Direktoratet for e-helse

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

HITR 1252 *høringsutkast* 2023

**Tittel:**
Bruk av direkte identifiserbare helseopplysninger til utvikling og testing av behandlingsrettede helseregistre

**Rapportnummer:**
HITR 1252 *høringsutkast* 2023

**Utgitt:**

**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».*

Bestemmelsen er omtalt i lovforslagets kapittel 7 i Prop. 91 L (2021-2022) Endringer i pasientjournalloven mv. (nasjonal digital samhandling), hvor det blant annet 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 følger blant annet at begrepet «prøvedrift i denne sammenhengen vil være omfattet av begrepet ”test”.»

Lovteksten bruker uttrykket «direkte identifiserende helseopplysninger». Der denne retningslinjen bruker uttrykket «helseopplysninger», menes helseopplysninger som er direkte identifiserbare. Direktoratet har videre lagt til grunn at dette omfatter både helseopplysninger og andre pasientrelaterte opplysninger som er taushetsbelagt etter helsepersonelloven § 21, som benyttes i forbindelse med utvikling og testing av behandlingsrettede helseregistre.

«Behandlingsrettet helseregister» er et vidt begrep, og omfatter hovedjournal, kjernejournal, pasientkort, individuell plan, ulike fagsystemer, pasientadministrative systemer mv. Helseopplysninger kan være registrert i alle disse systemene. Begrepet er forklart nærmere i kapittel 5.1.

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 vurderingstemaene 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 å ivareta taushetsplikt. En ikke-uttømmende oversikt følger i kapittel 4.

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

## 1.2 Om retningslinjen

Retningslinjen beskriver lovens vilkår for å benytte direkte identifiserbare helseopplysninger til test- og utviklingsformål, og redegjør for hvilke vurderinger den dataansvarlige virksomheten må gjøre før helseopplysninger eventuelt benyttes.

Retningslinjen beskriver videre hvilke sikkerhetstiltak som bør iverksettes i forbindelse med bruk av helseopplysninger til utviklings- og testformål. Dette omfatter:

- Testplan
- Dataflyt
- Risikovurderinger og DPIA
- Tilgangsstyring
- Logging
- Sletting

En beskrivelse av hvordan sentrale begreper benyttes i dette dokumentet, følger av kapittel 0.

## 1.3 Målgruppe

Retningslinjen er relevant for virksomheter i helse- og omsorgssektoren som har etablert et behandlingsrettet helseregister (pasientjournalsystem), og som skal planlegge, beslutte eller gjennomføre utvikling eller testing av virksomhetens behandlingsrettede helseregistre ved bruk av helseopplysninger.

Retningslinjen retter seg mot alle personer som blir involvert i prosessen, både ledere, ansatte og innleid personell. Retningslinjen er særlig relevant for personell innen fagområdene informasjonssikkerhet, personvern, IT og medisinsk teknologi.

Dersom helsevirksomheten beslutter å engasjere en leverandør til å utføre utviklingen eller testingen, vil retningslinjen gjelde tilsvarende for denne leverandøren. Helsevirksomheten må i slike tilfeller instruere leverandøren om å følge retningslinjen. Se også kapittel 4.2 om databehandleravtaler.

# 2. Vilkår for å bruke helseopplysninger til utviklings- og testformål

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

- 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. Dette vilkåret innebærer at det må vurderes konkret om formålet kan oppnås med fiktive, anonyme eller pseudonyme data.

Hovedregelen etter pasientjournalloven § 11 annet ledd, er at utvikling og testing med bruk av direkte identifiserbare helseopplysninger bare kan gjennomføres dersom formålet med testen eller utviklingen ikke kan oppnås med pseudonyme, anonyme eller fiktive opplysninger. Dette innebærer at helsevirksomheten alltid først skal vurdere om bruk av *fiktive/syntetiske, anonymiserte eller pseudonyme helseopplysninger* (ikke-identifiserbare opplysninger) er tilstrekkelig til å oppnå formålet.

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 med fiktive/syntetiske data, deretter anonyme data og deretter pseudonyme data. Virksomheten kan bare benytte helseopplysninger dersom det vil være umulig eller uforholdsmessig vanskelig å oppnå formålet ved å benytte fiktive, anonymiserte eller pseudonyme helse- og personopplysninger. Unntaksadgangen skal altså forstås som et begrenset og restriktivt unntak fra hovedregelen om å benytte ikke-identifiserbare opplysninger.

