til de berørte personene (f.eks. ansatte, pasienter, pårørende, leverandør), samt o Beskrivelse av hvor personopplysningene befinner seg etter avviket. - I tillegg til beskrivelse av de sannsynlige konsekvensene av bruddet, beskrivelse av tiltak som er gjort og planlagt for å hindre gjentakelse, og hva som er gjort for å redusere skadevirkninger.
4.	Melding til de registrerte	- Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal dataansvarlig uten ugrunnet opphold underrette den registrerte om bruddet. - Meldingen skal inneholde: o Navn og kontaktinformasjon til personvernombudet o Beskrivelse av de sannsynlige konsekvensene av bruddet o Beskrive tiltakene som er truffet eller foreslått truffet for å håndtere bruddet på personopplysningssikkerheten. o Hvis relevant, tiltakene for å redusere skadevirkningen av bruddet. - Det er likevel ikke påkrevd å melde de registrerte om bruddet dersom o Det er gjennomført egnede tekniske og organisatoriske sikkerhetstiltak, særlig tiltak som gjør personopplysninger uleselige for enhver uautorisert person (f.eks. kryptering) o Det er truffet etterfølgende tiltak som reduserer sannsynligheten for at den høye risikoen vil oppstå o Det er uforholdsmessig stor innsats å melde alle registrerte. Dersom dette er tilfelle, skal allmennheten underrettes, eller lignende tiltak.
5.	Samle inn og sikre hendelses-registre og eventuelle andre bevis	- 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
6.	Korrigerende tiltak	- Korrigerende tiltak er de mer langsiktige endringene som gjennomføres som konsekvens av avviket - De korrigerende tiltakene skal fjerne/redusere årsaken til avvikene og kan innebære mer omfattende endringer i IKT-systemer, organisasjonen og rutiner - Iverksetting av korrigerende tiltak bør også innebære en vurdering av strakstiltakene som er innført og hvorvidt disse skal opprettholdes eller endres
7.	Vurdering av tiltak og	- Tiltakene som er innført bør vurderes etter en tid. Dette kan gjøres i en sikkerhetsrevisjon. Det bør vurderes om tiltakene har vært

	forhindre gjentakelse	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. - Foreslå tiltak for å forhindre gjentakelse.

Eksempel på avviksskjema

Avviksskjema			Sendes til: Linjeleder og sikkerhetsleder/ personvernombud Sendes i tillegg til IT-sjef for avvik som gjelder feil i programvare og maskinvare
Formål: Sikre at alle brudd og antatte brudd på etablerte rutiner ved behandling av helse- og personopplysninger blir rapportert og behandlet på forsvarlig måte.			
Beskriv avviket (hva er observert eller hva har skjedd): - Vedlegg (eventuelle dokumenter):			
Mulig årsak til avviket (tror du): - Vedlegg (eventuelle dokumenter):			
Hvor mange registrerte (personer) er berørt: -			
Hvilke strakstiltak eller midlertidige tiltak ble iverksatt (hva er gjort for å stoppe/avbryte avviket): - Vedlegg (eventuelle dokumenter):			
Avviket er oppdaget av:	Navn:	Avdeling:	Dato/ kl:

Dersom det har skjedd et brudd på personopplysningssikkerheten i din virksomhet, og det er sannsynlig at bruddet vil medføre en risiko for de registrerte sine rettigheter og friheter, skal virksomhetsleder varsle Datatilsynet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/