Direktoratet for e-helse

Bruk av direkte identifiserbare helseopplysninger til utvikling og testing av behandlingsrettede helseregistre

Veiledning til praktisering av pasientjournalloven § 11 annet ledd

HITR 1252:2023

Publikasjonens tittel:
Bruk av direkte identifiserbare helseopplysninger til utvikling og testing av behandlingsrettede helseregistre: Veiledning til praktisering av pasientjournalloven § 11 annet ledd.

Rapportnummer
HITR 1252:2023

Utgitt:
November 2023

Utgitt av:
Direktoratet for e-helse

Kontakt:
postmottak@ehelse.no

Publikasjonen kan lastes ned på:
www.ehelse.no

Innhold

1 Innledning

1.1 Bakgrunn

Stortinget vedtok 10. juni 2022 et nytt annet ledd i pasientjournalloven § 11, angående bruk av helseopplysninger til utvikling og testing av behandlingsrettede helseregistre. Bestemmelsen har følgende ordlyd:

> *«Direkte identifiserbare helseopplysninger kan behandles i lukkede testmiljøer for å utvikle og teste behandlingsrettede helseregistre dersom det er umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke pseudonyme, anonyme eller fiktive opplysninger».*

Det presiseres i pasientjournalloven § 11 fjerde ledd at helseopplysningene i disse tilfellene kan behandles uten hinder av taushetsplikt, og at det ikke er nødvendig å innhente samtykke fra pasienten.

Lovbestemmelsen og retningslinjen kan være relevant ved utvikling og testing blant annet av

- elektroniske pasientjournalsystemer
- løsninger for pasientadministrasjon
- andre applikasjoner knyttet til et behandlingsrettet helseregister

Lovbestemmelsen omfatter også de tilfeller der utvikling og testing foregår med automatiske prosesser.

Følgende situasjoner vil imidlertid falle utenfor lovbestemmelsen:

- Utviklings- og testaktiviteter som ikke skjer i lukkede testmiljøer
- Prøvedrift som skjer utenfor lukkede testmiljøer
- Migrering av data ved bytte av journalsystem

Bestemmelsen er omtalt i lovforslaget i Prop. 91 L (2021-2022) Endringer i pasientjournalloven mv. (nasjonal digital samhandling), hvor det i kapittel 7 fremgår at bakgrunnen for lovforslaget var behovet for en klarere hjemmelssituasjon. Det presiseres at bestemmelsen er ment å være en snever unntaksbestemmelse, men ikke utgjør en endring av gjeldende rett. Forarbeidene presiserer også i noen grad vilkårene som må være oppfylt for å kunne benytte helseopplysninger i forbindelse med utvikling og testing av behandlingsrettede helseregistre.

Det er videre en forutsetning at virksomheten allerede har rettslig grunnlag for å behandle helseopplysningene i et behandlingsrettet helseregister. Også andre bestemmelser i helselovgivningen vil kunne være relevante, for eksempel retten til innsyn.

Lovteksten bruker uttrykket «direkte identifiserende helseopplysninger» om de opplysningene som kan benyttes til utvikling og testing dersom vilkårene er oppfylt. I forarbeidene omtales dette også som «reelle journalopplysninger». Der retningslinjen nedenfor benytter uttrykket «helseopplysninger», menes helseopplysninger som er direkte identifiserbare. Uttrykket omfatter også pasientrelaterte opplysninger som ikke nødvendigvis vil oppfattes som helseopplysninger, men som er taushetsbelagt etter helsepersonelloven § 21 og som benyttes i forbindelse med utvikling eller testing. Begrepet er nærmere beskrevet og avgrenset i kapittel 5.3.

Begrepet «behandlingsrettet helseregister» er et vidt begrep, og omfatter helsevirksomheters hovedjournal, pasientkort, individuell plan, radiologisystemer, laboratoriesystemer, andre typer fagsystemer, pasientadministrative systemer, Nasjonal kjernejournal og andre

systemer der helseopplysninger kan være registrert. Begrepet er nærmere forklart i kapittel 5.2.

Lovproposisjonen slår videre fast at begrepet «teste» i denne sammenhengen også kan omfatte «prøvedrift». Det presiseres samtidig at prøvedrift kun vil være omfattet når det skjer i et lukket testmiljø. Andre former for prøvedrift vil falle utenfor hjemmelen i pasientjournalloven § 11.

Disse og en rekke andre begreper er forklart i kapittel 5. For å sikre best mulig forståelse av begrepene som benyttes i retningslinjen, anbefales det at leseren setter seg inn i disse.

Dersom en virksomhet velger ikke å følge anbefalingene i retningslinjen, bør dette være basert på en konkret og begrunnet vurdering. Begrunnelsen for å fravike retningslinjen bør dokumenteres.

All bruk av eksempler nedenfor er kun ment å være til illustrasjon. Virksomheten må i alle tilfeller gjøre en konkret og selvstendig vurdering av om vilkårene i pasientjournalloven § 11 annet ledd er oppfylt, og om valgte sikkerhetstiltak er tilstrekkelige for å lukke testmiljøet.

1.2 Målgruppe

Dette dokumentet er relevant for virksomheter i helse- og omsorgssektoren som har etablert et behandlingsrettet helseregister og som skal planlegge, beslutte eller gjennomføre utvikling eller testing av virksomhetens behandlingsrettede helseregistre med helseopplysninger. Det retter seg mot alle personer som blir involvert i prosessen som ledere, helsepersonell, øvrige ansatte og innleid personell og er særlig relevant for personell innen fagområdene informasjonssikkerhet, personvern, IT og medisinsk teknologi.

Dersom den dataansvarlige beslutter å engasjere en leverandør til å utføre utviklings- og testoppgaver, vil anbefalingene og tiltakene gjelde for leverandøren og eventuelle underleverandører. Dette omfatter også IKT-driftsorganisasjoner i spesialisthelsetjenesten og virksomheter i interkommunale samarbeid. Den dataansvarlige bør instruere leverandører om å følge anbefalingene og tiltakene, og vurdere om det er behov for tilføyelser til databehandleravtalen. Se også kapittel 4.2 om databehandleravtaler.

