norskhelsenett

Testdatapolicy

Senter for test og kvalitetssikring– Norsk Helsenett SF

Versjon	Dato	Produsent	Eier/forankret hos
1.0	22.05.18	Guro Nordengen	Fiona Ring Østensvig Arne Erik Hurum
2.0	04.01.19	Siri P. Johansen og Guro Nordengen	Per-Morten Rummelhoff
2.1	23.04.19	Siri P. Johansen og Guro Nordengen	Per-Morten Rummelhoff
2.2	23.09.20	Fiona Ring Østensvig	

Innholdsfortegnelse

1 INNLEDNING

1.1 HENSIKT

Dette dokumentet har til hensikt å gi retningslinjer for håndtering av data som benyttes til testformål hos Norsk helsenett – her omtalt som testdata.

Testdata er data som behandles med testing (se kapittel 1.3) som formål.

Primærmålgruppen for dokumentet er alle ansatte i Norsk helsenett som behandler testdata.

Sekundærmålgruppen er alle integrerende aktører, for eksempel EPJ-systemer, RHF-er og Helsedirektoratet, som enten benytter seg av Norsk helsenett sine testdata, eller bringer egne testdata inn i Norsk helsenett sine testmiljøer.

1.2 DEFINISJONER

Ulike former for databearbeidelse før testing	
Ingen bearbeidelse	Produksjonslike/skarpe data
Pseudonymisering	Behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar fysisk person.[1]
Anonymisering	Behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til et identifiserbart individ, når man tar i betraktning alle de hjelpemidlene som med rimelighet kan tenkes brukt for å identifisere vedkommende. Prosessen må være irreversibel.[2]
Syntetisering	Konstruerte, fiktive data uten rot i produksjonsdata.

[1] https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#* Artikkel 4, nummer 5
[2] https://www.datatilsynet.no/globalassets/global/regelverk/veiledere/anonymisering-veileder-041115.pdf

Ulike former for testdata	
Statiske testdata	Testdata som enten ikke kan endres, eller som vil resettes tilbake til en nulltilstand ved jevne mellomrom.
Bevarte testdata	Testdata som ikke vil bli overskrevet av nye data ved bygging av en ny database.
Dynamiske testdata	Testdata som på ulikt vis forandrer seg automatisk i et testmiljø, for eksempel ved at et datasett simulerer en livssyklus (testpersoner blir født, andre dør, noen blir gift, noen utvandrer osv.).

Øvrige begrep	
Personopplysning	Enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.[3]
Testdata	Data som behandles med test som formål

1.3 INTRODUKSJON TIL TESTING OG TESTDATA

Under utvikling og forvaltning av produkter og tjenester, er test og kvalitetssikring en systematisk prosess for å vurdere om et produkt eller en tjeneste som utvikles oppfyller spesifikke krav (deriblant sikkerhets- og kvalitetskrav). Norsk helsenett har en egen avdeling som er viet til test og kvalitetssikring.

[3] https://lovdata.no/dokument/NL/lov/2018-06-15-38/*#* Artikkel 4, nummer 1

En tydelig og robust test- og kvalitetssikringsprosess øker kvaliteten på, og tilliten til produktet. Samtidig bidrar det til økt troverdighet til Norsk Helsenetts nasjonale løsninger.

For å kunne gjennomføre prosessene for test og kvalitetssikring, har produktene hos Norsk helsenett flere utviklings- og testmiljøer på ulike nivåer som koden må gjennom før løsningene produksjonssettes til et produksjonsmiljø. I et produksjonsmiljø er løsningene tilgjengelig for sluttbruker. Hvert utviklings- og testmiljø har stort sett egne databaser som inneholder testdata som kan benyttes til testaktiviteter i de enkelte miljøene.

Test- og kvalitetssikringsaktiviteter simulerer potensielle situasjoner som kan/vil skje i produksjonsmiljøet. Det er viktig at testene dekker både typiske situasjoner og unntakssituasjoner, slik at det sikres at løsningen håndterer ulike situasjoner på riktig måte. Samtidig må løsningen tilfredsstille en rekke ytelses- og sikkerhetskrav, og tåle ulike former for last.