Behovet for å benytte reelle journalopplysninger aktualiseres særlig i prosjektenes sluttfase, nært opptil produksjonssetting. Utviklings- og testmiljøet må være robust og hindre at uvedkommende får tilgang til taushetsbelagt informasjon.

## 2.1 Vilkårene for å bruke direkte identifiserende helselysninger til utvikling og testing

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 og testingen som medfører at vilkåret er oppfylt, og som gjør det nødvendig å bruke helseopplysninger for å oppfylle formålet (personvernforordningen art. 6, nr. 1, bokstav e og artikkel 9 nr. 2 bokstav h).

Nedenfor omtales hvilke vurderinger den dataansvarlige virksomheten må gjennomføre for å komme frem til om unntaksadgangen kan benyttes.

All den tid pseudonyme personopplysninger «*indirekte kan identifiseres*», jfr. personvern-forordningen art. 4, nr. 1, jfr. nr. 5, må bruk av slike opplysninger i utvikling og testing etter

pasientjournalloven § 11 annet ledd underlegges de samme vurderinger og krav som ved utvikling og testing på direkte identifiserbare helseopplysninger.

### 2.1.1 Vilkår 1: Umulig

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 helse- og personopplysninger. Eksempelvis vil fiktive opplysninger (syntetiske data) ikke alltid ha de egenskapene som er nødvendig for å kvalitetssikre systemer før produksjonssetting i helsetjenesten.

Vurderingen av om det vil være umulig å oppnå formålet uten bruk av helseopplysninger skal dokumenteres, for eksempel i virksomhetens protokoll, se kapittel 4.3.

### 2.1.2 Vilkår 2: Uforholdsmessig vanskelig

Det vil i de langt fleste tilfeller være praktisk mulig å oppnå formålet med utviklingen eller testingen ved å benytte fiktive, anonyme eller pseudonyme opplysninger. En konkret vurdering kan imidlertid tilsi at det vil være uforholdsmessig vanskelig å benytte slike opplysninger fremfor helseopplysninger. Den konkrete vurderingen skal i så fall dokumenteres, jf. forskrift om ledelse og kvalitetsforbedring i helse- og omsorgstjenesten § 5 annet ledd.

Vilkåret vil bare være oppfylt dersom bruken av fiktive, anonyme eller pseudonyme data vil være «uforholdsmessig». Bruken av direkte identifiserbare helseopplysninger må altså vurderes opp mot andre relevante momenter, eksempelvis hva som kan oppnås ved å benytte helseopplysninger og hvor omfattende inngrep i personvernet dette vil medføre. Utfordringene ved å benytte ikke-identifiserbare opplysninger må, etter en konkret vurdering, være uproporsjonalt store sammenlignet med formålet som søkes oppnådd med testingen eller utviklingen. Vilkåret vil eksempelvis altså lettere være oppfylt der det skal utvikles funksjonalitet som er særlig viktig for pasientbehandlingen, behovet for helseopplysninger er begrenset og risikoen er lav.

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

#### Pasientsikkerhet

Det vil alltid være et grunnleggende krav at pasientsikkerheten ivaretas, og dette vil derfor alltid være et særlig viktig moment i vurderingen. Et viktig moment vil derfor være i hvilken grad pasientsikkerheten kan bli påvirket av valget av utviklings- og testdatasett. Ved bruk av ikke-identifiserbare data, kan pasientsikkerheten eksempelvis bli utfordret ved at testen ikke gir gode nok resultater, og at systemet derfor ikke virker som forutsatt i prøvedrift eller i produksjon.

Pasientsikkerheten vil imidlertid også kunne bli utfordret ved bruk av helse- og personopplysninger, eksempelvis ved at produksjonsdata blir overskrevet av data fra testmiljøet.

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

## Oppfyllelse av pasientrettigheter

Virksomheten må vurdere om pasientens rettigheter etter henholdsvis personvernforordningen og helselovgivningen kan oppfylles i forbindelse med utviklingen eller testingen med bruk av helseopplysninger. 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 eller andre pasientrettigheter, eksempelvis ved ikke å kunne gi innsyn i databehandlingen som følge av manglende loggkapabilitet i testmiljøet, kan dette være et moment som tilsier at utviklings- eller testaktiviteten ikke bør gjennomføres med helse- og personopplysninger.

