DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Prop. 152 L

(2024–2025)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i helselovgivningen (tilgjengeliggjøring av helsedata og krav til tekniske og organisatoriske sikkerhetstiltak)

Innhold

DET KONGELIGE
HELSE- OG OMSORGSDEPARTEMENT

Prop. 152 L

(2024–2025)

Proposisjon til Stortinget (forslag til lovvedtak)

Endringer i helselovgivningen (tilgjengeliggjøring av helsedata og krav til tekniske og organisatoriske sikkerhetstiltak)

Tilråding fra Helse- og omsorgsdepartementet 10. juni 2025, godkjent i statsråd samme dag.
(Regjeringen Støre)

1 Proposisjonens hovedinnhold

Helse- og omsorgsdepartementet legger i denne proposisjonen frem forslag til endringer i pasientjournalloven, helseregisterloven og helsepersonelloven. Den sikkerhetspolitiske situasjonen og endringene i risikobildet synliggjør et behov for regelendringer for bedre å kunne ivareta helse- og omsorgstjenestens oppgaver og den enkeltes personvern, ved å redusere risiko for at kritiske samfunnsfunksjoner påvirkes og at store sett med helsedata blir tilgjengelig for aktører som kan utgjøre en trussel.

For det første muliggjør forslaget begrenset deling av enkelte store sett med helsedata, av hensyn til samfunnets evne til å verne grunnleggende verdier og funksjoner og liv og helse. «Helsedata» er et vidt begrep som kan omfatte alle typer opplysninger om helse, enten de frembringes i helse- og omsorgstjenestene, gjennom de store befolkningsundersøkelsene eller på andre måter. Begrepet helsedata favner videre enn begrepet helseopplysninger slik det er definert i personvernforordningen artikkel 4 nr. 15. Helsedata kan være anonyme, direkte identifiserbare eller indirekte identifiserbare.

For det andre foreslår departementet at det ved vurderingen av hva som er et forsvarlig sikkerhetsnivå etter pasientjournalloven § 22 og helseregisterloven § 21, også skal tas hensyn til den teknologiske utviklingen og kritiske samfunnsfunksjoner.

Den digitale trusselen er skjerpet, med risiko for bevisste anslag, også mot helse- og omsorgssektoren.

Høringsinstansene deler i hovedsak departementets syn på risikobildet og sikkerhetsutfordringene helse- og omsorgstjenesten står overfor. Departementet oppfatter at det også er bred enighet om behovet for oppdaterte og effektive sikkerhetstiltak. I høringen foreslo departementet også krav til bakgrunnssjekk av personell med enkelte kritiske funksjoner. Den endrede sikkerhetspolitiske situasjonen har medført at denne

delen av forslaget i hovedsak vil ivaretas gjennom sikkerhetsloven. Med unntak av hjemmelen for innhenting av politiattest, er forslaget om bakgrunnssjekk ikke videreført i lovforslaget.

Det er gjort enkelte justeringer i forslaget basert på innspill i høringen. Terminologien «nasjonale sikkerhetsinteresser» er i høringsnotatet benyttet på en måte som favner videre enn legaldefinisjonen i sikkerhetsloven § 1-5. Informasjonen det gjelder har et skadepotensiale som er løsere eller mer indirekte knyttet til nasjonale sikkerhetsinteresser (avledet skadepotensiale), slik at det ikke direkte kan sies å falle inn under sikkerhetslovens regler om beskyttelse av informasjon. Skadepotensialet er avledet og vil være noe mindre enn ved kompromittering av objekter som er skjermet etter sikkerhetsloven, men kritiske samfunnsfunksjoner vil likevel rammes. Departementet foreslår derfor å ta terminologien «nasjonale sikkerhetsinteresser» ut av lovforslaget, slik at hovedfokus heller blir alle typer kritiske funksjoner som ved bortfall truer helse- og omsorgstjenestens evne til å ivareta sine oppgaver.

2 Bakgrunnen for lovforslaget

2.1 Den sikkerhetspolitiske situasjonen

Den sikkerhetspolitiske situasjonen i Norge er mer uforutsigbar enn på mange år. Dette vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver. De siste årene har hendelser som Russlands invasjon av Ukraina, sabotasje og innsidevirksomhet preget trusselbildet. Det er viktigere enn noen gang at vi samarbeider om å verne verdier og kritiske samfunnsfunksjoner. Evnen til å levere helsetjenester av god kvalitet med tilstrekkelig pasientsikkerhet, er en slik kritisk samfunnsfunksjon. For å beskytte oss mot forskjellige trusler kreves det godt sikkerhets- og beredskapsarbeid på tvers av sektorer, og i den enkelte virksomhet og hos den enkelte medarbeider.

Dette understreker også behovet for at helse- og omsorgssektoren har et oppdatert regelverk og enhetlig krav å forholde seg til. Det synliggjør også viktigheten av tett samarbeid med tjenestene som tegner dagens trusselbilde og miljøer som studerer mer langsiktige trender.

I nasjonal trusselvurdering (NTV) for 2025 gir Politiets sikkerhetstjeneste (PST) en ugradert redegjørelse av trusselbildet som det norske samfunnet står overfor dette året. Vurderingen setter søkelys på etterretningstrusselen, med særskilt vekt på russisk og kinesisk etterretning, i tillegg forventes aktivitet fra Iran og Nord-Korea. I hovedpunkt i delen som gjelder statlig etterretningsvirksomhet, fremheves:

> Fremmed etterretning vil bruke en rekke ulike virkemidler og metoder, som stadig tilpasses endrede forutsetninger og norske mottiltak. Flere av disse tiltakene inngår i det som ofte omtales som sammensatt virkemiddelbruk. Det inkluderer cyberoperasjoner, rekruttering av kilder, påvirkningsoperasjoner, sabotasje, fordekte anskaffelser og sikkerhetstruende økonomisk virkemiddelbruk. I tillegg vil flyktninger, dissidenter og regimekritikere bli utsatt for kartlegging og overvåking fra flere autoritære regimer.

Nasjonal sikkerhetsmyndighet (NSM) uttaler i rapporten «Risiko 2025» at:

> Digitalisering av samfunnet gir store gevinster, men skaper samtidig nye sårbarheter. Uavhengig av om et system slutter å fungere som følge av en tilfeldig, teknisk eller menneskelig feil, eller villede handlinger, er konsekvensene av nedetid store. Utnyttelse av nye sårbarheter i programvarer øker, samtidig som mobiltelefoner, moderne kjøretøy og bruk av kunstig intelligens introduserer nye sårbarhetsflater.
>
> Mange virksomheter baserer egen kjernevirksomhet på teknologi og tjenester fra tredjeparter og underleverandører. Flere er også selv leverandører og blir en del av det nasjonale sikkerhetsarbeidet gjennom ulike leverandørkjeder. Uten god oppfølging av sikkerhetsnivået i hele leverandørkjeden eksponeres virksomheter for unødig risiko.

I Fokus 2025 uttaler Etterretningstjenesten at militær bruk av sivil teknologi utfordrer eksportkontrollregimer:

> Bruk av sivil teknologi i militære våpenprogrammer utfordrer tradisjonelle eksportkontrollregimer. Sivil teknologi kan utnyttes både i våpen og i militære systemer for overvåkning, deteksjon og kartlegging, prosjektering, bygging og vedlikehold.
>
> Russland, Kina, Iran og Nord-Korea er blant landene som benytter en rekke metoder for å anskaffe og utnytte sivil, vestlig teknologi til militære formål. Kompliserte anskaffelsesnettverk tilslører sluttbrukeren for både leverandøren og statlige eksportkontrollmekanismer.
>
> Aktørene skaffer også tilgang til vestlig teknologi med militær nytteverdi ved å delta i internasjonale teknisk-naturvitenskaplige forskningssamarbeid.
>
> Norskprodusert maritim teknologi og kommunikasjons- og navigasjonsteknologi, samt norsk forskning og utvikling innen halvleder- og sensorteknologi, materialteknologi, kryptologi, IKT-sikkerhet, bioteknologi og kunstig

intelligens, er attraktive objekter for fordekte anskaffelser fra aktører underlagt sanksjoner og eksportkontrollregimer.