For at man skal kunne gjennomføre en test- og kvalitetssikringsprosess med tilstrekkelig kvalitet, er man avhengig av to forhold. For det første er man avhengig av testmiljøer med produksjonslik kvalitet. For det andre er man avhengig av testdata med produksjonslik kvalitet og kvantitet. En mulighet for å fylle disse kriteriene, er å teste med produksjonsdata. Da skaper man en situasjon som i svært stor grad ligner den fremtidige situasjonen i produksjonsmiljøet. Som utgangspunkt benytter Norsk helsenett seg ikke av en slik løsning dersom disse dataene inneholder *personopplysninger*, da det er krevende å gjennomføre de nødvendige test- og kvalitetsaktivitetene innenfor personopplysningslovens rammer. Unntak gjelder for enkelte testdata om helsepersonell som allerede er offentlig tilgjengelig informasjon, se nærmere beskrivelse i kapittel 3.2.

Da testaktiviteter har til hensikt å sikre en produksjonssituasjons stabilitet, trygghet og forutsigbarhet, så er det fordelaktig at testsituasjonen er så lik produksjonssituasjonen som mulig. Dette innebærer at kompleksitet og variasjon i testdataene skal tilsvare reelle produksjonsdata, i tillegg til at volumet bør tilstrebes å tilsvare produksjon. Dette er spesielt viktig i akseptansetestmiljøet.

Produksjonsdata som ikke inneholder personopplysninger, for eksempel virksomhetsdata, kan i all hovedsak brukes til testformål, forutsatt at de blir tilgangsstyrt på samme måte i testmiljøet og produksjonsmiljøet. Produksjonsdata som inneholder personopplysninger som ikke er offentlige krever større aktsomhet for å kunne benyttes til testformål, og er å anse som et avvik, se kapittel 5.

2 OVERORDNET

2.1 TESTAKTIVITETER OG TESTMILJØER

Typiske testaktiviteter hos Norsk helsenett er eksempelvis systemtest, verdikjedetest og akseptansetest. Det kan leses mer om ulike testaktiviteter i Norsk helsenett sin teststrategi.

Typiske ulike typer testmiljøer hos Norsk helsenett er utviklingsmiljøer, systemtestmiljøer og akseptansetestmiljøer. Det kan leses mer om ulike aktiviteter i ulike miljøer i Norsk helsenett sin testpolicy.

2.2 ULIKE FORMER FOR TESTDATA

2.2.1 PERSONDATA

Testdata som omhandler personer, kan grovt sett deles i to:

1. Testdata med personopplysninger
2. Testdata uten personopplysninger

Eksempler på testdata med personopplysninger: skarpe data og pseudonymiserte testdata.

Eksempler på testdata uten personopplysninger: anonymiserte testdata og syntetiske testdata.

2.2.2 ØVRIG DATA

Eksempler på data som typisk ikke omhandler personer:

- Virksomhetsdata
- Sertifikater
- Produktinformasjon

3 PERSONOPPLYSNINGSLOVENS ANVENDELSE PÅ TESTDATA

Lov om behandling av personopplysninger (personopplysningsloven) av 15. juni 2018 nr. 38 kommer til anvendelse ved behandling av personopplysninger. Personopplysningsloven består av nasjonale regler og EUs personvernforordning (GDPR - General Data Protection Regulation).

Lovens saklige virkeområde fremkommer av forordningens art 2 punkt 1 «Denne loven får anvendelse på helt eller delvis automatisert behandling av personopplysninger og på ikkeautomatisert behandling av personopplysninger som inngår eller skal inngå i et register».

Forordningens art 4 definerer personopplysninger som «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)».

Når Norsk helsenett behandler digitale data, kan behandlingen utløse plikter og rettigheter etter personopplysningsloven. Behandlingen utløser imidlertid kun plikter og rettigheter etter personopplysningsloven dersom behandlingen gjelder personopplysninger, jf. forordningens art 2 punkt 1 og art 4, i og med at personopplysningsloven bare gjelder opplysninger som angår enkeltpersoner. Definisjonen av «personopplysning» er avgjørende for lovens anvendelse. Anonyme eller anonymiserte data kan ikke lenger knyttes til en enkeltperson og er ikke omfattet av personopplysningsloven. Det samme gjelder data som ikke knytter seg til personer i det hele tatt. Data er anonyme hvis det ikke lenger er mulig, med de hjelpemidlene som med rimelighet kan tenkes å ha blitt brukt, å identifisere enkeltpersoner i datasettet.