Dersom to eller flere virksomheter har delt dataansvar for det behandlingsrettede helseregisteret, må det være avklart mellom partene hvilken virksomhet som skal ha ansvaret for utviklingen eller testingen.

1.3 Involvering i vurderinger og beslutninger

En rekke ressurser bør involveres i vurderingene og beslutningene når helseopplysninger benyttes til utviklings- og testformål, herunder informasjonssikkerhetsressurser, personvernombud, brukerrepresentanter, avdelingsleder, klinikkleder med flere.

En beslutning om å benytte helseopplysninger til utviklings- og testformål må tas på riktig nivå i virksomheten, for eksempel i henhold til en fullmaktsmatrise eller lignende.

1.4 Om dokumentet

Dokumentet beskriver lovens vilkår for å benytte direkte identifiserbare helseopplysninger til utviklings- og testformål i kapittel 2, og vurderinger den dataansvarlige bør foreta dersom utviklings- eller testformålet ikke kan oppnås med fiktive (syntetiske), anonyme eller pseudonyme data.

Dokumentet gir dernest, i kapittel 3, eksempler på risikoreduserende tiltak som kan bidra til å lukke et testmiljø. Dette kan omfatte testplan, risikovurderinger og DPIA, tilgangsstyring, logging mv. Oversikten er ikke uttømmende.

Helsevirksomheter har plikt til å etablere behandlingsrettede helseregistre for helsepersonells dokumentasjonsplikt, og har rettslig grunnlag for behandlingen av helseopplysningene i helsepersonelloven og i pasientjournalloven. All behandling av helseopplysninger må følge pasientjournallovens regler, også når slike opplysninger benyttes til utviklings- og testformål. Utover de vilkårene som følger direkte av pasientjournalloven § 11 annet ledd, er det flere forhold som må vurderes før virksomheten kan ta i bruk helseopplysninger til utvikling og testing, herunder tiltak for å ivareta taushetsplikten. En ikke-uttømmende oversikt er inntatt i kapittel 4.

2 Vilkår for å bruke helseopplysninger til utviklings- og testformål

Pasientjournalloven § 11 annet ledd oppstiller følgende vilkår, der alle må være oppfylt for at det skal være lovlig å benytte helseopplysninger til utvikling og testing:

- Utviklingen og testingen må skje i et lukket testmiljø.
- Formålet må være å utvikle og teste behandlingsrettede helseregistre.
- Det må være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å bruke pseudonyme, anonyme eller fiktive opplysninger.

2.1 Utviklingen må skje i et lukket testmiljø

Utviklings- og testmiljøer der det benyttes direkte identifiserbare helseopplysninger må være robuste og hindre at uvedkommende får tilgang til helseopplysningene. Det er først når det er innført tilstrekkelige tiltak for å lukke utviklings- eller testmiljøet og testmiljøets samlede risikobilde er vurdert og akseptert av virksomheten, at testmiljøet kan vurderes som lukket i henhold til pasientjournalloven § 11 annet ledd.

Virksomheten har i denne forbindelse også plikt til å ta hensyn til utviklingen i risikobildet og den teknologiske utviklingen. Endringer i risikobildet vil for eksempel kunne gjøre det nødvendig med andre sikkerhetstiltak enn de som først ble innført.

Se kapittel 3 for en beskrivelse av tiltak som kan bidra til å lukke et testmiljø.

2.2 Formålet må være å utvikle og teste behandlingsrettede helseregistre

All behandling av personopplysninger, herunder helseopplysninger, skal ha et uttrykkelig angitt og berettiget formål, jf. personvernforordningen art. 5 nr. 1 bokstav b.

Før helseopplysninger kan benyttes til utvikling og testing, må den dataansvarlige angi hva som er formålet med behandlingen av opplysningene. Basert på det definerte formålet skal det gjøres uttrekk som er tilpasset til utviklingen eller testingen som skal gjennomføres. Utviklings- og testaktiviteten skal ikke ha større omfang enn det som er nødvendig for å oppnå formålet med denne, og det skal ikke benyttes flere helseopplysninger enn det som er nødvendig. Se også kapittel 4.5 om dataminimering og 3.5 om vurdering av datagrunnlaget.

Helseopplysninger som er kopiert til bruk i utvikling og testing, kan ikke benyttes for andre formål, jf. prinsippet om formålsbegrensning. Se kapittel 3.8 om sletting.

2.3 Kan formålet oppnås ved å benytte fiktive, anonyme eller pseudonyme opplysninger?

Det må alltid vurderes om det konkrete utviklings- eller testformålet kan oppnås ved bruk av fiktive, anonyme eller pseudonyme opplysninger. Utvikling og testing ved bruk av direkte identifiserbare helseopplysninger kan bare gjennomføres dersom formålet med utviklingen eller testingen ikke kan oppnås med «pseudonyme, anonyme eller fiktive opplysninger». Det er for eksempel ofte et større behov for å benytte helseopplysninger i prosjektenes sluttfase, nært opptil produksjonssetting, for å sikre at integriteten på helseopplysningene i løsningen blir ivaretatt i en driftssituasjon.

Pasientjournalloven § 11 annet ledd gir ikke noen prioritering mellom de ulike typene av datasett, men den dataansvarlige skal alltid velge den tilnærmingen som kan oppfylle formålet med lavest risiko for inngrep i personvernet (se kapittel 4.5 om dataminimering). Dette betyr at virksomheten først må vurdere om formålet kan oppnås ved fiktive opplysninger, deretter anonyme data og deretter pseudonyme data. Adgangen til å benytte helseopplysninger skal altså forstås som et snevert unntak fra en hovedregel om å benytte ikke-identifiserbare opplysninger.

