Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Bruk av testdata i systemer som inneholder helse- og personopplysninger

Støttedokument
Faktaark nr. 43
Versjon: 2.1
Dato: 01.10.2018

Formål	Formålet med faktaarket er å sikre konfidensialitet, integritet, tilgjengelighet og kvalitet når testdata brukes i utvikling og test av IT-systemer med helse- og personopplysninger.		
Ansvar	Det er virksomhetens leder som har ansvaret for at testdata blir behandlet forsvarlig. Det daglige ansvaret for å påse dette i praksis kan delegeres til for eksempel IT-ansvarlig.		
Gjennomføring	Ved bruk av testdata i systemer med helse- og personopplysinger under etableringen, i bruk og ved sletting.		
Omfang	Når testdata skal etableres ifm forberedelser, uttrekk og bruk slik at kravet til personvern og informasjonssikkerhet ivaretas.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder/ sikkerhetskoordinator ☐ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☒ Personvernombud
Hjemmel	Pasientjournalloven § 22 Helseregisterloven § 21		
Referanser	Norm for informasjonssikkerhet.		

Merknad 01.10.2018: 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.

Test av systemer, databaser og integrasjoner er en sentral del av utviklingsarbeidet med nye systemer, oppgraderinger eller ved feilsøkning i driften. I den anledning er det nødvendig å benytte relevante testdata slik at testene blir så nær opp til virkeligheten som mulig.

Om virksomheten gjennomfører tester iht. et rammeverk anbefales det å inkorporere krav og anbefalinger i dette faktaarket, i dokumentene til det aktuelle rammeverket.

Eksempler på bruk av testdata

- Utvikling av nye systemer
- Endring av eksisterende systemer
- Verifisere at nye versjoner av systemet ikke korrumperer data
- Test av nye og eksisterende integrasjoner
- Identifisere årsaker til driftsproblemer som f.eks. avdekke flaskehalser som kan oppstå etter produksjonssetting som igjen kan gi redusert eller mangel på tilgang til helse- og personopplysninger
- Bytte av system eller leverandør som medfører konvertering av data

Et testmiljø kan etableres som en permanent løsning (kopi av produksjonsmiljøet) eller ha en tidsavgrenset varighet. Der det er mulig bør det benyttes anonymiserte testdata.

Grunnkrav for etablering og bruk av testdata

a) Personer som primært driver med systemutvikling og -vedlikehold skal som regel ikke ha tilgang til helse- og personopplysinger, men det ligger i sakens natur at de under sitt arbeid vil kunne komme til å få tilgang til helse- og opplysninger. Det må likevel tilstrebes at dette begrenses i den grad det er mulig. For eksempel gjennom anonymisering av testdata

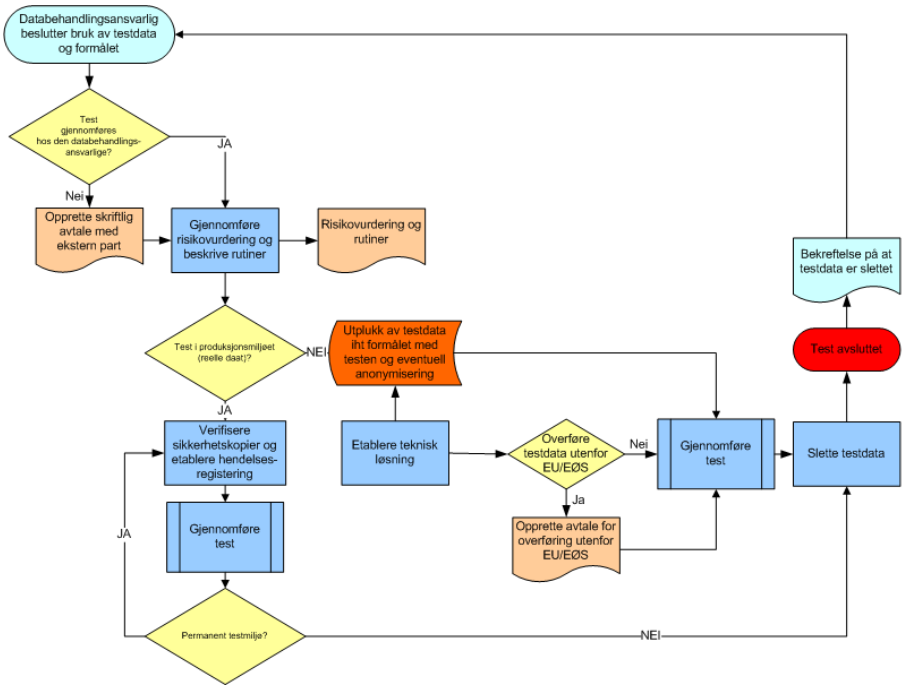
b) Den dataansvarlige skal påse at eksterne parter som kan få tilgang til helse- og personopplysninger oppfyller kravene i Normen. Det vil i hovedsak dreie seg om databehandlere, leverandører eller andre helsevirksomheter
c) Det må foreligge en skriftlig (databehandler-) avtale mellom den dataansvarlige og den part som vil kunne få tilgang til helse- og personopplysninger

