SYKEHUSET I VESTFOLD

Informasjonssikkerhet - Risikovurdering ved nye og endrede IKT-behov og databehandlinger

Gjelder for:	Hele SiV
Dokumenttype:	Prosedyre
Sist endret:	05.09.2019

1. HENSIKT

Formålet med denne prosedyre er å etablere en felles metodikk for gjennomføring av risikovurdering som del av virksomhetens styringssystem for informasjonssikkerhet i samsvar med personopplysningsloven og tilhørende forskrift. Dette sikrer at virksomheten oppfyller sitt lovpålagte ansvar for informasjonssikkerhet ved lagring, nyinstallasjon og endring i IKT-løsninger hvor det behandles helse- og personopplysninger.
Prosedyren skal benyttes i forkant for alle elektroniske lagringer, nyinstallasjoner og endringer som kan påvirke informasjonssikkerheten ved virksomhetens behandling av helse- og personopplysninger.
Lagring av helse- og personopplysninger, inkludert ved bruk av kode som erstatter navn og personnummer, på områder som ikke allerede er sikkerhetsmessig godkjente, er også en ny IT-løsning som krever risikovurdering.

2. ANSVAR

- **Administrerende direktør:** Er databehandlingsansvarlig og har ansvaret for at lagring og bruk av helse- og personopplysninger skjer med tilstrekkelig informasjonssikkerhet avklart ved gjennomført risikovurdering..
- **Informasjonssikkerhetsleder:** Gjennomfører eller bistår i gjennomføring av risikovurdering, og vurderer og eventuelt godkjenner akseptabelt sikkerhetsnivå på vegne av adm dir.
- **Ledere** innen ulike enheter og områder har ansvar for å påse at denne prosedyre implementeres og etterleves innen eget ansvarsområde. Det vil si at dokumentet er kjent, tilgjengelig og blir brukt.
- **Alle ansatte og innleide** ved virksomheten som skal lagre/bruke helse- og personopplysninger elektronisk, skal forholde seg til denne prosedyre. Dette gjelder uavhengig av organisatorisk plassering, yrkesgruppe og forskningsområde.

3. FREMGANGSMÅTE

Ved gjennomføring av risikovurdering, benyttes "**Mal for risikovurdering**", se vedlegg under «**Interne referanser**». I vedlegg A i ROS MAL dokumentet ligger «***HSØ risikoskala for informasjonssikkerhet***» og «***Sikkerhetsprinsipper og –krav for IKT-infrastruktur og applikasjoner***» som skal følges. I utfylt stand følger «Sikkerhetsprinsippene» ROS dokumentet, ved å sette det inn igjen som vedlegg.
MAL for Tjenestedesign finnes på samme område i EK under «Styrende dokumenter» og skal også følge ROS dokumentet som angitt i malen.

Gjennomført risikovurdering skal forelegges informasjonssikkerhetsleder for vurdering og eventuelt godkjenning med eller uten restanse, sendes videre til systemeier for endelig godkjenning før endring eller nyinstallasjon i IKT-systemet kan gjennomføres, inkludert lagring av forskningsstudier og andre registre utenfor godkjente forsknings- og kvalitetsservere. Dette sikrer akseptabelt risikonivå for informasjonssikkerhet ved alle endringer og nyetableringer i virksomhetens IKT-løsninger. Ved bruk av ekstern IT-leverandør/databehandler, må tilsvarende risikovurdering av leverandørens/databehandlerens IKT-løsning gjennomføres og godkjennes før lagring av helse- og personopplysninger kan gjøres.

Kartleggingsfasen
I kartleggingsfasen er målet å avdekke alle forhold som kan berøre sannsynlighet for eller konsekvens av sikkerhetsbrudd. Det er således aktuelt å avdekke:

- formål knyttet til behandlinger av helse- og personopplysninger, samt hvilke opplysninger som inngår i databehandlingene og hvilket sikkerhetsbehov som er knyttet til bruken
- hvor helse- og personopplysninger befinner seg (på tjenermaskiner, på klientmaskiner, på bærbart utstyr, hos databehandlere, på hjemmekontor mv.)
- arkitektur og elektroniske protokoller og trafikkretninger i samlet elektronisk løsning
- hvordan helse- og personopplysninger overføres og kommuniseres (elektronisk, brevpost, bud mv.)
- hvem som bruker (innsamler, registrerer, sammenslår, lagrer, utleverer mv.) helse- og personopplysninger (medarbeidere, pasienter, databehandlere, leverandører mv.)
- hvilke sikkerhetstiltak som er etablert

Gjennomføringsfasen
Gjennomføring av selve risikovurderingen skal gi en vurdering av om uønskede hendelser kan inntre, hvilken sannsynlighet for at dette skjer med påfølgende konsekvens, og om dette er innenfor eller utenfor akseptabelt risikonivå. Dette vil danne grunnlaget for å avklare om det er behov for nye eller endrede sikkerhetstiltak.