2.4 Vurderingen av vilkåret «umulig eller uforholdsmessig vanskelig»

Bestemmelsen oppstiller en høy terskel for å bruke helseopplysninger til utviklings- og testformål (”umulig eller uforholdsmessig vanskelig”). Helsevirksomheten må foreta en konkret vurdering av om det er forhold ved utviklingen eller testingen som gjør at vilkåret er oppfylt.

Med ”umulig”, menes at formålet med utviklingen og testingen ikke på noen måte kan nås ved bruk av fiktive, anonyme eller pseudonyme opplysninger. Den eneste måten formålet kan oppnås på, vil altså være å benytte helseopplysninger. Eksempelvis vil fiktive opplysninger ikke alltid ha de egenskapene som er nødvendige for å kvalitetssikre systemet før produksjonssetting.

Det vil imidlertid, i de aller fleste tilfeller, være praktisk mulig å oppnå formålet med utviklingen eller testingen ved å benytte fiktive, anonyme eller pseudonyme opplysninger. Dersom virksomheten selv ikke er i stand til å generere fiktive eller anonyme opplysninger, bør det undersøkes om fiktive opplysninger av nødvendig kvalitet kan fremskaffes på annen måte.

En konkret vurdering kan imidlertid tilsi at det i noen tilfeller vil være uforholdsmessig vanskelig å benytte fiktive, anonyme eller pseudonyme opplysninger fremfor helseopplysninger. Dette betyr at ulempene ved å benytte ikke-identifiserbare opplysninger må være uproporsjonalt store sammenlignet med formålet som søkes oppnådd med testingen eller utviklingen. Det må, i det konkrete tilfellet, være så vanskelig å oppnå formålet med utviklingen eller testingen at bruk av fiktive, anonyme eller pseudonyme opplysninger med stor sannsynlighet vil medføre så dårlig kvalitet på resultatet at det ikke kan tillegges tillit i en driftssituasjon.

Forholdsmessighetsvurderingen må baseres på momenter som kan være relevante, og da spesielt hva som kan oppnås ved å benytte helseopplysninger til utviklingen eller testingen og hvor omfattende inngrep i personvernet dette vil medføre.

Det må også alltid vurderes om det er nødvendig at alle fasene i et utviklings- og testløp gjennomføres med bruk av helseopplysninger.

Den konkrete vurderingen skal dokumenteres, jf. forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 5 annet ledd.

I det følgende omtales noen momenter som kan ha betydning ved forholdsmessighets-vurderingen. Oversikten er ikke uttømmende.

2.4.1 Pasientsikkerhet

Det vil alltid være et grunnleggende krav til helsevirksomheten at pasientsikkerheten ivaretas, og pasientsikkerhet vil derfor være et særlig viktig moment i vurderingen. Virksomheten må altså vurdere hvordan pasientsikkerheten kan bli påvirket av valget av utviklings- eller testdatasett. Ved bruk av ikke-identifiserbare data, kan pasientsikkerheten eksempelvis bli utfordret ved at testen ikke gir resultater av tilstrekkelig god kvalitet, og at systemet derfor ikke virker som forutsatt i produksjon.

Pasientsikkerheten vil imidlertid også kunne bli utfordret ved bruk av helseopplysninger, eksempelvis ved at data fra et testmiljø kan bli overført til produksjonsmiljøet. Det vil også kunne være risiko for at klinisk personell som har tilgang til testmiljøet ikke alltid er oppmerksom på at de jobber i et testmiljø, og derfor tar beslutninger på bakgrunn av uriktige opplysninger, eller dokumenterer pasientbehandling i feil miljø.

Hvorvidt pasientsikkerheten vil kunne påvirkes, må vurderes i forkant av utviklingen eller testingens oppstart, eksempelvis i en risiko- og sårbarhetsvurdering.

2.4.2 Oppfyllelse av pasientrettigheter

Virksomheten må alltid vurdere om de berørte pasientenes rettigheter etter personvernforordningen og helselovgivningen kan oppfylles der helseopplysninger benyttes til utvikling eller testing. Det må eksempelvis vurderes om det vil være mulig å gi pasienten innsyn i databehandlingen etter personvernforordningen artikkel 15.

Dersom helsevirksomheten ikke vil være i stand til å oppfylle den registrertes rettigheter, eksempelvis ved ikke å kunne gi innsyn i databehandlingen som følge av manglende loggkapabilitet i testmiljøet, kan det ikke benyttes helseopplysninger.

2.4.3 Tid og ressursbruk

Det følger av forarbeidene at det blant annet kan legges vekt på om det vil være «svært tid- og ressurskrevende for aktøren å lage anonyme eller fiktive opplysninger». Tidsbruken eller ressursbruken må imidlertid også her være uproporsjonalt høy sammenlignet med formålet som søkes oppnådd med testingen eller utviklingen.

At virksomheten har begrenset tilgang på ressurser eller er forsinket med utviklings- og testaktiviteter, vil ikke i seg selv være tilstrekkelig til at det kan benyttes helseopplysninger. Men det kan i enkelte tilfeller oppstå situasjoner hvor det er umiddelbar fare for pasientsikkerheten, og hvor det ikke er tid til å fremskaffe personalressurser og kompetanse til å foreta nødvendig utvikling eller testing med fiktive data. Men dersom mangelen på ressurser og kompetanse er gjentagende, må det i stedet vurderes tiltak som kan avhjelpe ressurs- og kompetansemangelen.

Rene økonomiske hensyn vil ikke kunne tillegges vekt ved vurderingen. Det vil for eksempel ikke kunne legges vekt på at det vil ha en lavere kostnad å benytte helseopplysninger sammenlignet med andre typer opplysninger.

2.4.4 Ekstraordinære hendelser

Det kan fra tid til annen oppstå ekstraordinære hendelser som utløser behov for feilretting eller nyutvikling av funksjonalitet, for å avverge umiddelbar fare for liv og helse. Dette kan for eksempel være utbedring av kritiske feil i et system som er i bruk, eller akutte behov for ny funksjonalitet i en pandemisituasjon.