## Tid- og ressursbruk

Det fremgår av forarbeidene at det, ved vurderingen av om det vil være uforholdsmessig vanskelig å oppnå formålet med bruk av anonyme eller fiktive opplysninger, blant annet kan legges vekt på om det «er svært tid- og ressurskrevende for aktøren å lage anonyme eller fiktive opplysninger.»

At virksomheten har begrenset tilgang på ressurser eller er forsinket med utviklings- og testaktiviteter, vil ikke være tilstrekkelig til at helseopplysninger kan benyttes til utvikling og testing. Tidsbruken eller ressursbruken må også være uproporsjonalt høy sammenlignet med formålet som søkes oppnådd med testingen eller utviklingen.

Et eksempel der tidsbruken bør veie tungt i vurderingen, kan være en situasjon der det har oppstått en uventet feil og lav fremdrift i utviklings- og testarbeidet vil føre til at systemer som skal understøtter helsehjelpen blir utilgjengelige eller at sentral funksjonalitet ikke virker som forutsatt. Dersom virksomheten vurderer det slik at utvikling og testing med fiktive eller anonyme opplysninger vil ta så lang tid at det oppstår fare for pasientsikkerheten, sammenholdt med utvikling og testing med helseopplysninger, kan dette være et moment som taler for at det kan benyttes helseopplysninger til utviklingen.

# 3. Tiltak for å lukke et utviklings- og testmiljø

Dersom helseopplysninger kan benyttes til utvikling og testing, er det et vilkår i pasientjournalloven § 11 annet ledd at dette skjer i «*lukkede testmiljøer*». Også for denne typen databehandling gjelder de krav til informasjonssikkerhet og personvern som følger av pasientjournalloven § 22, jf. personvernforordningen art. 32. Det gjelder altså de samme kravene til informasjonssikkerhet og personvern i et produksjonsmiljø og i et testmiljø.

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

I dette kapittelet beskrives hvilke risikoreduserende tiltak som bør vurderes dersom identifisert risiko tilsier at det er nødvendig. Det er først når de generelle kravene til det lukkede testmiljøet er oppfylt (se begrepsforklaringen for lukket testmiljø i kapittel 5.11) og testmiljøets samlede risikobilde er vurdert og akseptert av virksomheten, at testmiljøet kan vurderes som lukket i henhold til pasientjournalloven § 11 annet ledd.

Følgende to risikoelementer 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.

## 3.1 Utvikling, testing og prøvedrift

Ved utvikling av nye, eller endring av eksisterende systemer, vil man ofte starte med en utviklingsfase, etterfulgt av en eller flere testfaser før produksjonssetting. Med «utvikling» menes det å lage eller oppgradere et IKT-system slik at det er klart for testing. Underveis i utviklingsprosessen vil det ofte også være behov for testing, som del av utviklingsprosessen. I de tilfellene det oppdages feil under testing, vil man gå tilbake til utvikling for å rette opp eventuelle feil.

Testing er viktig for å kunne sikre at systemer har nødvendig funksjonalitet og stabilitet før de settes i produksjon. Testing gjennomføres for å kontrollere at systemer og endringer man ønsker å ta i bruk fungerer slik de skal, og at man har kontroll på blant annet integrasjoner, visning av data og ytelse.

Med prøvedrift menes den innledende fasen etter at et utviklings- eller testløp er ferdigstilt, og hvor systemet er i produksjon for å kontrollere at funksjonaliteten er tilfredsstillende. Selv om databehandlingen i prøvedrift foregår *utenfor* de lukkede testmiljøene vil pasientjournalloven § 11, annet ledd likevel kunne komme til anvendelse, da det følger av forarbeidene at «prøvedrift i denne sammenhengen vil være omfattet av begrepet ”test”.» (Prop. 91 L (2021-2022) Endringer i pasientjournalloven mv. (nasjonal digital samhandling) kapittel 7.4).