De regionale helseforetakene og Norsk helsenett SF uttaler i Trusselvurdering 2025 – Det digitale trusselbildet mot spesialisthelsetjenesten, at:

> Spesialisthelsetjenesten opplever daglig forsøk på angrep fra organiserte kriminelle. Angrep fra organiserte kriminelle som rammer spesialisthelsetjenestens evne til å levere helsetjenester vil kunne påvirke liv og helse, men også redusere befolkningens tillit til at de vil få god og trygg behandling av det offentlige helsevesenet. Spesialisthelsetjenesten er derfor et ettertraktet og utsatt mål, og vi forventer økt oppmerksomhet fra utpressingsgrupper og deres samarbeidspartnere i kommende periode. Vi vurderer det som meget sannsynlig at spesialisthelsetjenesten vil bli utsatt for angrepsforsøk fra organisert kriminalitet og at trusselen er meget høy.

Videre uttales at:

> Teknologiutviklingen gjør at cyberspionasje og etterretningsvirksomhet kan gjennomføres mer effektivt, i et større omfang og med lavere risiko. Trusselbildet er komplekst og uoversiktlig, noe som gjør det vanskelig å skille cyberspionasje fra andre typer cyberangrep. Statlige aktører gjennomfører cyberspionasjekampanjer mot vestlig helsevesen, og vi forventer at dette også vil treffe spesialisthelsetjenesten i Norge. Vi vurderer at trusselen fra cyberspionasje er høy. Vi vurderer det som sannsynlig at spesialisthelsetjenesten vil utsettes for cyberspionasje fra aktører med direkte eller indirekte koblinger til russiske og kinesiske etterretningsorganisasjoner.

Norsk helsenett SF (Helse- og kommuneCERT), har i situasjonsbilde oppdatert januar 2024 uttalt:

- Det er meget sannsynlig at fremmede stater ser på helsesektoren som et mål for spionasje.
- Det er sannsynlig at norsk helse- og kommunesektor vil treffes av angrep fra aktører som et ledd i det generelle arbeidet til statlige eller stats-sponsede etterretningstjenester.

2.2 Høringen

2.2.1 Generelt

Forslag til endringer i pasientjournalloven, helseregisterloven og helsepersonelloven ble sendt på høring 26. juni 2024, med frist 1. oktober 2024.

2.2.2 Høringsinstansene

Høringen ble sendt til følgende instanser:

Departementene

Arbeid- og velferdsdirektoratet
Barne-, ungdoms- og familiedirektoratet
Bioteknologirådet
Datatilsynet
De fylkeskommunale eldrerådene
De regionale komiteene for medisinsk og helsefaglig forskningsetikk (REK)
Den nasjonale forskningsetiske komité for medisin og helsefag (NEM)
Den rettsmedisinske kommisjon
Digitaliseringsdirektoratet
Direktoratet for medisinske produkter
Direktoratet for strålevern og atomsikkerhet
Diskrimineringsnemnda
Folkehelseinstituttet
Forbrukertilsynet
Forbrukerrådet
Fylkesrådet for funksjonshemmede
Helsedirektoratet
Helse- og sosialombudet i Oslo
Helsepersonellnemnda
Helseøkonomiforvaltningen (HELFO)
Høgskoler med helsefaglig utdanning
Institutt for helse og samfunn HELSAM
Landets kontrollkommisjoner
Landets regionale kompetansesentre for rusmiddelspørsmål
Landets regionale ressurssentre om vold, traumatisk stress og selvmordsforebygging
Nasjonalt klageorgan for helsetjenesten (Helseklage)
NOKUT (Nasjonalt organ for kvalitet i utdanningen)
Norges forskningsråd
Norges institusjon for menneskerettigheter (NIM)
Norsk helsenett SF
Norsk pasientskadeerstatning (NPE)
Pasient- og brukerombudene
Personvernnemnda
Regelrådet

Regionsentrene for barn og unges psykiske helse
Regjeringsadvokaten
Riksrevisjonen
Råd for et aldersvennlig Norge
Sametinget
Senter for medisinsk etikk ved Universitetet i Oslo
Senter for omsorgsforskning
Sikt – Kunnskapssektorens tjenesteleverandør
Sivilombudet
Statens helsetilsyn
Statens råd for likestilling av funksjonshemmede
Statistisk sentralbyrå (SSB)
Statsforvalterne
Sysselmesteren på Svalbard
Universitetene

Landets kommuner
Landets fylkeskommuner
Landets helseforetak
Landets regionale helseforetak

Actis
ACOS AS
ADHD Norge
ANSA (Association of Norwegian Students Abroad)
LHL Hjerneslag og Afasi

Akademikerne
A-larm bruker- og pårørendeorganisasjon for åpenhet om rus og behandling
Aleris Helse AS
Alliance Healthcare Norge Apotekdrift AS
Alliance Healthcare Norge AS
Allmennlegeforeningen
Amnesty International Norge
Anonyme alkoholikere
Apotek 1 Gruppen AS
Apotekforeningen
Apotekgruppen
Arbeiderbevegelsens rus- og sosialpolitiske forbund
Aurora – støtteforening for mennesker med psykiske helseproblemer
Autismeforeningen i Norge
Barn av rusmisbrukere – BAR
Barnekreftforeningen
BarnsBeste
Bedriftsforbundet
Bikuben – regionalt brukerstyrt senter
Bipolarforeningen
Blå Kors Norge
Borgestadklinikken
Buddhistforbundet
CGM (Compugroup Medical Norway AS)
Colosseumklinikken AS tannlege
Dedicare
Delta
Den norske Advokatforening
Den norske Dommerforening
Den Norske Jordmorforening
Den norske legeforening
Den norske tannlegeforening
Det Hjelper
Diabetesforbundet
DIPS ASA
DNT – edru livsstil
Erfaringssentrum
Europharma AS
Fagforbundet
Fagrådet innen rusfeltet i Norge
Familieklubbene i Norge
Fana medisinske senter
Farma Holding
Fellesorganisasjonen (FO)
Finans Norge
FMR Felleskap – Menneskeverd – Rusfrihet
Foreningen for blødere i Norge
Foreningen for hjertesyke barn
Foreningen for human narkotikapolitikk
Foreningen for Muskelsyke
Foreningen for kroniske smertepasienter
Foreningen Norges Døvblinde (FNDB)
Foreningen tryggere ruspolitikk
Foreningen vi som har et barn for lite
Forskerforbundet
Forskningsstiftelsen FAFO
Frambu
Frelsesarmeen
Frivillighet Norge
Funksjonshemmedes Fellesorganisasjon (FFO)
Fürst medisinske laboratorium AS
Gatejuristen
Helseutvalget
HIV-Norge
Hjernerådet
Hvite Ørn – interesse- og brukerorganisasjon for psykisk helse
Hørselshemmedes Landsforbund
IKT Norge
Infodoc
Informasjonssenteret Hieronimus
Institutt for aktiv psykoterapi (IAP)
Institutt for barne- og ungdomspsykoterapi
Institutt for gruppeanalyse og gruppepsykoterapi
Institutt for mentalisering
Institutt for psykoterapi
Institutt for samfunnsforskning
IOGT Norge
IRIS