Dersom virksomheten vurderer at fremskaffing av fiktive eller anonyme opplysninger vil ta så lang tid at det vil oppstå fare for pasientsikkerheten, kan dette være et argument for at det kan benyttes helseopplysninger til utviklingen. Dette kan for eksempel være situasjoner der det i tilknytning til en løsning i drift, oppstår en uventet feil som vil føre til at systemet blir utilgjengelig eller at viktig funksjonalitet ikke virker som forutsatt, og hvor tid er en av faktorene som påvirker pasientsikkerheten.

3 Tiltak for å lukke et utviklings- og testmiljø

For at helseopplysninger skal kunne benyttes til utvikling og testing, er det et vilkår i pasientjournalloven § 11 annet ledd at dette skjer i «lukkede testmiljøer». I forarbeidene presiseres det at det er en forutsetning at et utviklings- eller testarbeid skjer i samsvar med kravene i pasientjournalloven §§ 15, 16 og 22 om henholdsvis taushetsplikt, forbud mot urettmessig tilegnelse av helseopplysninger og informasjonssikkerhet. Det gjelder altså de samme kravene til taushetsplikt og informasjonssikkerhet i utviklings- og testmiljøer som i et produksjonsmiljø.

Virksomheten skal vurdere om informasjonssikkerhets- og personvernrisikoen forbundet med utviklings- og testaktivitetene kan aksepteres, og om det er tiltak som bør iverksettes før aktiviteten starter. Virksomheten skal utføre en risikovurdering, og ved behov også en personvernkonsekvensvurdering (DPIA), før det vurderes uttrekk av helseopplysninger fra produksjonsmiljøet. Risikovurderinger og personvernkonsekvensvurderinger skal oppdateres løpende, og minimum når endringer blir vurdert eller besluttet.

Hvilke tiltak som vil være påkrevd for å lukke et utviklings- og testmiljø må vurderes konkret. Tiltakene vil blant annet være avhengig av hvilke informasjonsverdier som skal sikres, formålet med utviklingen og testingen, samt virksomhetens risikoakseptansenivå.

I dette kapittelet beskrives risikoreduserende tiltak som bør vurderes der det identifiseres risiko som tilsier at tiltak er nødvendige.

Virksomheten må for hver enkelt utviklings- og testaktivitet identifisere risikoscenarier som kan inntreffe for den konkrete utviklingen og testingen. Følgende to risikoscenarier vil regelmessig være relevante ved bruk av helseopplysninger i lukkede testmiljøer:

- Omstilling av testregimet i en virksomhet fra behandling av fiktive data til helseopplysninger vil være komplekst og omfattende. Som følge av kompleksiteten, vil det være en risiko for at ikke alle nødvendige sikkerhetstiltak identifiseres.
- Økt risiko knyttet til testregimet når helseopplysninger inngår, eksempelvis manglende sletting eller integritetsbrudd ved svikt i kontrollen med dataflyt.

Nedenfor beskrives ulike organisatoriske og tekniske sikkerhetstiltak som vil kunne adressere disse risikoelementene.

I Normen er det inntatt krav til risikovurderinger og risikohåndtering i kapittel 3.4, mens det i kapittel 3.5 er krav til gjennomføring av DPIA. Direktoratet for e-helse har videre utarbeidet en mal og veiledning for utfylling av en DPIA.

3.1 Separate utviklings- og testmiljøer

Det skal etableres separate miljøer for utvikling og testing av behandlingsrettede helseregistre, adskilt fra produksjonsmiljøene. Det er viktig at eventuelle feil som oppstår i utviklings- og testmiljøene ikke påvirker produksjonsmiljøer som benyttes ved ytelse av helsehjelp. Testmiljøer og testsystem bør merkes tydelig for å unngå at de blir benyttet til

pasientbehandling eller at det skjer testing i produksjonsmiljøet. Det å etablere separate utviklings- og testmiljøer vil understøtte pasientsikkerheten, og forebygger blant annet at uvedkommende får urettmessig tilgang til personopplysninger og at pasientjournaler inneholder feil data, ved at testdata har blitt benyttet i produksjonsmiljøet.

Et testmiljø kan etableres som et permanent miljø eller ha en tidsavgrenset varighet. Helseopplysninger som benyttes i testmiljøet må imidlertid alltid slettes umiddelbart når formålet med behandlingen er oppnådd, se punkt 3.8.

Mer veiledning knyttet til testing og testdata kan blant annet finnes i Normens faktaark 43 Testing og testdata.

3.2 Kompetanse og taushetsplikt

Virksomheten må sørge for at utviklings- og testaktivitetene ledes og gjennomføres av personell med tilstrekkelig kompetanse. Helsevirksomheten som er dataansvarlig for utviklingen eller testingen, bør utpeke en ressurs som har det operative ansvaret for ivaretakelse av informasjonssikkerhet og personvern under hele utviklings- og testfasen.

Alle involverte ressurser, herunder også eksterne ressurser, som vil håndtere helseopplysninger fra behandlingsrettede helseregistre, vil være underlagt lovbestemt taushetsplikt og forbud mot urettmessig tilegnelse av helseopplysninger, i henhold til pasientjournalloven §§ 15 og 16, jf. helsepersonelloven §§ 21 flg. Virksomheten skal ivareta taushetsplikten på en egnet måte. Personer som er involvert i databehandlingen må orienteres om taushetsplikten. Det kan for eksempel benyttes taushetserklæringer som signeres av den enkelte medarbeider.

3.3 Dataflyt

Virksomheten bør utarbeide detaljerte oversikter over hvor helseopplysninger transporteres og lagres i forbindelse med utviklingen eller testingen. Dette kan for eksempel gjøres i et dataflytskjema. Oversikt og kontroll over dataflyten vil være et utgangspunkt for vurdering av tiltak for å hindre at data som benyttes til testing kommer over i produksjonssystemer, overføres utilsiktet til andre miljøer internt i virksomheten eller eksponeres eksternt ut mot internett.