Etablering av trusselscenarier
Det må etableres en mest mulig dekkende oversikt over mulige trusselscenarier. Et trusselscenario er en beskrivelse av hvordan en sårbarhet/svakhet kan utnyttes med resultat at en uønsket hendelse kan forårsakes. Utarbeidelse av trusselscenarier gjøres ved at det identifiseres sårbarheter og andre svakheter som vil være avgjørende for sannsynligheten for at en hendelse inntreffer. Andre svakheter er av ikke-teknisk art og har årsak i menneskelige, miljømessige eller organisatoriske forhold. Trusselkilder som er aktuelle her er for eksempel miljømessige sårbarheter eller personers adferd. Ved å utarbeide trusselscenarier, dokumenterer man hvordan sårbarheter som danner et trusselscenario kan føre til at en hendelsen inntreffer. Et trusselscenario kan være basert på en eller flere sårbarheter, og en sårbarhet kan danne grunnlag for et eller flere trusselscenarier.

Vurdering og begrunnelse av om trusselscenariene vil kunne resultere i uønskede hendelser
Hendelser er tilstander eller handlinger med en årsak og med virkning i forhold til behovet for konfidensialitet, tilgjengelighet eller integritet. Hendelser beskrives ved å angi årsak og virkning. Det er viktig å skille klart mellom årsak og virkning – bla. for å sikre at alle sentrale virkninger blir vurdert, og ikke kun en lang rekke årsaker knyttet til den samme virkningen.

Årsak beskrives gjennom å angi situasjoner som forårsaker hendelsen. Årsak er således et spørsmål om hvordan, og – i forlengelsen av dette – et spørsmål om hvem. Beskrivelser av årsaker er grunnlaget for vurdering av sannsynlighet for sikkerhetsbrudd.
Virkning beskrives i forhold til behovet for sikring av konfidensialitet, tilgjengelighet og integritet. En naturlig inndeling for beskrivelse av virkning er:

- **utlevering/oppdaget** – som er påvirkning av behovet for konfidensialitet gjennom utilsiktet utlevering av opplysninger. Utleveringen oppdages tidsnok til at det kan iverksettes tiltak for å begrense skade.
- **utlevering/uoppdaget** – som er påvirkning av behovet for konfidensialitet gjennom utilsiktet utlevering av opplysninger. Utleveringen oppdages ikke tidsnok til at tiltak kan iverksettes.
- **utilgjengelig/tidsbegrenset** – som er påvirkning av behovet for tilgjengelighet ved at opplysninger er utilgjengelig innenfor et tidsrom
- **utilgjengelig/permanent** – som er påvirkning av behovet for tilgjengelighet ved at opplysninger er utilgjengelige for alltid
- **feil/gjenopprettelig** – som er påvirkning av behovet for integritet ved at opplysninger er feil, men hvor feilen kan gjenopprettes.

- **feil/uopprettelig** – som er påvirkning av behovet for integritet ved at opplysninger er feil, og hvor feilen ikke kan gjenopprettes.

Beskrivelser av virkninger er grunnlaget for vurdering av konsekvens av sikkerhetsbrudd.
En virkning kan ha flere årsaker, og en årsak kan gi opphav til flere virkninger. Spesielt, når en hendelse har flere årsaker, skal det beskrives de forskjellige årsakene, siden disse vil inntreffe med forskjellige sannsynligheter. Årsakene skal være beskrevet med relevans i den konkrete situasjon.

Bestem sannsynligheten for at hendelsene kan oppstå og klassifiser konsekvensene ifølge tabellene i mal for risikovurdering (se vedlegg). Begrunn klassifiseringene slik at det er mulig for andre å forstå konklusjonen og eventuelle forutsetninger i ettertid. Angi spesielt systemtekniske og/eller organisatoriske sikkerhetsmekanismer som underbygger konklusjonen for angitt konsekvens og sannsynlighet.
Risikonivået baseres på en funksjon av sannsynlighet og konsekvens (se Metodikk for risikovurdering). Dersom risikoen er høyere enn akseptabelt risikonivå, må det defineres sikkerhetstiltak som reduserer risikoen. Lag en oversikt over tiltak, og angi hvem som er ansvarlig for at tiltakene blir gjennomført og en tidsfrist for gjennomførelse. Beregn deretter restrisiko.

Konklusjon og eventuelt behov for ytterligere sikkerhetstiltak
Informasjonssikkerhetsleder vil på vegne av adm. dir. avgjøre om oppnådd sikkerhetsnivå og gjenværende risiko er akseptabel, eller om det er behov for ytterligere sikkerhetstiltak. I denne vurdering vil Datatilsynets veiledning være sentral om det er tvil, i det tilsynet har kompetanse og myndighet til å avgjøre dette ved tilsyn.

4. GENERELT
Lagring og bruk av person- og helseopplysninger elektronisk uten gjennomført og godkjent risikovurdering av informasjonssikkerheten, er
avvik og skal meldes i foretakets avvikssystem samt til nærmeste overordnende.

- Lov 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
- Lov av 14. april 2000 nr 31: Behandling av personopplysninger (personopplysningsloven) med tilhørende forskrift
- Lov 1999-07-02 nr 64: Lov om helsepersonell m.v. (helsepersonelloven)
- Lov av 20. juni 2008 nr 44: Medisinsk og helsefaglig forskning (helseforskningsloven)
- Lov 1999-07-02 nr 63: Lov om pasientrettigheter (pasientrettighetsloven)
- Sikkerhetsnorm

5. INTERNE REFERANSER

1.1.11.2.12	Informasjonssikkerhet - Kilder og definisjoner i regionalt styringssystem for informasjonssikkerhet
1.1.11.4.12	Informasjonssikkerhet - MAL Helseforetakets godkjenning av risikonivå

6. EKSTERNE REFERANSER

7. VEDLEGG