Ja, det nytter
Junior- og barneorganisasjonen JUBA
JURK
Juss-Buss
Jussformidlingen
Jusshjelpa
Juvente
Kirkens bymisjon
Kliniske ernæringsfysiologiske forening
Kommunalbanken
Kommunal landspensjonskasse
Kompetansesenter for brukererfaring og tjenesteutvikling (KBT)
Kreftforeningen
Kriminalomsorgen
KS
Landets private sykehus
Landsforbundet for utviklingshemmede og pårørende (LUPE)
Ivareta – Pårørende berørt av rus
Landsforeningen 1001 dager – mental helse under graviditet og etter fødsel
Landsforeningen Alopecia Areata
Landsforeningen for etterlatte ved selvmord – LEVE
LHL
Landsforeningen for Huntingtons sykdom
Landsforeningen for Nyrepasienter og Transplanterte
Landsforeningen for pårørende innen psykisk helse
Landsforeningen for slagrammede
Landsforeningen mot fordøyelsessykdommer
Landsforeningen we shall overcome
Landsgruppen av psykiatriske sykepleiere
Landsgruppen av helsesøstre, NSF
Landslaget for rusfri oppvekst
Landsorganisasjonen i Norge (LO)
Legeforeningens forskningsinstitutt
Legemiddelgrossistforeningen
Legemiddelindustrien
Legemiddelparallellimportørforeningen
Legestudentenes rusopplysning
Likestillingssenteret
LISA-gruppene
MA – Rusfri Trafikk
Marborg
Matmerk
Mental Helse Norge
Mental Helse Ungdom
MIRA-senteret
Moreno-instituttet – Norsk psykodramainstitutt
Munn- og halskreftforeningen
MS – forbundet
NA – Anonyme Narkomane
Nasjonalforeningen for folkehelsen
Nasjonal kompetansetjeneste for aldring og helse
Nasjonal kompetansetjeneste for sjeldne diagnoser
Nasjonal kompetansetjeneste for utviklingshemning og psykisk helse
Nasjonalt kompetansemiljø om utviklingshemming – NAKU
Nasjonalt kompetansesenter for prehospital akuttmedisin – NAKOS
Nasjonalt kompetansesenter for migrasjons- og minoritetshelse – NAKMI
Nasjonalt kompetansesenter for psykisk helsearbeid – NAPHA
Nasjonalt senter for e-helseforskning
Nasjonalt senter for erfaringskompetanse innen psykisk helse
NORCE Norwegian Research Center AS
Norges Astma- og Allergiforbund
Norges Blindeforbund
Norges Døveforbund
Norges Farmaceutiske Forening
Norges Fibromyalgi Forbund
Norges Handikapforbund
Norges kristelige legeforening
Norges Kristne Råd
Norges ingeniør og teknologiorganisasjon/ Bioingeniørfaglig institutt (NITO/BFI)
Norges Juristforbund
Norges kommunerevisorforbund
Norges kvinne- og familieforbund
Norges Parkinsonforbund
Norges Tannteknikerforbund
Norlandia
Normal Norge
Norsk barne- og ungdomspsykiatrisk forening
Norsk Biotekforum
Norsk Cøliakiforening
Norsk Epilepsiforbund
Norsk Ergoterapeutforbund
Norsk Farmasøytisk Selskap
Norsk Forbund for Osteopatisk Medisin
Norsk Forbund for psykoterapi
Norsk Forbund for Svaksynte
Norsk Forbund for Utviklingshemmede
Norsk Forening for barn og unges psykiske helse (N-BUP)
Norsk Forening for cystisk fibrose
Norsk Forening for Ernæringsfysiologer
Norsk Forening for Helse- og Treningsfysiologer (NFHT)
Norsk forening for infeksjonsmedisin
Norsk forening for kognitiv terapi
Norsk Forening for nevrofibromatose
Norsk forening for palliativ medisin

Norsk Forening for Psykisk Helsearbeid
Norsk forening for rus- og avhengighetsmedisin (NFRAM)
Norsk forening for slagrammede
Norsk Forening for Tuberøs Sklerose
Norsk Forum for terapeutiske samfunn
Norsk Fysioterapeutforbund
Norsk Førstehjelpsråd
Norsk Gestaltterapeut forening
Norsk gynekologisk forening
Norsk Helsesekretærforbund
Norsk Immunsviktforening
Norsk Intravenøs Forening
Norsk karakteranalytisk institutt
Norsk Kiropraktorforening
Norsk legemiddelhåndbok
Norsk Logopedlag
Norsk Manuellterapeutforening
Norsk Medisinaldepot AS
Norsk OCD forening, ANANKE
Norsk Ortopedisk Forening
Norsk Osteoporoseforening
Norsk paramedicforening
Norsk Presseforbund
Norsk Psoriasis Forbund
Norsk Psykiatrisk Forening
Norsk Psykoanalytisk Forening
Norsk Psykologforening
Norsk Radiografforbund
Norsk Revmatikerforbund
Norsk selskap for ernæring
Norsk senter for stamcelleforskning
Norsk sykehus- og helsetjenesteforening (NSH)
Norsk sykepleierforbund
Norsk Tannhelsesekretærers Forbund
Norsk Tannpleierforening
Norsk Tjenestemannslag (NTL)
Norsk Tourette Forening
Norske Fotterapeuters Forbund
Norske Homeopaters Landsforbund
Norske Kvinners Sanitetsforening
Norske Ortoptister forening
Norske Sykehusfarmasøyters Forening
NUPI
Næringslivets Hovedorganisasjon (NHO)
Organisasjonen Voksne for Barn
Oslo amatørbryggerlaug
Omsorgsjuss
Parat Helse
Pensjonistforbundet
Personskadeforbundet
Tannleger i privat sektor TiPS
Privatpraktiserende Fysioterapeuters Forbund
Prima Omsorg
Program for helseøkonomi i Bergen
proLAR
Psykiatrialliansen BIL
Pårørendealliansen
Pårørendesenteret
Rettspolitisk forening
ROM – Råd og muligheter
ROS – Rådgivning om spiseforstyrrelser
Rusmisbrukernes interesseorganisasjon (RIO)
Ryggforeningen i Norge
Ryggmargsbrokk og hydrocephalusforeningen
Røde Kors
Rådet for psykisk helse
Sagatun brukerstyrt senter
Samarbeidsforumet av funksjonshemmedes organisasjoner (SAFO)
Selvhjelpsstiftelsen
Senior Norge
Senter for klinisk dokumentasjon og evaluering (SKDE)
Senter for psykoterapi og psykososial rehabilitering ved psykoser (SEPREP)
Senter for seniorpolitikk
SINTEF Helse
Sintef Unimed, Helsetjenesteforskning i Trondheim
Skeiv ungdom
Spekter
Spillavhengighet Norge
Spiseforstyrrelsesforeningen
Stabburshella bruker- og pårørendeforum og værested
Statstjenestemannsforbundet
Stiftelsen Albatrossen ettervernsenter
Stiftelsen Angstringen Norge (ARN)
Stiftelsen Det er mitt valg
Stiftelsen Fransiskushjelpen
Stiftelsen Golden Colombia
Stiftelsen Institutt for spiseforstyrrelser
Stiftelsen iOmsorg
Stiftelsen Kraft
Stiftelsen Menneskerettighetshuset
Stiftelsen Norsk Luftambulanse
Stiftelsen Organdonasjon
Stiftelsen Phoenix Haga
Stiftelsen Pinsevennenes evangeliesentre
Stiftelsen Psykiatrisk Opplysning
Stiftelsen Pårørendesenteret
Stiftelsen Verdighetssenteret – omsorg for gamle
Stoffskifteforbundet
Tekna
Teknologirådet
Trust Arktikugol
Turner Syndrom foreningen i Norge
Tyrili Utvikling og prosjekt – stiftelse
Ungdom mot narkotika – UMN

Ung i Trafikk
Unio
Universitets- og høyskolerådet
Utdanningsforbundet
Utviklingssentrene for sykehjem og hjemmetjenester
Velferdsforskningsinstituttet NOVA
Vestlandske Blindeforbund
Virke
Visma
Volvat Medisinske Senter AS
Vårres regionalt brukerstyrt senter Midt-Norge
Yngre legers forening
Yrkesorganisasjonenes Sentralforbund (YS)

2.2.3 Høringsuttalelsene

Departementet har mottatt i alt 71 høringsuttalelser. 6 av disse hadde ingen merknader.