Bruk av et dataflytskjemaer vil også kunne benyttes ved utarbeidelse av planer for å sikre systemene mot inntrengere og andre uønskede hendelser. For å sikre dataflyten og utviklings- og testmiljøet, bør det blant annet vurderes om tilgang til internett eller andre nettverk bør monitoreres, og om inntrengningstesting (penetrasjonstesting) kan være et hensiktsmessig sikkerhetstiltak. Hvis en leverandør eller andre eksterne parter har tilgang til utviklings- og testmiljøet, bør dette inngå i dataflytskjemaet.

Oversikter over dataflyt bør revideres jevnlig, og brukes aktivt ved oppdatering av risikovurderinger og justering av testplaner.

Dersom konfigurasjoner eller innstillinger kopieres fra et produksjonssystem til et testsystem, vil det være viktig at konfigurasjonene endres, slik at data ment for testing ikke sendes til produksjonssystemet.

I forbindelse med utvikling og testing kan det være behov for lagring av data på lagringsmedier som minnepinner og eksterne harddisker, eller på lagringsområder i virksomheten som normalt ikke er beregnet for lagring av helseopplysninger. Dersom eksterne lagringsmedier benyttes, må disse sikres på forsvarlig måte. Alle lagringsmedier skal slettes forsvarlig når de tas ut av bruk, se kapittel 3.8.

Det kan også være behov for å benytte perifert utstyr i forbindelse med utvikling eller testing (medisinsk utstyr, mobiltelefoner mv.). Det er viktig at dette kommer frem av dataflytskjemaet

og i risikovurderingen, samt at informasjon på disse enhetene blir slettet etter at prosessen er avsluttet, se kapittel 3.8.

3.4 Testplan

Virksomheten bør etablere en utviklings- og testplan som kan inneholde en beskrivelse av aktivitetenes formål, omfang, fremgangsmåte, ressurser og fremdriftsplan. I planen bør utviklings- og testobjektene defineres, og man bør beskrive hvilke egenskaper som skal testes, hvilke oppgaver som skal utføres og hvem som er ansvarlig for å utføre de forskjellige oppgavene. Testplanen bør inngå som et av underlagene til risikovurderinger.

Virksomheten bør inkludere sine utviklings- og testaktiviteter i eksisterende rammeverk for endringsledelse (change management). I noen tilfeller kan testaktiviteter påvirke andre systemer som er i produksjon. For å redusere faren for feil eller nedetid på systemer som benyttes i virksomheten, bør testplanen følge virksomhetens rammeverk for endringsledelse.

3.5 Vurdere datagrunnlaget

Før helseopplysningene (datagrunnlaget) kopieres ut fra virksomhetens behandlingsrettede helseregister til det konkrete testformålet, skal datafelter og datamengde defineres på bakgrunn av formålet som skal oppnås. Opplysninger om diagnose eller sykdom kan bare behandles når det er nødvendig for å nå formålet, jf. pasientjournalloven § 11 fjerde ledd.

Virksomheten må vurdere hvorvidt data som skal benyttes til utviklings- og testformål inneholder kategorier av opplysninger som har et særlig vern. Dette kan omfatte opplysninger om personer med fortrolig eller strengt fortrolig adresse (kode 6 og 7) eller opplysninger som eksempelvis er sperret for innsyn fra pasienten.

Dersom det er strengt nødvendig at opplysninger om personer med adressesperre inngår i datagrunnlaget, må virksomheten etablere strenge rutiner for blant annet hvem som skal ha tilgang til opplysningene, hvor lenge tilgangen skal vare og hvor lenge opplysningene skal behandles i utviklings- og testmiljøet. I Normens faktaark 55 om Sperret adresse i Folkeregisteret er det inntatt veiledning til virksomheter som behandler opplysninger som nevnt. Der det ikke er mulig å ivareta et tilstrekkelig vern for personer som er registrert med fortrolig adresse, må hensynet til liv og helse veie tyngre enn hensynet til komplette data for utvikling og testing.

Dersom datagrunnlaget kan omfatte opplysninger der det er vurdert at pasienten selv ikke har rett til innsyn, bør det vurderes om bruk av dataene til utvikling eller testing vil kunne gi risiko for innsyn via innsyn i testdataene, se kapittel 2.4.2. Taushetsplikten vil også gjelde overfor pasienten der unntak fra innsynsretten er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller der innsyn er klart utilrådelig av hensyn til personer som står vedkommende nær, jf. pasient- og brukerrettighetsloven § 5-1 annet ledd. Dersom lovkrav ikke kan oppfylles eller risikoen for sikkerhetsbrudd er for høy, må slike opplysninger ekskluderes fra uttrekket. I tillegg skal prinsippet om dataminimering følges når helseopplysninger benyttes til utvikling og testing, se kapittel 4.5.

3.6 Tilgangsstyring og kontrollrutiner

Det er en forutsetning at et utviklings- eller testarbeid skjer i samsvar med kravene i pasientjournalloven §§ 15, 16 og 22 om henholdsvis taushetsplikt, forbud mot urettmessig tilegnelse av helseopplysninger og informasjonssikkerhet.

Virksomheten skal ha rutiner for autentisering og autorisering, herunder også for korrekt endring og rettidig avslutning av tilganger til det lukkede utviklings- eller testmiljøet.

Det er særlig viktig at virksomheten implementerer grundige kontrollrutiner for tilgangsstyring i forbindelse med testaktiviteter, da testressursenes behov for tilgang til helseopplysninger vil kunne endre seg under aktivitetens fremdrift.

Eksempler på sikkerhetstiltak knyttet til tilgangsstyring:

- Virksomheten fører oversikt over testpersonell som har tilgang til testmiljøet (testbrukere) og hvilke rettigheter de har
- Virksomheten sørger for at testbrukere er underlagt taushetsplikt gjennom ansettelsesavtale eller ved særskilt skjema som signeres før oppstart av testingen

For å sikre at det skilles mellom tilganger til testmiljøer og vanlige brukertilganger, er det viktig at det opprettes egne brukerkontoer for testing (testkontoer) der dette er mulig. Dette er også viktig for å ivareta krav til logging, se kapittel 3.7 nedenfor.