Ofte vil fasen med prøvedrift startes med noe lavere kapasitet enn i en normal driftssituasjon. I prøvedrift er det normalt at helsevirksomheten, leverandører og andre har utvidede tilganger til systemet. Årsaken til økte tilganger er å gi teknisk bistand, feilretting, brukerstøtte og opplæring, og for å effektivt sikre at systemet fungerer etter forventingene.

I helse- og omsorgssektoren er det særlig viktig at også testing ivaretar sentrale prinsipper om integritet, tilgjengelighet og konfidensialitet.

## 3.2 Separate utviklings- og testmiljøer

Så langt det er mulig, skal det 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 produksjonsmiljøene som benyttes ved ytelse av helsehjelp. Testmiljøer bør også merkes tydelig, for å unngå at testsystemet blir benyttet ved 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 som følge av at testdata har blitt benyttet i produksjonsmiljøet.

Et testmiljø kan etableres som en permanent løsning, eller ha en tidsavgrenset varighet. Helseopplysninger som benyttes i testmiljøet må imidlertid slettes når formålet med behandlingen er oppnådd, se punkt 3.10.

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

## 3.3 Kompetanse og taushetsplikt

Helsevirksomheten 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 etter pasientjournalloven § 15, jfr. 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.

## 3.4 Dataflyt

Det vil være viktig å ha kontroll på dataflyten både i utviklings- og testmiljøet, for å unngå at data kan komme på avveie. Det bør derfor utarbeides detaljerte oversikter over dataflyten i begge miljøene, for eksempel i et dataflytskjema. Bruk av et dataflytskjema kan blant annet være et tiltak for å hindre at data som benyttes til testing kommer over i produksjonssystemer, eller overføres uplanlagt til andre miljøer internt i virksomheten eller eksternt.

Bruk av et dataflytskjema 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 3.10**Feil! Fant ikke referansekilden.**.

Det kan også være behov for å benytte perifert utstyr i forbindelse med utvikling eller testing (BYOD, medisinsk utstyr, mobiltelefoner mv.). Det er viktig at dette kommer frem av dataflytskjemaet og i risikovurderingen, se kapittel 3.7, samt at informasjon på disse enhetene blir slettet etter at prosessen er avsluttet, se kapittel 3.10.

## 3.5 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 deler av helsevirksomhetens systemer som er i produksjon. For å redusere faren for feil eller nedetid på systemer som er i drift i virksomheten, bør testplanen følge virksomhetens rammeverk for endringsledelse.

## 3.6 Vurdere datagrunnlaget

Ved bruk av helse- og personopplysninger, vil testdataene trekkes ut fra virksomhetens behandlingsrettede helseregister (datagrunnlaget) til det konkrete testformålet. Datafelter og datamengde defineres på bakgrunn av formålet som skal oppnås. Hensynet til dataminimering må ivaretas i denne forbindelse, se kapittel 4.5 nedenfor.

Virksomheten må vurdere om data som benyttes til testformål inneholder opplysninger som er begrenset eller skjermet. Dette kan omfatte opplysninger som eksempelvis er sperret av pasienten, eller opplysninger om personer med fortrolig eller strengt fortrolig adresse. Dersom uttrekket kan omfatte opplysninger der det er vurdert til 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 3.9.

Virksomheten må ivareta lovens krav til nekting av innsyn, sperring og fortrolig adresse. Dersom bruk av opplysninger underlagt slike begrensninger vurderes som nødvendig for å oppnå formålet med behandlingen, må virksomheten vurdere særskilt hvordan prinsippene

om konfidensialitet, integritet og tilgjengelighet skal ivaretas for denne delen av datagrunnlaget.

Dersom lovens krav ikke kan oppfylles, må slike opplysninger ekskluderes fra uttrekket.

I Normens faktaark 55 om Sperret adresse i Folkeregisteret er det inntatt veiledning til virksomheter som behandler opplysninger som nevnt.

Prinsippet om dataminimering skal følges når man benyttet helseopplysninger til utvikling og test, se kapittel 4.5

## 3.7 Risikovurdering og personvernkonsekvensvurdering

Virksomheten skal vurdere om informasjonssikkerhets- og personvernrisikoen forbundet med utviklings- og testaktivitetene kan aksepteres, og om det er tiltak som bør implementeres før aktiviteten starter. Slike vurderinger kan virksomheten utføre i en risiko- og sårbarhetsanalyse og i en personvernkonsekvensvurdering (DPIA).