Følgende instanser hadde ikke merknader:

Justis- og beredskapsdepartementet
Samferdselsdepartementet

Statistisk sentralbyrå
Statsforvalteren i Østfold, Buskerud, Oslo og Akershus
Norsk Tannpleierforening

Diskrimineringsnemnda uttalte at de ikke avgir høringsuttalelse.

Følgende instanser hadde merknader:

Datatilsynet
Direktoratet for strålevern og atomsikkerhet
Folkehelseinstituttet
Helsedirektoratet
Kripos
Likestillings- og diskrimineringsombudet
Nasjonal sikkerhetsmyndighet
Politidirektoratet
Politiets enhet for vandelskontroll og politiattester
Politiets sikkerhetstjeneste
Sivil klareringsmyndighet
Sysselmesteren på Svalbard

Helsetjenestens Driftsorganisasjon for Nødnett
Helse Bergen HF
Helse Midt-Norge RHF
Helse Møre og Romsdal HF
Helse Nord IKT
Helse Nord RHF
Helse Nord-Trøndelag HF
Helse Stavanger HF
Helse Sør-Øst RHF
Helse Vest IKT
Helse Vest RHF
Hemit HF
Luftambulansetjenesten HF
Nordlandssykehuset HF
Norsk helsenett SF
Oslo universitetssykehus HF
St. Olavs hospital HF
Sjukehusapoteka Vest HF
Sykehusapotekene i Midt-Norge HF
Sykehuspartner HF
Sørlandet sykehus HF
Universitetssykehuset Nord-Norge HF
Vestre Viken HF

Akershus fylkeskommune
Andøy kommune
Buskerud fylkeskommune
De regionale forskningsetiske komiteer for medisinsk og helsefaglig forskningsetikk
KS
Norges teknisk-naturvitenskapelige universitet
UiT Norges Arktiske Universitet
Universitetet i Bergen
Universitetet i Oslo
Vestfold fylkeskommune

Advokatforeningen
Apotekforeningen
Arbeidsgiverforeningen Spekter
ELIXIR Norge
Fagforundet
Fürst Medisinsk Laboratorium
Helseplattformen AS
Kernel AS
Legemiddelindustrien LMI
Mental Helse Ungdom
NITO – Norges Ingeniør- og Teknologorganisasjon
Norske Ortoptisters Forening
Norsk Forening for Farmakoepidemiologi
Norsk Radiografforbund
Norsk Sykepleierforbund
Pilar – kompetansetjenesten for psykisk helse og barnevern (uten merknader)
Senior Norge
Spekter
Tekna – Teknisk-naturvitenskapelig forening
Visma Flyt AS

3 Gjeldende rett

3.1 Pasientjournalloven

Lovens formål er at behandling av helseopplysninger skal skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at relevante og nødvendige opplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell. Samtidig skal loven sikre at opplysninger ikke gis til uvedkommende, og sikre pasienters og brukeres personvern, pasientsikkerhet og rett til informasjon og medvirkning.

Pasientjournalloven gjelder behandling av helseopplysninger som er nødvendige for å yte, administrere eller kvalitetssikre helsehjelp til enkeltpersoner, jf. § 3.

Krav til informasjonssikkerhet følger av § 22. I bestemmelsen er det bestemt at den dataansvarlige og databehandleren, skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll. Bestemmelsen er direkte knyttet til personvernforordningen artikkel 32 ved henvisning.

Av § 22 andre ledd følger at departementet i forskrift kan fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger.

3.2 Helseregisterloven

Lovens formål er å legge til rette for innsamling og annen behandling av helseopplysninger, for å fremme helse, forebygge sykdom og skade og gi bedre helse- og omsorgstjenester. Loven skal sikre at behandlingen foretas på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste. Dette følger av § 1.

Lovens saklige virkeområde er regulert i § 3. Loven gjelder for behandling av helseopplysninger til statistikk, helseanalyser, forskning, kvalitetsforbedring, planlegging, styring og beredskap i helse- og omsorgsforvaltningen og helse- og omsorgstjenesten.

Helseregisterloven § 19 til § 19 h regulerer adgangen til å tilgjengeliggjøre og sammenstille helseopplysninger fra helseregistre. Utarbeidelse og tilgjengeliggjøring av anonym statistikk og andre anonyme opplysninger er regulert i § 19. Det er fri adgang til å tilgjengeliggjøre anonym statistikk og andre anonyme opplysninger, fordi slike data ikke kan knyttes til enkeltpersoner og derfor ikke omfattes av reglene om personvern og taushetsplikt.

Paragrafene (§ 19 til § 19 h) er utformet i samsvar med prinsippet om dataminimering i personvernforordningen artikkel 5 nr. 1 bokstav c. Det følger av dette prinsippet at graden av personidentifikasjon skal være så liten som mulig (jf. helseregisterloven § 6 andre ledd første punktum). Utgangspunktet er derfor at opplysninger fra helseregistre som tilgjengeliggjøres skal være anonyme. Direkte eller indirekte personidentifiserende opplysninger kan bare tilgjengeliggjøres dersom det er nødvendig ut fra formålet med behandlingen.

Tilgjengeliggjøring av helseopplysninger er regulert i § 19 a. Bestemmelsen fastsetter vilkårene for tilgjengeliggjøring av direkte og indirekte personidentifiserbare helseopplysninger fra helseregistre, inkludert sammenstilte datasett. Dersom vilkårene i helseregisterloven § 19 a er oppfylt, er det ikke bare tillatt, men også en plikt, for den dataansvarlige å tilgjengeliggjøre opplysningene.

Reglene for dispensasjon fra taushetsplikten følger av § 19 e. Helseopplysninger i helseregistre er taushetsbelagte, jf. helseregisterloven § 17 som viser til helsepersonelloven §§ 21 flg. Dersom søkeren skal kunne få opplysningene, må enten de registrerte ha samtykket til tilgjengeliggjøringen eller så må tilgjengeliggjøringen være i samsvar med unntak eller dispensasjon fra taushetsplikten. Helseregisterloven § 19 e fastsetter hvilke vilkår som må være oppfylt for å kunne gi dispensasjon fra taushetsplikten ved tilgjengeliggjøring fra helseregistre. Bestemmelsen regulerer vedtak om dispensasjon fra taushetsplikten ved tilgjengeliggjøring av opplysninger som er omfattet av helseregisterloven. Ved helsepersonells tilgjengeliggjøring av opplysninger fra pasientjournaler

og andre behandlingsrettede helseregistre, gjelder helsepersonelloven § 29.

I helseregisterloven § 19 b er det gitt et særskilt unntak fra taushetsplikten ved tilgjengeliggjøring av indirekte identifiserbare helseopplysninger fra nasjonale helseregistre omfattet av lovens § 11. Vilkåret er at «hensynet til den registrertes integritet og konfidensialitet er ivaretatt og behandlingen av opplysningene er av vesentlig interesse for samfunnet.»

Bestemmelsene om tilgjengeliggjøring er nærmere beskrevet i Prop. 63 L (2019–2020) *Endringer i helseregisterloven m.m. (tilgjengeliggjøring av helsedata)*.

Kravene til informasjonssikkerhet følger av helseregisterloven § 21. Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll. Bestemmelsen er direkte knyttet til personvernforordningen artikkel 32 ved henvisning. Av § 21 andre ledd følger at departementet i forskrift kan fastsette nærmere krav til informasjonssikkerhet ved behandling av helseopplysninger.