Etablering og bruk av testdata

Nr.	Handling
1.	**Forberedelser** a) Ved bruk av ekstern part til gjennomføring av testing skal den dataansvarlige opprette skriftlig avtale med ekstern part (databehandler, leverandør, virksomhet) som skal ha tilgang til testdata. Avtalen må dekke: - Formålet med og varigheten av testen (se ovenfor for eksempler) - Normen gjelder og skal følges - Hvilke roller som er ansvarlig for hva (f.eks. prosjektleders rolle) - Bruk av identifiserbare helse- og personopplysninger eller anonymiserte data - Utplukk av hele eller deler av datasettet - Separat testmiljø eller test på data i produksjonsmiljøet - Hvem som skal ha tilgang til testdataene og prosedyrene for tilgangsstyring - Taushetsplikt - Gjennomføring av risikovurdering av bruk av testdata - Fysisk og logisk sikring - Varigheten på testdata og tiltak for sletting av data når testen er avsluttet - Hvilke særskilte prosedyrer som gjelder b) Avklare roller: - Det skal avklares ansvar og arbeidsoppgaver til ulike roller internt i helsevirksomheten og hos ekstern part c) Vurdere bruk av identifiserbare data eller anonymiserte data: - Som et utgangspunkt bør det benyttes anonymiserte data - Bruk av identifiserbare testdata kan være ved: o Testkonvertering for å ivareta integriteten, hvor hovedregelen er at både konvertering og test av resultatet må foretas på reelle data for å kunne teste en fullstendig konvertering o Integrasjoner der det i de fleste tilfeller er nødvendig med tilnærmet fullstendige og reelle data, for å kunne få til en realistisk kommunikasjonstest med eksterne parter d) Gjennomføre risikovurdering av testmiljøet: - Ut fra akseptkriteriene bør risikovurderingen hensynta omfanget av helse- og personopplysinger i testdataene, antall som skal ha tilgang til testdata og testens varighet - Bruk av separat testmiljø eller test på reelle data i produksjonsmiljøet - Test på identifiserbare eller anonymiserte data - Det fysiske testmiljøet o Fysisk og logisk skille mellom testdata og produksjonsdata o Fysisk og logisk driftsmiljø - Tilgangsstyring, hendelsesregistrering og oppfølging av tilgangsstyringen e) Ved etablering av testdata skal det utarbeides prosedyre for: - Utplukk av testdata fra eksisterende registre (for eksempel EPJ-system) - Anonymisering av testdata - Bruk av testdata - Tilgangsstyring til testdata

Nr.	Handling
	- Overføring av testdata til andre (databehandler, leverandør, virksomhet). For overføring til virksomheter i utlandet, se http://www.datatilsynet.no/Sektor/Overfoering/ - Sletting av testdata etter at test er gjennomført f) Etablere teknisk løsning for behandling av testdata: - Det bør etableres enten et fysisk eller logisk (logiske adskilt database) skille mellom produksjonsmiljø og testmiljø om testen ikke skal foregå i produksjonsmiljøet - Overføring av testdata til testmiljø utenfor dataansvarliges eget nettverk innebærer økt eksponering av risiko. For å gjøre dette på en forsvarlig måte bør det benyttes mekanismer som sikrer at data kommer frem til rett mottaker, og er gjort utilgjengelig for uvedkommende ved tilstrekkelig kryptering. Hva gjelder krypteringsstyrke, tilrådes det å følge Datatilsynets til enhver tids fastsatte anbefaling. Ved overføring av større mengder opplysninger eller gjentatt samhandling bør det benyttes PKI som baseres på kvalifiserte sertifikater. Slike systemer vil både sikre korrekt autentisering av motparten, en trygg forsendelse og eventuell ikke-benektning i den grad det er av betydning. Om det benyttes identifiserbare testdata skal teknisk løsning etableres og sikres tilsvarende produksjonsmiljøet - For testing av EDI-meldinger vises det til Helsedirektoratet, avdeling standardisering (EISI) sin testserver for meldinger: http://www.kith.no/templates/kith_WebPage____576.aspx
2.	**Gjennomføring** a) Utplukk av testdata til det konkrete formålet: - Utplukksregler skal beskrives iht det fastsatte formålet - Prosessen med utplukk av testdata skal sikres iht Normen. Dette er i realiteten en egen behandling av helse- og personopplysninger - Testdata skal i størst mulig grad anonymiseres b) Test på reelle data: - Før testen skal det verifiseres at det er tatt sikkerhetskopier og at det fins prosedyrer for tilbakekopiering om testen korrumperer data - Det skal føres hendelsesregistre - Det anbefales å føres manuelle hendelsesregistre over endringer for å kunne spore uønskede hendeler til konkrete operasjoner og tidspunkter
3.	**Avslutning/opprydding** a) Ved tidsavgrenset bruk skal testdataene slettes når formålet er nådd b) I permanente testmiljøer skal testdata som ikke lenger har et formål slettes c) Ansvarlig for bruk av testdata skal sende bekreftelse til dataansvarlig at alle testdata er slettet ift formål og avtale

Illustrasjon på prosessflyt


Databehandlingsansvarlig beslutter bruk av testdata og formålet
Test gjennomføres hos den databehandlings-ansvarlige?
JA
Nei
Opprette skriftlig avtale med ekstern part
Gjennomføre risikovurdering og beskrive rutiner
Risikovurdering og rutiner
Test i produksjonsmiljøet (reelle daat)?
NEI
Utplukk av testdata iht formålet med testen og eventuell anonymisering
JA
Verifisere sikkerhetskopier og etablere hendelses-registering
Etablere teknisk løsning
Overføre testdata utenfor EU/EØS
Nei
Gjennomføre test
Slette testdata
Ja
Opprette avtale for overføring utenfor EU/EØS
Gjennomføre test
JA
Permanent testmiljø?
NEI
Test avsluttet
Bekreftelse på at testdata er slettet