Risikovurderinger og DPIAer skal oppdateres løpende, og minimum når endringer blir vurdert eller besluttet.

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.

## 3.8 Tilgangsstyring og kontroll

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.

For testaktiviteter er det særlig viktig at virksomheten implementerer grundige kontrollrutiner for tilgangsstyringen, da testressursenes behov for tilgang til helseopplysninger vil kunne endre seg under aktivitetens fremdrift.

Det er viktig at utviklings- og testmiljøer inkluderes i virksomhetens systemer for sikkerhetsovervåking, og at testmiljøer inkluderes i forbindelse med rapportering.

Eksempler på sikkerhetstiltak knyttet til tilgangsstyring:

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

For å sikre at det skilles mellom tilganger til testmiljøer og vanlige brukertilganger, er det viktig at det opprettes egne brukerkontoer for testing (testkontoer). Dette er også viktig for å ivareta krav til logging, se kapittel 3.9 nedenfor.

## 3.9 Logging

Virksomheten skal loggføre tilganger og hendelser i det lukkede testmiljøet. Formålet med loggingen, er at helsevirksomheten skal kunne fremvise en oversikt over bruken av testdataene, avdekke uautorisert eller forsøk på uautorisert tilgang, og slik forebygge, avdekke og forhindre sikkerhetsbrudd og legge til rette for innsyn fra pasienter og medarbeidere.

Loggopplysningene skal oppbevares til de ikke lenger er nødvendige for det formålet de er ment for. De skal deretter slettes, se kapittel 3.10.

Supplerende veiledning om logging kan finnes i Normens kapitel 5.4.4.

## 3.10 Sletting

Helseopplysninger som er brukt til utvikling eller testing av behandlingsrettede helseregistre skal slettes når formålet med aktivitetene er oppfylt. Eventuelle utskrifter og kopier fra 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 helsevirksomheten må vurdere

## 4.1 Rettslig grunnlag for behandling av helseopplysninger til utvikling og testformål

Det rettslige grunnlaget for behandling av direkte identifiserbare opplysninger til utviklings- og testformål av behandlingsrettede helseregistre er pasientjournalloven § 11 andre 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 informasjonssystemer på eget initiativ ønsker å utvikle et system i den hensikt å selge dette til helse- og omsorgstjenesten. I et slikt tilfelle vil databehandlingen ikke ha rettslig grunnlag i pasientjournalloven § 11 annet ledd.

## 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 slike data 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 virksomheten allerede har en databehandleravtale med, og hvor den planlagte aktiviteten er dekket av avtalen. Dersom foreliggende databehandleravtale ikke er dekkende må den oppdateres til å inkludere den de aktivitetene som inngår i utvikling og testing, alternativet er å skrive egen databehandleravtale for utvikling og testing.

## 4.3 Oppdatering av behandlingsprotokollen

Den dataansvarlige virksomheten har ansvar for å ha oversikt over all behandling av helse- og personopplysninger. Virksomheten skal føre protokoll over databehandlingen, jfr. personvernforordningen art. 30. Dette omfatter også den databehandlingen som foregår i forbindelse med utviklings- og testaktiviteter.

Protokollen skal vedlikeholdes kontinuerlig som en løpende aktivitet, og skal inneholde detaljert informasjon om alle behandlingsaktiviteter i virksomheten. 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 betyr at det tas hensyn til personvern i alle faser av utviklingen av et system eller en løsning.

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

## 4.5 Dataminimering

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. Det skal ikke benyttes personidentifiserbare data i større utstrekning enn dette.

Mengden data og type data vil være avhengig av hva man skal teste (formålet). Skal man for eksempel teste full funksjonalitet eller ha prøvedrift av systemet, vil man behøve nok data til at testen blir reell. Skal det derimot testes avgrenset funksjonalitet, vil et mindre utvalg data kunne være tilstrekkelig.

# 5. Sentrale begreper i retningslinjen

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

## 5.1 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, kjernejournal, pasientkort, individuell plan, ulike fagsystemer, pasientadministrative systemer 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.

## 5.2 Rettslig grunnlag

All behandling av helseopplysninger 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 opplysninger, for eksempel helseopplysninger, må behandlingen også falle inn under et av unntakene i artikkel 9.

