Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Kartlegge og klassifisere systemer

Støttedokument
Faktaark nr 4
Versjon: 3.1
Dato: 19.09.2018

Formål	• Kartlegge hvilke systemer som er kritiske for at virksomheten kan yte sine tjenester • Prioritere systemene i henhold til kritikalitet - i hovedsak gjelder dette ikke-planlagte stopp
Ansvar	Virksomhetsleder er ansvarlig for å kartlegge og klassifisere alle systemer som benyttes til behandling av helse- og personopplysninger i virksomheten. I praksis er ansvaret delegert til avdelingsledere / systemeiere.
Gjennomføring	Kartlegging og klassifisering av systemer i henhold til kritikalitet skal dokumenteres før behandling av helse- og personopplysninger starter.
Omfang	Omfatter alle systemer som inneholder helse- og personopplysninger inklusive registre/systemer i elektromedisinsk utstyr, som virksomheten benytter eller er avhengig av for å yte sine tjenester.
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 32 Pasientjournalloven § 22
Referanser	Norm for informasjonssikkerhet, kap 5.9 Faktaark 13 – Oversikt over behandlinger av helse- og personopplysninger

Merknad 19.09.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Kritikalitet skal primært vurderes ift tilgjengelighet (ikke-planlagt stopp), men vil også kunne påvirkes av integritet.

Handling/Utførelse

Nr.	Virksomhetstype
1	**Store virksomheter (f.eks. sykehus, kommuner mv.)** Med utgangspunkt i virksomhetens "Oversikt over behandlinger av helse- og personopplysninger" kan systemer prioriteres som følger: - Prioritet 1: systemer hvor stopp av tjeneste er eller kan være livstruende for pasient inklusive feilbehandling av pasient, eller kritisk for virksomhetens drift - Prioritet 2: systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre betydelig merarbeid for personell, tapt effektivitet i virksomheten - Prioritet 3: systemer hvor stopp av tjeneste kan føre til svekkelse av pasientens tillit - Prioritet 4: systemer hvor stopp inntil 72 timer kan aksepteres - Prioritet 5: systemer som ikke er prioritert Det skal også kartlegges hvilke andre systemer de prioriterte systemene er avhengig av. Disse skal ha samme prioritet som de prioriterte systemene.

Nr.	Virksomhetstype
	For hver av de 5 prioritetene skal ledelsen fastsette akseptkriterier for tilgjengelighet, som et minimum hva som er akseptabel avbruddstid, f.eks: - Klasse 1: avbruddstid (stans i system) aksepteres ikke – ingen tap av data - Klasse 2: avbruddstid (stans i system) inntil 30 minutter – ingen tap av data - Klasse 3: avbruddstid (stans i system) inntil 4 timer – ingen tap av data - Klasse 4: avbruddstid (stans i system) inntil 24 timer – ingen tap av data - Klasse 5: ikke prioritert
2	**Mindre virksomheter (f.eks rehabilitering- og opptreningsvirksomheter)** Med utgangspunkt i virksomhetens "Oversikt over behandlinger av helse- og personopplysninger" kan systemer prioriteres som følger: - Prioritet 1: systemer hvor stopp av tjeneste er eller kan være livstruende for bruker/pasient inklusive feilmedisinering, eller kritisk for virksomhetens drift - Prioritet 2: systemer hvor stopp av tjeneste kan få alvorlige konsekvenser, f.eks. medføre ▪ tapt tillit hos bruker ▪ betydelig merarbeid for personell ▪ tapt effektivitet - Prioritet 3: systemer hvor stopp inntil 24 timer kan aksepteres For hver av de 3 prioriteringene skal ledelsen fastsette akseptkriterier for tilgjengelighet, som et minimum hva som er akseptabel avbruddstid. F.eks. følgende grupper: - Klasse 1: ingen avbrudd i åpningstiden på virkedager – ingen tap av data - Klasse 2: avbruddstid (stans i system) inntil 4 timer – ingen tap av data - Klasse 3: avbruddstid (stans i system) inntil 24 timer – ingen tap av data
3	**Små virksomheter (f.eks. legekontor, tannlegekontor, fysioterapeutinstitutt, psykologfellesskap, kiropraktor, manuellterapeut, bedriftshelsetjeneste, mv.)** Ved små virksomheter kan systemer prioriteres som følger: - Prioritet 1: systemer hvor helse- og personopplysninger skal være tilgjengelig når behandlende personell har tjenstlig behov for dem For prioriteringen fastsettes følgende akseptkriterier: - Klasse 1: ingen tap av data

Eksempel

System	Prioritet	Klasse (Akseptkriterier for tilgjengelighet)
Elektronisk pasientjournal (EPJ)	1	1. Avbruddstid (stans i system) aksepteres ikke – ingen tap av data
Pasientadministrativt system (PAS)	1	1. Avbruddstid (stans i system) aksepteres ikke – ingen tap av data
Laboratoriesystem	2	2. Avbruddstid (stans i system) inntil 30 minutter – ingen tap av data
Elektronisk meldingsutveksling av svar på laboratorieprøver	2	3. Avbruddstid (stans i system) inntil 4 timer – ingen tap av data
Elektronisk meldingsutveksling av resepter	2	3. Avbruddstid (stans i system) inntil 4 timer – ingen tap av data