3.3 Sikkerhetsloven

Loven skal bidra til a) å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser, b) å forebygge, avdekke og motvirke sikkerhetstruende virksomhet og c) at sikkerhetstiltak gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn. Se loven § 1-1.

Objekter og infrastruktur er skjermingsverdige dersom det enten kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, eller kan skade nasjonale sikkerhetsinteresser på annen måte, jf. § 7-1.

Dersom informasjonen det gjelder har et skadepotensiale som er løsere eller mer indirekte knyttet til nasjonale sikkerhetsinteresser, vil det ikke direkte falle inn under sikkerhetslovens regler om beskyttelse av informasjon.

Av loven § 8-1 følger at personer som skal få tilgang til sikkerhetsgradert informasjon, skal autoriseres i samsvar med § 8-9. Det samme gjelder personer som skal ha adgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3.

Videre følger at personer som skal autoriseres for tilgang til informasjon gradert konfidensielt eller høyere, må ha gyldig sikkerhetsklarering. Personer som skal autoriseres for tilgang til skjermingsverdige objekter og infrastruktur som det er fattet vedtak om etter § 8-3, må ha gyldig adgangsklarering. Adgangsklarering kan benyttes som sikkerhetstiltak dersom fysisk eller logisk tilgang til hele eller deler av et objekt eller en infrastruktur gjør det mulig å skade grunnleggende nasjonale funksjoner. Det følger av klareringsforskriften (forskrift om sikkerhetsklarering og annen klarering) § 15 at hvert departement, innenfor sitt ansvarsområde kan fatte vedtak om krav til adgangsklarering der et objekt eller en infrastruktur kan være et mål for ikke-statlig terror, attentat eller annen alvorlig kriminalitet. Kan objektet eller infrastrukturen være mål for statlig sabotasje eller andre tilsiktede anslag fra en annen stat, kan departementet fatte vedtak om krav til utvidet adgangsklarering.

En person kan bare klareres dersom det ikke finnes rimelig grunn til å tvile på at personen er sikkerhetsmessig skikket, jf. § 8-4. Klareringsmyndigheten fatter avgjørelse om klarering. I vurderingen skal det legges vekt på forhold som er relevante for personens pålitelighet, lojalitet og dømmekraft i forbindelse med behandling av gradert informasjon og tilgang til skjermingsverdige objekter og infrastruktur. Vurderingen skal gjøres basert på en bakgrunnssjekk.

3.4 Offentleglova

Formålet med loven er å legge til rette for at offentlig virksomhet er åpen og gjennomsiktig, for slik å styrke informasjons- og ytringsfriheten, den demokratiske deltakelsen, den enkeltes rettssikkerhet, tillit til det offentlige og kontrollen fra allmenheten. Loven skal også legge til rette for viderebruk av offentlig informasjon.

Hovedregelen om innsyn følger av § 3:

> Saksdokument, journalar og liknande register for organet er opne for innsyn dersom ikkje anna følgjer av lov eller forskrift med heimel i lov. Alle kan krevje innsyn i saksdokument, journalar og liknande register til organet hos vedkommande organ.

Etter offentlighetsloven § 21 kan det «gjerast unntak frå innsyn for opplysningar når det er påkravd av nasjonale tryggingsomsyn eller forsvaret av landet». Bestemmelsen gir forvaltningen en

adgang, men ikke en plikt til å nekte innsyn i slike dokumenter. Dette innebærer at det også skal vurderes om det likevel skal gis innsyn (merinnsyn).

Unntaket etter bestemmelsen favner videre enn opplysninger som er gradert iht. sikkerhetsloven, men er likevel begrenset. Unntak fra innsyn må være nødvendig. Dette betyr at det må være en reell fare for at innsyn kan føre til betydelige skadevirkninger på nasjonens sikkerhet eller landets forsvar. Små og fjerne farer er ikke tilstrekkelig. Hvis det er svært sannsynlig at skadevirkninger vil oppstå ved offentliggjøring, kreves det ikke at skadevirkningene må være like store som i situasjoner der det er lite sannsynlig at skadevirkninger vil oppstå. Nasjonale sikkerhetshensyn omfatter opplysninger som kan skade politiets virksomhet, brannvesenet og det sivile beredskapsopplegget. Det kan også gjøres unntak for opplysninger om nøkkelpersoner i samfunnet, som deres oppholdssted og transportplaner.

3.5 Personopplysningsloven og personvernforordningen

EUs personvernforordning er gjennomført i norsk rett ved lov 15. juni 2018 nr. 38 om behandling av personopplysninger § 1. Personvernforordningen fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, samt regler om fri utveksling av personopplysninger. Det er presisert i artikkel 1 at forordningen sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger. Personvernforordningen skal leses i lys av andre menneskerettigheter.

Personvernforordningen bygger på noen grunnleggende prinsipper som må ivaretas ved behandling av person- og helseopplysninger. Dette følger av artikkel 5 og består av:

- Prinsippene om lovlighet, rettferdighet og åpenhet
- Prinsippet om formålsbegrensning
- Prinsippet om dataminimering
- Prinsippet om riktighet
- Prinsippet om lagringsbegrensninger
- Prinsippene om integritet og konfidensialitet
- Prinsippet om ansvar

Prinsippene gir uttrykk for både grunnleggende hensyn som personvernforordningen skal ivareta, og konkrete krav til hvordan personopplysninger skal behandles. Prinsippene er selvstendige regler som stiller krav til all behandling av personopplysninger. I tillegg skal de brukes i tolkningen av andre bestemmelser i forordningen og personvernbestemmelser i andre lover, herunder lover som regulerer behandling av personopplysninger i helse- og omsorgssektoren.

Enhver behandling av person- og helseopplysninger krever en eller flere behandlingsansvarlige (dataansvarlige). Behandlingsansvaret påhviler i utgangspunktet den virksomheten «som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes». Dette følger av personvernforordningen artikkel 4 nr. 7.

Videre krever behandling av «vanlige» og såkalt særlig kategorier av personopplysninger – blant annet helseopplysninger – et behandlingsgrunnlag etter personvernforordningen artikkel 6 nr. 1. Behandlingen av særlig kategorier av personopplysninger må også oppfylle vilkårene i et av unntakene i artikkel 9.

Det er et vilkår i artikkel 6 nr. 3 og artikkel 9 nr. 2 bokstav h at behandlingen også skal fastsettes i nasjonal rett eller unionsretten. Dette kalles et supplerende rettslig grunnlag.

3.6 Digitalsikkerhetsloven

Lov om digital sikkerhet (digitalsikkerhetsloven) ble vedtatt av Stortinget i desember 2023, men har ikke trådt i kraft ennå. Loven gjelder blant annet for tilbydere av samfunnsviktige tjenester etter § 6 i nærmere angitte sektorer, herunder «helse», jf. § 2 første ledd bokstav a. Etter § 6 tredje ledd kan Kongen gi forskrift om hvilke virksomheter som skal regnes som tilbydere av samfunnsviktige tjenester. Justis- og beredskapsdepartementet har i høringsnotat 11. september 2024 foreslått en bestemmelse i forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) § 1 nr. 19 til 22 at følgende tilbydere av samfunnsviktige tjenester i sektoren helse er:

- Helse- og omsorgsdepartementet med underliggende etater og foretak, som utgjør den nasjonale helseberedskapen
- tjenester som tilbys av de regionale helseforetakene
- sentrale systemer for rekvirering og utlevering av legemidler og andre medisinske produkter
- helse- og omsorgstjenester som tilbys av en kommune med
  - flere enn 50 000 innbyggere, eller
  - flere enn 20 000 brukere som er avhengige av tjenesten, og
  - tjenesten ikke kan overføres eller avlastes av andre tjenester.