Utviklings- og testmiljøer bør inkluderes i virksomhetens sårbarhetskartlegginger og sikkerhetsovervåking. Sikkerhetsrelevante data fra utviklings- og testmiljøer, for eksempel sikkerhetslogger og driftslogger, bør håndteres i sentral loggdatabase på samme måte som for produksjonsmiljøet.

3.7 Logging

Virksomheten skal loggføre tilganger og aktiviteter i det lukkede testmiljøet. Formålet med loggingen er at virksomheten skal kunne avdekke uautorisert bruk eller forsøk på uautorisert tilgang, og slik forebygge, avdekke og forhindre sikkerhetsbrudd. Formålet med loggingen er også at virksomheten skal kunne fremvise en oversikt over bruken av testdataene, og dermed legge til rette for innsyn fra de registrerte.

Loggopplysningene skal oppbevares til de ikke lenger er nødvendige for det formålet de er ment for. De skal deretter slettes, se kapittel 3.8.

I vurderingen av om formålet er oppnådd, må virksomheten ta hensyn til behovet for å kunne kontrollere tilganger i ettertid. Selv om testen eller utviklingsprosessen er gjennomført, kan det oppstå behov for å kontrollere at tilganger har vært benyttet i henhold til tjenstlig behov i en periode etter avslutning av prosessen. For logger over tilganger i et behandlingsrettet helseregister vil det gjennomgående være behov for lang lagringstid.

Det er tilsvarende krav til logging i utviklings- og testmiljøer som i produksjonsmiljøet. Det innebærer at følgende minimum skal logges:

- Identiteten til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger
- Organisatorisk tilhørighet
- Det tjenstlige behovet for tilgjengeliggjøringen
- Tidsperioden for tilgjengeliggjøringen

Den registrerte har rett til innsyn i dokumentasjonen i samme utstrekning som for loggen i det behandlingsrettede helseregisteret.

3.8 Sletting

Helseopplysninger som er brukt til utvikling eller testing, skal slettes når formålet med aktivitetene er oppfylt. Eventuelle utskrifter og kopier av utviklings- og testdataene skal makuleres eller slettes etter bruk.

Slettingen skal gjøres på en forsvarlig måte. Det skal brukes en metode som gjør at det ikke er mulig å rekonstruere opplysningene. Det er ikke tilstrekkelig å begrense tilgangen til

opplysningene ved hjelp av tilgangsstyring. For å oppfylle sletteplikten, må virksomheten slette alle kopier av opplysningene, i utgangspunktet også filer og data i sikkerhetskopier.

Dersom virksomheten har benyttet seg av en databehandler for å gjennomføre testing, skal virksomheten innhente skriftlig bekreftelse fra databehandleren på at alle helseopplysninger er slettet etter at testingen er gjennomført og formålet er oppnådd. Dette skal reguleres i en databehandleravtale, se kapittel 4.2.

I Normens faktaark 25 om lagringstid og sletting er det i kapittel 6 inntatt beskrivelser av forhold som en dataansvarlig helsevirksomhet bør vurdere for å ivareta sikker sletting av data.

4 Øvrige forhold virksomheten må vurdere

4.1 Rettslig grunnlag for behandling av helseopplysninger til utvikling og testformål

Behandling av helseopplysninger i forbindelse med utvikling og testing vil ha hjemmel i personvernforordningen artikkel 6 nr. 1 bokstav e og artikkel 9 nr. 2 bokstav h. Det supplerende rettslige grunnlaget, er i denne forbindelse pasientjournalloven § 11 annet ledd. Det er imidlertid en forutsetning for å behandle helseopplysninger etter denne bestemmelsen at virksomheten allerede har rettslig grunnlag for å behandle helseopplysningene i et behandlingsrettet helseregister. Helse- og personopplysningene som benyttes til utvikling og testing må altså være (kopi av) helseopplysninger som den dataansvarlige allerede har et lovlig behandlingsgrunnlag for.

Pasientjournalloven § 11 annet ledd vil ikke gi selvstendig rettslig grunnlag til å benytte helseopplysninger i andre tilfeller, eksempelvis der en leverandør av et behandlingsrettet helseregister på eget initiativ ønsker å utvikle et system. Datagrunnlaget kan gjenbrukes til nye formål dersom det nye formålet er forenlig med det opprinnelige formålet helseopplysningene ble innhentet til, og det foreligger et rettslig grunnlag for den nye behandlingen av helseopplysningene (formålsbegrensning).

4.2 Databehandleravtale

Leverandører som bistår i utvikling og testing der det blir besluttet å benytte person- og helseopplysninger, vil være å anse som databehandlere hvor de behandler helseopplysninger på vegne av den dataansvarlige.

En databehandler kan ikke behandle helseopplysninger på annen måte enn det den dataansvarlige har bestemt. For å regulere ansvar, rettigheter og plikter mellom den dataansvarlige og databehandleren, skal det inngås en databehandleravtale, jf. personvernforordningen art. 28 nr. 3.

Det vil ikke være nødvendig å inngå en separat databehandleravtale dersom testingen skal utføres av en leverandør helsevirksomheten allerede har en databehandleravtale med, og hvor den planlagte aktiviteten er dekket av avtalen. Dersom foreliggende databehandleravtale ikke er dekkende, må den suppleres, slik at den omfatter de aktivitetene som inngår i utviklingen eller testingen. Alternativt kan det inngås en ny databehandleravtale for utviklingen og testingen.