Å anonymisere data dreier seg om å fjerne muligheten for å identifisere enkeltpersoner i et datasett, ved å bearbeide datasettet slik at man gjør tilknytningen mellom informasjon og individ umulig. Det er kun snakk om reell anonymisering hvis prosessen er irreversibel. Det betyr at det ikke skal være mulig å gjenfinne koblingen mellom informasjonen om enkeltindivid, når man tar i betraktning de hjelpemidlene som med rimelighet kan tenkes brukt.

Å anonymisere data er utfordrende, og det er mer utfordrende i dag enn det var tidligere. Det er større fare for reidentifisering fordi det finnes et enormt tilfang av offentlig tilgjengelige data, kombinert med tilgang til stadig billigere og mer kraftfull analyseteknologi. Det er derfor viktig å foreta grundige risikovurderinger før anonyme data eventuelt benyttes, og bruke solide anonymiseringsteknikker.

3.1 BEHANDLING AV TESTDATA SOM OMHANDLER PASIENTER (PASIENTDATA)

I Norsk helsenett er utgangspunktet at behandling av testdata som angår enkeltpersoner kun gjennomføres med syntetiske (eller eventuelt anonymiserte) testdata.

Syntetiske testdata innebærer at dataene er konstruert og ikke har rot i virkeligheten, og dataene knytter seg ikke til reelle personer. Anonymiserte testdata innebærer at dataene ikke lenger kan identifisere enkeltpersoner i datasettet, med de hjelpemidlene som med rimelighet kan tenkes å ha blitt brukt.

Personopplysningsloven kommer ikke til anvendelse på Norsk helsenetts behandling av testdata som gjennomføres med syntetiske (eller eventuelt anonymiserte) pasientdata.

3.2 BEHANDLING AV TESTDATA SOM OMHANDLER HELSEPERSONELL – OPPLYSNINGER SOM ER OFFENTLIG TILGJENGELIG

I noen tilfeller behandler Norsk helsenett testdata som angår helsepersonell (som enkeltpersoner). I disse tilfellene gjenbrukes kun informasjon som allerede er offentlig tilgjengelig.
Dette gjelder informasjon som finnes i Helsepersonellregisteret (HPR) og Legestillingsregisteret (LSR). Testversjonen av disse registrene beholder noe offentlig tilgjengelig informasjon som også benyttes i produksjon (for eksempel HPR-nummer, autorisasjoner og fødselsdato). Ikke-offentlig informasjon (for eksempel fødselsnummer, dødsdato, avsluttetstatus, utdanning, suspensjoner, LSRkommentarer m.v.) fjernes og opprettes på nytt syntetisk. Informasjon som hentes fra disse registrene kobles til en fiktiv person i test-PREG med samme fødselsdato (offentlig informasjon) som den registrerte.

Etter personvernforordningen art 6. kreves et behandlingsgrunnlag ved behandling av personopplysninger. Med hjemmel i art. 6 punkt 1 bokstav f) som sier at en virksomhet kan behandle personopplysninger dersom det er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes personvern, kan Norsk helsenett behandle testdata om helsepersonell som allerede er offentlig tilgjengelig informasjon.

4 HÅNDTERING AV TESTDATA

Prinsippet om at Norsk helsenett som utgangspunkt benytter seg av syntetisk/anonymiserte testdata, gjelder i alle ledd i test- og utviklingsprosessen, både for interne og eksterne aktører. I tillegg har Norsk helsenett generelle retningslinjer for hvordan man skal håndtere testdata fra et testfaglig perspektiv.

4.1 INTEGRASJON MOT NORSK HELSENETTS TESTMILJØER

I de tilfeller der integrerende aktør kobler seg på testmiljøene til Norsk helsenett og tilfører sine testdata i testmiljøene eller bruker Norsk helsenetts løsninger for å vise eller videreformidle data/informasjon, krever Norsk helsenett at aktørene stiller med tilfredsstillende testdata – det vil si syntetiske eller anonymiserte testdata.