Digitalsikkerhetsloven forplikter virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å opprettholde et forsvarlig sikkerhetsnivå for nettverk og informasjonssystemet gjennom å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser. Loven stiller overordnede krav til sikkerhet og varsling, og etablerer rammeverk for tilsyn med virksomhetene. Videre åpner loven for ileggelse av pålegg og eventuelt overtredelsesgebyr ved manglende oppfyllelse av pliktene. Myndighetene skal også ta imot varsler om alvorlige digitale hendelser.

Justis- og beredskapsdepartementet har som nevnt i høringsnotat 11. september 2024 foreslått forskriftsbestemmelser til digitalsikkerhetsloven. Forskriften er ikke fastsatt ennå. Blant annet er det foreslått presiseringer av kravene til digital sikkerhet, herunder at tilbyder av samfunnsviktig tjeneste etablerer og vedlikeholder et styringssystem for sikkerhet, at det utarbeides, vedlikeholdes og dokumenteres risikovurderinger og at det utarbeides plan for å håndtere risiko. Videre foreslås det bestemmelser om organisatoriske, teknologiske og fysiske sikkerhetstiltak. I forskriftsforslaget § 12 er det foreslått sikkerhetstiltak for personell. Tilbyder skal etter forslaget til første ledd iverksette nødvendige sikkerhetstiltak for ansatte, leverandører og oppdragstakere som kan få tilgang til virksomhetens nettverk og informasjonssystemer. Videre skal tilbydere iverksette tiltak for adgangskontroll, brukerautentisering og tilgangskontroll, slik at kun personell med tjenstlig behov får tilgang til tilbyders nettverk og informasjonssystemer, jf. forslaget til andre ledd. Tilbyder skal også sørge for at personell nevnt i første ledd er gjort kjent med relevante sikkerhetstiltak og at de har tilstrekkelig kompetanse innenfor sikkerhet og gis nødvendig opplæring ved behov, jf. forslaget til tredje ledd.

I Norge skal NIS1-direktivet implementeres gjennom digitalsikkerhetsloven med forskrifter, se Prop. 109 LS (2022–2023) og Innst. 78 L (2023–2024). Som nevnt har ikke loven trådt i kraft ennå, og forskriften er ikke fastsatt.

NIS2-direktivet (EU) 2022/2555 ble vedtatt i EU 14. desember 2022 og skal erstatte NIS1-direktivet (EU) 2016/1148. NIS2-direktivet er en del av en større pakke med tiltak fra EU, hvor også direktiv (EU) 2022/2557 om kritiske enheters motstandsdyktighet (CER-direktivet) inngår. Medlemsstatene skal sikre en koordinert gjennomføring av NIS2-direktivet og CER-direktivet.

NIS2-direktivet innfører mer presise bestemmelser om varsling av hendelser, herunder hva det skal varsles om og når det skal varsles. Direktivet er også nært knyttet til CER-direktivet. Formålet med CER-direktivet er å sikre leveransen av tjenester i det indre marked, som er avgjørende for å opprettholde kritiske samfunnsfunksjoner eller økonomiske aktiviteter, og å styrke motstandskraften til enheter som tilbyr slike tjenester. Spørsmål knyttet til cybersikkerhet er omhandlet i NIS2 direktivet.

NIS2-direktivet og CER-direktivet er foreløpig ikke inntatt i EØS-avtalen eller i norsk rett. Begge direktivene er vurdert EØS-relevante og akseptable.

4 Begrenset deling av store datasett

4.1 Bakgrunn

Departementet har, på bakgrunn av endringene i den sikkerhetspolitiske situasjonen og utviklingen av det tekniske mulighetsrommet, grunn til å anta at også store aggregerte datasett med anonyme eller indirekte identifiserbare helsedata er av interesse for trusselaktører og kan true samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare.

Dette kan være datasett som ikke tidligere har vært ansett å utgjøre en sikkerhetsrisiko, og kan også være offentlig tilgjengelig. Den teknologiske utviklingen og bruk av kunstig intelligens har ytterligere aktualisert problemstillingen. Se omtale av det generelle trusselbildet i punkt 2.1.

4.2 Høringsforslaget

Departementet foreslo endringer i helseregisterloven §§ 19, 19 a, 19 e og helsepersonelloven § 29, som gir hjemmel til å begrense tilgjengeliggjøring av store sett med helsedata, dersom tilgjengeliggjøringen kan ha betydning for nasjonale sikkerhetsinteresser. Forslaget gjaldt store aggregerte datasett med anonyme eller identifiserbare helsedata. Med store datasett mener departementet datasett som alene eller sammen med andre datasett, sier noe om en befolkningsgruppe.

Videre foreslo departementet at det skulle kunne kreves bakgrunnssjekk av mottaker, med mindre mottaker kan fremlegge dokumentasjon på gyldig relevant klarering etter sikkerhetsloven eller relevant bakgrunnssjekk.

Departementet presiserte i forslaget at behovet for skjerming ikke gjelder alle store datasett, og at hovedregelen fortsatt bør være at det gis tilgang.

4.3 Høringsinstansenes syn

Helsedirektoratet støtter i all hovedsak de foreslåtte tiltakene, og slutter seg til departementets beskrivelse av utfordringsbildet. Direktoratet påpeker imidlertid at de foreslåtte endringene i helsepersonelloven § 29, samt helseregisterloven §§ 19, 19 a og 19 e, ikke vil være dekkende for helserefusjonsområdet. Behov for unntak fra tilgjengeliggjøring av data av hensyn til nasjonale sikkerhetsinteresser, vil også gjelde for registre knyttet til dette området. Eksempelvis er primærkilden (KUHR) for data som ligger i Kommunalt pasient- og brukerregister og som også leverer data til Norsk pasientregister, ikke omfattet. Helsedirektorat foreslår derfor at bestemmelser om å begrense tilgjengeliggjøring av store datasett, utvides til også å omfatte opplysninger som er hjemlet i folketrygdloven.

Vurderingen av hvilke datasett som vil kunne utgjøre en trussel mot nasjonale sikkerhetsinteresser når de tilgjengeliggjøres, og til hvem, vil kunne være krevende, og forutsetter at man i noen grad ser det litt større bildet. Helsedirektoratet anser det derfor som nødvendig at det gis nærmere kriterier som er egnet til å gi virksomhetene tilstrekkelig veiledning.

Videre påpekes at forholdet mellom dispensasjonsmyndigheten og dataansvarlig (registerforvalter mv.) må være tydelig avklart. Ut fra lovforslaget synes mye av ansvaret å være lagt til dispensasjonsmyndigheten.

I forslagene i helsepersonelloven § 29 og helseregisterloven § 19 e er det stilt krav om bakgrunnssjekk av «mottaker». Etter lovforslaget er bakgrunnssjekk knyttet opp til individer hos den dataansvarlige. Helsedirektoratets gjeldende praksis er at dispensasjonsvedtak gis til dataansvarlig, dvs. virksomheten eller personen som søker om tilgang til dataene, og ikke til enkeltindivider. Direktoratet legger til grunn at dataansvarlig har ansvaret for at dataene behandles i samsvar med dispensasjonsvedtaket, herunder sørger for at enkeltpersoner som er tilknyttet prosjektet som skal bruke dataene, overholder vilkårene i vedtaket. Ved innføring av krav om bakgrunnssjekk som alternativ til å nekte dispensasjon i tilfeller der datasettene er av en slik art at det kan true nasjonale sikkerhetsinteresser, vil forslaget innebære at vedtaket må begrenses til å omfatte

navngitte prosjektmedarbeidere hos søkervirksomheten, og kreve bakgrunnssjekk av disse. Slik Helsedirektoratet forstår forslaget, vil det forutsette at dispensasjonsmyndigheten må ha god kunnskap, ikke bare om hvilke datasett som kan true nasjonale sikkerhetsinteresser dersom de tilgjengeliggjøres, men også kunnskap som setter en i stand til å gjenkjenne aktører med potensiell skadehensikt.