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 rettslige grunnlaget følger her av pasientjournalloven § 11 annet ledd.

Det rettslige grunnlaget stiller krav til formålet med bruken av dataene, altså hva virksomheten ønsker å oppnå. For å falle innenfor pasientjournalloven § 11 annet ledd, må formålet være å utvikle og teste behandlingsrettede helseregistre. Det må altså vurderes om det er nødvendig å bruke direkte identifiserbare helseopplysninger for å oppnå dette formålet. Bestemmelsen setter også andre vilkår for å benytte helseopplysninger til utvikling og testing (se kapittel 2). Alle vilkårene må være oppfylt for at virksomheten skal kunne benytte helseopplysninger til dette.

## 5.3 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 kapittel0 4.

## 5.4 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.»*

Det er lagt til grunn i retningslinjen her at det fra behandlingsrettede helseregistre også vil kunne trekkes ut ordinære personopplysninger, som vil kunne benyttes i forbindelse med utvikling og testing i henhold til pasientjournalloven § 11 annet ledd.

## 5.5 Direkte identifiserbare helseopplysninger

Pasientjournalloven § 11 annet ledd benytter begrepet ”*direkte identifiserbare helseopplysninger*”. At opplysninger er ”*direkte identifiserbare”* betyr i denne sammenhengen at de behandles i *klartekst*, uten noen form for pseudonymisering, kryptering eller andre tiltak ment for å redusere risikoen for personvernkrenkelser. I situasjoner hvor dataansvarlige helsevirksomheter benytter direkte identifiserbare opplysninger i utvikling og testing etter pasientjournalloven § 11 annet ledd, er det derfor viktig å redusere risikoen for personvernkrenkelser ved å lukke testmiljøet, se kapittel 03.

## 5.6 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*.»

Bruken av pseudonyme personopplysninger vil i mindre grad utfordre personvernet enn bruk av direkte identifiserbare helseopplysninger. Ved utvikling og testing etter pasientjournalloven § 11 annet ledd, må den dataansvarlige helsevirksomheten alltid først vurdere om formålet kan oppnås ved bruk av fiktive eller anonyme opplysninger, se kapittel 2.

## 5.7 Anonyme opplysninger

Retningslinjen legger her 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 til utvikling og testing fra behandlingsrettede helseregistrene, må alle personentydige kjennetegn, slik 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 imidlertid 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.

## 5.8 Fiktive opplysninger / syntetiske data

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.

Bruk av fiktive opplysninger medfører ingen risiko knyttet til ivaretakelse av personvernreglene.

## 5.9 Produksjonsmiljø

Et produksjonsmiljø består av maskinvare, programvare og informasjon som til sammen leverer et sett funksjonalitet og tjenester til sluttbrukerne. Eksempelvis vil et EPJ-system i ordinær drift kjøre i enten helsevirksomhetens eller dens leverandørers produksjonsmiljø.

Produksjonsmiljøet skal ha tekniske og organisatoriske beskyttelsesmekanismer for å ivareta de informasjonsverdiene som inngår i produksjonsmiljøet, for eksempel helse- og personopplysninger.

## 5.10 Utviklings- og testmiljø

Helsevirksomheter vil i større eller mindre grad ta i bruk ulike typer testmiljøer, som karakteriseres av å være kontrollerte domener med spesifikke formål og funksjoner, særlig tilrettelagt for utviklings- og testaktiviteter. Det vil ofte være et mål å skape et testmiljø som i størst mulig grad svarer til produksjonsmiljøet, for å skape gode og realistiske rammer for testingen.

Helse- og omsorgssektoren behandler særskilt sensitive og kritiske informasjonsverdier. Informasjonsverdienes iboende risiko må håndteres på en god og sikker måte, også i utviklings- og testmiljø.

## 5.11 Lukket utviklings- og testmiljø

Begrepet benyttes i denne retningslinjen om et utviklings- eller testmiljø der det er implementert nødvendige mekanismer og tiltak for å hindre at uvedkommende kan få tilgang til helseopplysninger i miljøet, 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 et utviklings- og testmiljø, må vurderes konkret av virksomheten, og vil være avhengig av hvilke informasjonsverdier som skal sikres, formålet med utviklingen eller testen, samt virksomhetens risikoakseptansenivå.