4.3 Oppdatering av behandlingsprotokollen

Den dataansvarlige virksomheten skal ha oversikt over all behandling av helse- og personopplysninger. Virksomheten skal føre protokoll over databehandlingen, jf. personvernforordningen art. 30. Dette omfatter også behandling av data i forbindelse med utviklings- og testaktiviteter, for eksempel overføring av helseopplysninger fra produksjonsmiljøet til utviklings- og testmiljøet, og behandlingen som gjennomføres i forbindelse med utviklingen eller testingen.

Protokollen skal minimum inneholde informasjonen som nevnt i personvernforordningen art. 30, og skal til enhver tid være oppdatert. Både den dataansvarlige og en eventuell databehandler som opptrer på dennes vegne skal føre protokoll over behandlingsaktivitetene.

4.4 Innebygd personvern

Innebygd personvern er et sentralt krav i personopplysningsloven, og innebærer at det skal tas hensyn til personvern i alle faser av utviklingen av et system eller en løsning. Kravet innebærer at alle personvernprinsippene og den registrertes rettigheter og friheter skal ivaretas på en god måte i behandlingen av personopplysninger.

Før det gjennomføres utvikling eller testing av et behandlingsrettet helseregister, må virksomheten planlegge hvordan personvern kan bygges inn, slik at personvernprinsippene og de registrertes rettigheter og friheter blir ivaretatt i løsningen.

Det er utarbeidet en rekke veiledere til dette kravet, eksempelvis veilederen fra Personvernrådet (European Data Protection Board, EDPB) og Datatilsynets veileder om innebygd personvern.

4.5 Dataminimering

Bruk av helseopplysninger skal begrenses til et minimum. Dataminimeringsprinsippet må overholdes også ved utviklings- og testaktiviteter.

Dersom den dataansvarlige virksomheten konkluderer med at det er nødvendig å bruke helseopplysninger for å oppnå formålet med utviklings- eller testaktivitetene, må det foretas en konkret vurdering av hvilken type og hvilket omfang av opplysninger som vil være nødvendige for å oppnå formålet.

Mengden og typen data vil være avhengig av hva man skal testes (formålet). Skal virksomheten for eksempel foreta en komplett test av all funksjonalitet i et system eller foreta prøvedrift, vil det være behov for en tilstrekkelig mengde data til å sikre at testen gjenspeiler en reell driftssituasjon. Ved testing av avgrenset funksjonalitet, kan et mindre utvalg data være tilstrekkelig.

5 Sentrale begreper

Ved utarbeidelsen av dokumentet er det blant annet tatt utgangspunkt i begrepsbeskrivelsene som følger av Normen kapittel 6.2. Nedenfor følger en oversikt over hvordan et utvalg sentrale begreper i retningslinjen er ment å forstås.

5.1 Anonyme opplysninger

Dokumentet legger til grunn den samme begrepsforståelsen som følger av personvernforordningens fortalepunkt 26, hvor det står at anonyme opplysninger er opplysninger som

> *«[…] ikke kan knyttes til en identifisert eller identifiserbar fysisk person, eller personopplysninger som er blitt anonymisert på en slik måte at den registrerte ikke lenger kan identifiseres».*

For å generere et anonymt datauttrekk fra behandlingsrettede helseregistrene til utvikling og testing, må alle personentydige kjennetegn, som navn, fødselsnummer og øvrige kjennetegn, fjernes på en slik måte at opplysningene ikke lenger kan identifisere fysiske personer. Videre må virksomheten sikre at alle muligheter for re-identifisering av dataene er fjernet. Når uttrekket er anonymisert, anses ikke lenger opplysningene å utgjøre personopplysninger.

Anonymisering er en metode for å redusere risikoen knyttet til behandling av helseopplysninger. Det er samtidig viktig å være oppmerksom på at prosessen med anonymisering i seg selv er en databehandling, som forutsetter at vilkårene for behandling av helseopplysninger er oppfylt.

Anonymisering kan være vanskelig å gjennomføre i praksis. Datatilsynet har utarbeidet en veileder om anonymisering av personopplysninger.

5.2 Behandlingsrettet helseregister

I pasientjournalloven § 2 bokstav d er et behandlingsrettet helseregister definert som et pasientjournal- og informasjonssystem eller annet register, fortegnelse eller lignende, der helseopplysninger er lagret systematisk, slik at opplysninger om den enkelte kan finnes igjen, og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner.

Behandlingsrettet helseregister er et vidt begrep og omfatter hovedjournal, pasientkort, individuell plan, ulike fagsystemer, pasientadministrative systemer, Nasjonal kjernejournal mv. Helseopplysninger kan være registrert i alle disse systemene. Opplysningene i et behandlingsrettet helseregister kan således være nedtegnet og lagret adskilt i ett eller flere systemer. Det enkelte system kan være virksomhetsinternt eller det kan være systemer som to eller flere virksomheter samarbeider om (virksomhetsovergripende systemer). Se Prop. 72 L (2013–2014) for en mer utfyllende omtale av begrepene.

5.3 Direkte identifiserende helseopplysninger

Pasientjournalloven § 11 annet ledd benytter begrepet ”direkte identifiserbare helseopplysninger”. Der det i dette dokumentet står «helseopplysninger», menes det helseopplysninger som er direkte identifiserbare. Uttrykket omfatter også pasientrelaterte opplysninger som ikke strengt tatt er helseopplysninger, men som er taushetsbelagt etter helsepersonelloven § 21 og som benyttes i forbindelse med utvikling eller testing.

At opplysninger er ”direkte identifiserbare” betyr i denne sammenhengen at de identifiserer fysiske personer uten noen form for pseudonymisering eller andre tiltak ment for å redusere

risikoen for personvernkrenkelser. I situasjoner hvor dataansvarlige virksomheter benytter direkte identifiserbare opplysninger til utvikling og testing etter pasientjournalloven § 11 annet ledd, er det derfor viktig å redusere risikoen for personvernkrenkelser ved å lukke testmiljøet, se kapittel 3.