Folkehelseinstituttet deler departementets syn på den endrede sikkerhetssituasjonen og ambisjonene om å øke sikkerheten i helsesektoren. Folkehelseinstituttet stiller seg positive til at det foreslås forebyggende sikkerhetstiltak. Folkehelseinstituttet ser imidlertid at det kan bli krevende for organisasjonen å imøtekomme kravene i praksis. Folkehelseinstituttet innspill peker derfor på særlige utfordringer knyttet til lovkravene som foreslås.

Lovforslaget omfatter slik Folkehelseinstituttet forstår det store datasett som enten inneholder direkte (typisk samtykkebaserte studier) eller indirekte personidentifiserende helseopplysninger, men også anonyme helsedata som kan true nasjonale sikkerhetsinteresser. Folkehelseinstituttet forstår det slik at begrepet «aggregert» brukes i betydningen «samling», og ikke er relatert til aggregert anonym statistikk slik det brukes i dagligtale for å indikere at statistikken faktisk er anonym. Innenfor forskning er det sjelden at store datasett med individdata i dag kan klassifiseres som «anonyme». Et unntak er såkalte syntetiske (oppdiktede) data, som vil kunne ivareta kravene til anonymitet, men teoretisk kan disse være så like reelle data at de allikevel må anses som indirekte personidentifiserende helseopplysninger. Folkehelseinstituttet forstår at i visse tilfeller kan også anonyme data utgjøre en risiko, for eksempel at karakteristika om en befolkningsgruppe i noen tilfeller kan true nasjonale sikkerhetsinteresser. Vurderingene her er vanskelige.

Utlevering av store datasett med indirekte identifiserbare individdata er i dag utfordrende. Folkehelseinstituttet anser at enkelte av datasettene som nå etterspørres, potensielt kan representere en sikkerhetsrisiko. Det utleveres svært detaljert data, i noen tilfeller omtrent hele kvalitetsregistre koblet opp mot andre sentrale helseregistre. Dette er prosjekter hvor en regionaletisk komite har gitt tillatelse til prosjektet. Noen ganger er dette prosjekter med omfattende og til dels uklare forskningsformål, og hvor datautlevering skal oppdateres årlig. Det er svært sjelden søknader om data avslås. Denne typen søknader er imidlertid svært krevende, fordi de oppfattes å ligge i randsonen av hva lovverket tillater. Denne typen søknader er også de som er mest ressurskrevende både for Helsedataservice og registerforvalter, og som dermed medfører at gjennomsnittstiden for datautleveringer blir lang. Folkehelseinstituttet mener at det i noen tilfeller burde være større muligheter til å stanse en utlevering. Samtidig er Folkehelseinstituttet enige med departementet i at denne typen utfordringer ikke gjelder alle store datasett, og at hovedregelen fortsatt bør være tilgjengeliggjøring. Videre mener Folkehelseinstituttet at for en del store prosjekter, burde data kun utleveres til en nasjonal plattform (TSD, SAFE, Hunt Cloud) med full uttakskontroll, altså hvor uttak av individdata fra plattformen ikke er mulig.

Kripos påpeker at det må klargjøres hvem «mottaker» er. Dersom mottaker er den enkelte forsker eller lignende kan det stilles spørsmål ved effekten av en bakgrunnssjekk dersom man ikke samtidig har kontroll på hvordan vedkommende behandler opplysningene videre. For at å sikre at forslaget oppnår sitt formål må, det således også stilles krav til informasjonssikkerhet, herunder tilgangsstyring, hos vedkommende mottaker. Hvis det er konkludert med at tilgjengeliggjøring kan true nasjonale sikkerhetsinteresser antar Kripos at det sikreste er å la være å tilgjengeliggjøre opplysningene.

Helse Vest RHF støtter departementets vurderinger og forslag til lovendringer som omfatter muligheten til å begrense deling av store sett med helsedata. *Helse Bergen HF* støtter forslaget, men påpeker at i den grad anonyme data utarbeidet gjennom forskning, registre e.l. skal være gjenstand for en vurdering mht. sikkerhetspolitiske interesser før utlevering, må det være tydelige føringer for hva slags data som kan tilgjengeliggjøres. Ellers er det en risiko for at det etablerer seg ulike praksiser mellom foretakene. Uten klare føringer er det også en viss risiko for at kravene kan bidra til at Norske virksomheter blir mindre attraktive samarbeidspartnere i internasjonal forskning. Videre uttaler Helse Bergen HF:

> Dersom vurdering av om tilgjengeliggjøring av opplysninger fra registre kan true nasjonale sikkerhetsinteresser skal gjøres av medarbeidere i sykehus må det tas hensyn til at sykehusene trolig ikke har tilgang til tilstrekkelig grunnlagsinformasjon til å kunne gjøre fullgode slike vurderinger.

Oslo universitetssykehus HF er enig med departementet i at endringene i den sikkerhetspolitiske situasjonen og den teknologiske utviklingen påvirker risikobildet overfor store aggregerte datasett i

helsesektoren. Oslo universitetssykehus HF er derfor også enig med departementet i at det bør etableres lovhjemmel for å kunne begrense deling av aktuelle datasett dersom tilgjengeliggjøring kan true nasjonale sikkerhetsinteresser.

Oslo universitetssykehus HF forstår det slik at beslutninger som bygger på vurderinger av hensynet til nasjonale sikkerhetsinteresser vil måtte tas jevnlig og dynamisk, noe som også gjør det nødvendig at virksomheten har den nødvendige faglige kompetanse på løpende basis. Unntak fra deling med denne begrunnelse, må vurderes konkret for hver søknad og for statistikk etter hvert som denne produseres. Oslo universitetssykehus HF foreslår at det gis en tydelig retningslinje for rammer og eventuell støtte til opplæring. Hvis endringene gir for sterk begrensing på datadeling, så kan dette være problematisk for forskningssamarbeid.

Helse Stavanger HF påpeker at begrenset deling av store datasett vil ha stor betydning for forskningsaktiviteter og at det er krevende å se hvem som er kompetent til å gjøre denne vurderingen utenom forskerne på området selv. Dersom ansvaret og vurderingen tildeles et profesjonelt nasjonalt klareringsorgan, så kan dette lett medføre at organet ilegger begrenset deling eller blokkerer deling av datasett som følge av egen usikkerhet. Siden forskningens vesen alltid er å strekke seg inn i områder hvor vi foreløpig har lite eller begrenset innsikt, så vil dette i praksis kunne skape unødvendige hindringer for effektiv utvikling av ny og viktig kunnskap.

Sørlandet sykehus HF etterspør en grundigere diskusjon for hvordan dette kan påvirke forskningen og medisinsk utvikling. Helseforetaket påpeker at sektoren er avhengig av tilgang til store helsedata for å drive frem medisinsk innovasjon, og restriksjoner kan potensielt hemme viktige forskningsprosjekter. Det påpekes videre at departementet ikke er konkrete nok, når det kommer til hvordan dette skal balanseres mot nasjonale sikkerhetsinteresser.

Vestre Viken HF påpeker at det for å ivareta kravet til klar lovhjemmel i EØS-retten, bør det framgå klart at sett med helseopplysninger som ikke i seg selv kan true nasjonale sikkerhetsinteresser kan holdes tilbake der det foreligger klare holdepunkter for at opplysningene vil sammenstilles med andre datasett.

St. Olavs hospital HF presiserer at det stiller seg bak den felles høringsuttalelsen for helseforetakene i regionen, som er sendt fra Helse Midt-Norge RHF. St. Olavs hospital HF ønsker imidlertid å påpeke noen særlige forhold knyttet til blant annet utdanning. I tillegg påpekes viktigheten av å være oppmerksom på at «mottaker» i mange tilfeller ikke vil være en enkeltperson, men en eller flere personer som er ansatt i en eller flere virksomheter. De som får opplysningene utlevert vil gjerne behandle disse i en eller flere løsninger som igjen gjerne driftes og forvaltes av andre virksomheter med eget personell. I forlengelsen av dette kunne det med fordel vært sagt noe mer om hvordan formuleringen «av mottaker» skal forstås og praktiseres.