I de tilfeller der integrerende aktør behandler Norsk helsenetts testdata i sine egne systemer, krever Norsk helsenett at disse testdataene ikke behandles (kobles opp mot eller brukes sammen med) med data som angår enkeltpersoner og inneholder personopplysninger. Norsk helsenetts syntetiske (eventuelt anonymiserte) testdata skal kun behandles sammen med andre tilfredsstillende testdata – det vil si syntetiske eller anonymiserte testdata.

4.2 OPPRETTELSE AV TESTDATA

Ved opprettelse eller endring av testdata, må man påse at man ikke benytter seg av testdata som angår reelle personer og inneholder personopplysninger.

For at testaktivitetene skal kunne sikre produksjonssituasjonens stabilitet, trygghet og forutsigbarhet, er det fordelaktig om testsituasjonen er så lik produksjonssituasjonen som mulig. Dette innebærer at kompleksiteten og variasjonen i testdataene bør tilsvare reelle produksjonsdata, i tillegg til at volumet bør tilstrebes å tilsvare produksjon.

4.3 GENERELL BRUK AV TESTDATA

Som utgangspunkt skal brukerne av testdata sørge for å variere sin bruk slik at testdataenes mangfold blir utnyttet i testene. Norsk helsenett fraråder å ta i bruk statiske uttrekk av testdata som brukes over lengre perioder.

Man skal til enhver tid bestrebe å være uavhengig av enkeltelementer av testdata. I alle tilfeller hvor det er mulig, bør man lete opp nye, relevant testdata i forkant av hver testkjøring. Dette gjelder både for

manuelle og automatiske tester. Testdata bør ikke lagres i statiske oversikter, og heller ikke hardkodes inn i tester.

Typiske tilfeller hvor det kan være aktuelt å vike fra utgangspunktet som nevnt over, er:

- Retest av bug
- Avhengighet til ytre faktorer (som smartkort, enkelte integrasjoner e.l.)

4.4 AUTOMATISKE TESTER

Automatiske tester bør, dersom mulig, både opprette og slette testdata som en del av testen. Har testen utført endringer på testdata som testen ikke har opprettet, bør disse tilbakestilles som en del av testen. Automatiske tester som ikke oppretter testdata bør, dersom mulig, hente ut testdata automatisk. Dette kan gjøres ved bruk av søkeverktøy. Slik vil man kunne teste med ulik testdata hver gang en test kjøres (enten manuelt eller automatisk), med kun testdatakravene fra testcaset som fellestrekk, og dermed øke testdekningen.

5 AVVIKSHÅNDTERING

I Norsk helsenett anses to forhold som avvik fra Norsk helsenetts testdatapolicy:

1. Norsk helsenett eller integrerende aktør benytter pasientdata eller andre persondata som ikke er offentlig informasjon om helsepersonell til testing
2. Norsk helsenett eller integrerende aktør benytter testdata som ikke er av god nok kvalitet eller tilstrekkelig kvantitet

Testleder har det overordnede ansvaret for å ha oversikt over situasjonen på testdata og kontrollere at testdataene er i henhold til Norsk helsenetts testdatapolicy. I dette ansvaret ligger for det første å sikre at Norsk helsenett som utgangspunkt kun behandler syntetiske eller anonymiserte testdata hvis det angår enkeltpersoner. Norsk helsenett forutsetter at eventuelle integrerende aktører praktiserer åpenhet vedrørende sine testdataforhold. For det andre har testleder ansvaret for å kontrollere kvalitet og kvantitet på Norsk helsenetts testdata og eventuelle integrerende aktørs testdata.

Når testleder har mistanke om avvik fra Norsk helsenetts testdatapolicy skal følgende prosess følges:

1. Eskalere håndtering av avviket til nærmeste leder
2. Dokumentere avviket og årsaken til/begrunnelsen for avviket
3. Gjennomføre RoS. Eventuelle tiltak må dokumenteres

4. Endelig beslutning av hvorvidt avviket aksepteres (med eller uten eventuelle tiltak) tas på avdelingsdirektør-nivå