5.4 Fiktive opplysninger / syntetiske opplysninger

Fiktive opplysninger omtales i andre sammenhenger også som «syntetiske» opplysninger. Fiktive opplysninger er opplysninger som er laget for testformål, og som, i motsetning til anonymiserte opplysninger, ikke er basert på reelle personopplysninger. Behandling av fiktive opplysninger krever derfor ikke behandlingsgrunnlag etter personvernforordningen, og er ikke regulert i særlovgivningen for helse- og omsorgssektoren.

Ved bruk av fiktive opplysninger, kommer ikke personvernforordningen til anvendelse, da det ikke behandles personopplysninger.

5.5 Helseopplysninger

Det følger av personvernforordningen art. 4, nr. 15 at helseopplysninger er

> *«[…] personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder om ytelse av helsetjenester, som gir informasjon om vedkommendes helsetilstand.»*

I behandlingsrettede helseregistre vil det være omfattende mengder helseopplysninger. Slike opplysninger er sensitive informasjonsverdier, og er underlagt særlige krav til beskyttelse etter pasientjournalloven §§ 22 og 23. I tilfeller hvor slike opplysninger skal benyttes ved utvikling og testing i henhold til pasientjournalloven § 11 annet ledd, må det stilles strenge krav til behandlingen av dataene, se kapittel 4.

Helseopplysninger regnes som en særlig kategori av personopplysninger. Det kreves hjemmel i et av unntakene i personvernforordningen art. 9 for å behandle slike opplysninger.

5.6 Lukket utviklings- og testmiljø

Begrepet benyttes her om utviklings- eller testmiljøer der det er implementert nødvendige mekanismer og tiltak for å hindre at uvedkommende kan få tilgang til helseopplysningene, samtidig som virksomheten ivaretar kontroll på dataflyten både inn og ut av testmiljøet for å hindre integritetsbrudd.

Hvilke mekanismer og tiltak som er påkrevd for å lukke utviklings- og testmiljøer, må vurderes konkret, og vil være avhengig av hvilke informasjonsverdier som skal sikres, formålet med utviklingen eller testen, samt virksomhetens risikoakseptansenivå.

5.7 Personopplysninger

Det følger av personvernforordningen art. 4, nr. 1 at *personopplysninger* er

> *«[…] 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.»*

Fra behandlingsrettede helseregistre vi det også kunne trekkes ut ordinære personopplysninger, som vil kunne benyttes i forbindelse med utvikling og testing i henhold til pasientjournalloven § 11 annet ledd.

5.8 Pseudonyme opplysninger

Det følger av personvernforordningen art. 4, nr. 5 at *pseudonymisering* er

> «[…] *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*.»

Bruk av pseudonyme personopplysninger vil i mindre grad utfordre personvernet enn bruk av direkte identifiserbare helseopplysninger.

5.9 Produksjonsmiljø

Et produksjonsmiljø består av maskinvare, programvare og informasjon som til sammen leverer et sett funksjonalitet og tjenester til sluttbrukerne. Sluttbrukerne det blir referert til her vil normalt være helsepersonell. Når et elektronisk behandlingsrettet helseregister kjører i et produksjonsmiljø, betyr det at det skal brukes til klinisk behandling. Dette blir noen steder i dokumentet omtalt som en «driftssituasjon».

Produksjonsmiljøet skal ha tekniske og organisatoriske beskyttelsesmekanismer for å ivareta de informasjonsverdiene som inngår i produksjonsmiljøet, for eksempel helse- og personopplysninger. Et elektronisk behandlingsrettet helseregister vil enten kjøre i helsevirksomhetens eget produksjonsmiljø eller eventuelt en leverandørs produksjonsmiljø.

5.10 Rettslig grunnlag

All behandling av personopplysninger må ha et rettslig grunnlag for å være lovlig. Det finnes flere ulike typer rettslige grunnlag. Disse fremgår av personvernforordningen artikkel 6. Dersom man skal behandle særlige kategorier personopplysninger, for eksempel helseopplysninger, må behandlingen også falle inn under et av unntakene i artikkel 9.

Behandling av helseopplysninger til test og utvikling vil ha hjemmel i personvernforordningen artikkel 6 nr. 1 bokstav e og artikkel 9 nr. 2 bokstav h.

I tillegg til å ha rettslig grunnlag etter personvernforordningen, må virksomheten også ha et grunnlag i norsk lov for å kunne bruke helseopplysninger til utvikling og testing. Det supplerende rettslige grunnlaget følger her av pasientjournalloven § 11 annet ledd.

Det er imidlertid en forutsetning for å behandle helseopplysninger etter denne bestemmelsen, at virksomheten allerede har rettslig grunnlag for å behandle helseopplysningene i et behandlingsrettet helseregister. Helseopplysningene som benyttes til utvikling og testing må altså være (kopi av) helseopplysninger som den dataansvarlige allerede har et lovlig behandlingsgrunnlag for.

5.11 Utvikling og testing

Med utvikling, menes det her å lage eller oppgradere et IKT-system slik at det er klart for testing. Underveis i utviklingsprosessen vil det ofte være behov for testing, som del av utviklingsprosessen. I de tilfellene det oppdages feil under testingen, vil det måtte foretas ny utvikling for å rette opp feilene.

Testing gjennomføres for å kontrollere at IKT-systemer og endringer i disse fungerer slik de skal, og at man har kontroll blant annet på integrasjoner mot andre systemer, visning av data og ytelsen.

5.12 Utviklings- og testmiljø

Begrepet benyttes om utviklings- eller testmiljøer der det er implementert nødvendige mekanismer og tiltak for å hindre at uvedkommende kan få tilgang til helseopplysninger i miljøene, samtidig som virksomheten ivaretar kontroll på dataflyten både inn og ut av testmiljøet for å hindre integritetsbrudd.

Hvilke mekanismer og tiltak som er påkrevd for å lukke utviklings- og testmiljøer, må vurderes konkret av virksomheten, og vil være avhengig av hvilke informasjonsverdier som skal sikres, formålet med utviklingen eller testingen, samt virksomhetens risikoakseptansenivå.