Helseforetaket påpeker videre at det knyttet til forslaget til helseregisterloven § 19 a, er lagt til den dataansvarlige å vurdere hvorvidt tilgjengeliggjøring av datasett vil utgjøre en trussel mot nasjonale sikkerhetsinteresser. Dette er vurderinger som det kan være vanskelig for den dataansvarlige å gjøre, og et sentralt kontaktpunkt eller organ som kan veilede dataansvarlig, eller eventuelt foreta vurderingen på vegne av dataansvarlig, bør vurderes. Et slikt organ vil for øvrig kunne bidra til en ensartet praksis i sektoren.

Regionale komiteer for medisinsk og helsefaglig forskningsetikk støtter i all hovedsak forslaget om å lovfeste adgangen til å begrense tilgang på aggregerte data og indirekte identifiserbare helseopplysninger. Det er viktig at risikovurderingens innhold og kriteriene for å beslutte begrenset deling av store datasett utdypes, og beskrives i forskrifter og eventuelt i rundskriv. Forslaget kan imidlertid føre til en innskrenkning i dagens praksis med deling av data, og at det blir et mindre handlingsrom for deling av data. Dette vil kunne være i konflikt med prinsippet om åpne tilgjengelige datasett i forbindelse med publisering av forskningsresultater og i forbindelse med forskningssamarbeid med utenlandske aktører. På den andre siden er de norske registrene og bruken av disse avhengig av befolkningens tillit til trygg oppbevaring og bruk. Det taler for økt forsiktighet rundt hvem som skal ha tilgang til opplysningene, som et forebyggende tiltak mot eventuelt misbruk av innsamlede helseopplysninger og store aggregerte datasett.

Det bør fremgå tydelig om Regionale komiteer for medisinsk og helsefaglig forskningsetikk og andre offentlige organer er gitt kompetanse til å treffe vedtak om begrensning i deling av datasett. Regionale komiteer for medisinsk og helsefaglig forskningsetikk legger i denne sammenheng til grunn at beslutninger om begrensning av tilgang på datasett gjort av offentlige organer har status som enkeltvedtak, og følger allerede fastsatte klagesaksordninger.

UiT Norges Arktiske Universitet er enig i at det er behov for å kunne sikre et forsvarlig sikker-

hetsnivå for informasjon og systemer som ikke faller inn under sikkerhetsloven. Høringsnotatet inneholder ingen vurdering av i hvilken grad de foreslåtte endringene påvirker balansen mellom hensynet til konfidensialitet og hensynet til tilgjengelighet. Det er ikke vurdert hvorvidt de foreslåtte begrensningene i deling av store datasett kan påvirke helseforskning og forskningssamarbeid. Helseforskning er et område med mye internasjonalt samarbeid, forskning på tvers av landegrenser og forskning med store datasett. Ofte vil større internasjonale kohorter være en forutsetning for forskningen.

> Slik lovforslaget foreligger i dag ser vi også utfordringer med de faktiske vurderingene av hvilke datasett som vil kunne ha betydning for nasjonale sikkerhetsinteresser. Dette er krevende vurderinger, som krever en kompetanse som UiT ikke har per i dag. Etter vår vurdering, kan de foreslåtte endringene i tilgjengeliggjøring av data komme i konflikt med lovgivers tidligere intensjoner om et oversiktlig og harmonisert regelverk, som skulle sikre lik praksis.

Universitetet i Oslo anerkjenner viktigheten av å ivareta nasjonal sikkerhet og beskytte sensitiv informasjon. Samtidig er det avgjørende at sikkerhetstiltak, blir balansert på en måte som ikke undergraver den akademiske friheten og muligheten til fri forskning. Ved å innskrenke mulighetene for internasjonalt forskningssamarbeid og fri forskning kan man avskrekke, kjøle ned og i verste fall forhindre forskning på viktige områder.

Norges teknisk-naturvitenskapelige universitet mener forslaget ikke skiller godt nok mellom anonymiserte og avidentifiserte data. Bruk av anonymiserte data er vanlig i forskning og en viktig del av åpen vitenskap og deling av data. Disse data er ikke sensitive eller omfattet av personvernforordningen, og bør ikke omfattes av krav om bakgrunnssjekk. Avidentifiserte data er underlagt strenge restriksjoner gjennom personvernlovgivningen og helseforskningsloven. Norges teknisk-naturvitenskapelige universitet er bekymret for at forslaget knyttet til begrenset deling av datasett, kan føre til utfordringer for Norge som kunnskapsnasjon og for den enkelte institusjonen, gjennom at noe helsedata blir vanskeligere tilgjengelig eller ikke vil være tilgjengelig i det hele tatt for forskningsformål. Norges teknisk-naturvitenskapelige universitet mener forslaget ikke er tilstrekkelig tilpasset forskningens egenart og kunnskapsinstitusjonenes samfunnsoppdrag. Departementet må sikre at de endringene som innføres er praktisk gjennomførbare inkludert håndterbare for den enkelte organisasjonen og at de ikke går på bekostning av å utvikle Norge som en ledende kunnskaps- og forskningsnasjon. Norges teknisk-naturvitenskapelige universitet anbefaler å følge lovgiving og retningslinjer på EU-nivå slik at norsk forskning fortsatt vil være relevant i internasjonal sammenheng.

Universitetet i Bergen påpeker at dersom ny lovgiving begrenser mulighetene for Norge å delta i større og langvarige nasjonale og internasjonale forsknings- og utviklingssamarbeid hvor store sett med helsedata inngår, vil dette kunne føre til at Norge blir isolert fra resten av Europa (og verden for øvrig) på disse områdene.

Universitetet i Bergen mener videre det er behov for en begrepsavklaring av «mottaker» i foreslåtte lovtekst. Dersom det blir behov for bakgrunnssjekk ved utlevering av store datasett med helseopplysninger, står det formulert at dette skal gjøres av mottaker. Dersom en forsker skal ha utlevert et stort sett med helsedata og bli gjenstand for bakgrunnssjekk, vil det også fra et sikkerhetsmessig ståsted være behov for å ha kontroll med resten av kjeden som eventuelt vil kunne få tilgang til disse opplysningene. Dette vil potensielt gjelde intern IT-avdeling som gjerne drifter plattformer for lagring og prosessering av data, eventuelle leverandører som får tilgang og eventuelle forskingssamarbeidspartnere i det aktuelle forskningsprosjektet som ber om utlevering av disse datasettene.

Universitetet i Bergen reagerer også på at forslaget åpner for å begrense tilgang også til datasett som er anonymiserte. Dette kan gjøre det vanskeligere for studenter og forskere å bruke registerdata, biobanker og helseundersøkelser i oppgaver og forskningsprosjekter.

ELIXIR-Noreg påpeker at åpenhet og kunnskapsdeling er en forutsetning for forskningen. Med åpen forskning blir måten forskningen blir utført, delt og vurdert på endret, og potensialet for høy kvalitet og verdiskaping i samfunnet øker. Departementets forslag vil kunne blokkere deler av denne åpne forskningen ved at det blir vanskeligere å dele data. I tillegg til deling av data, omhandler politikken rundt åpen forskning også åpen deling av programvare og analyseverktøy. Mye av dette er laget av individuelle forskere/utviklere som kommer fra ulike deler av verden.

Videre uttaler ELIXIR-Noreg at forslagets definisjon av store datasett, er en definisjon som kan omfatte det aller meste av biomedisinsk forskning på mer enn noen få personer. Det er allerede i dag krevende å bruke sensitive data på grunn av

eksisterende lovgivning, både nasjonal og europeisk, sammen med lokale tolkninger av regelverket. Med den sterke utviklingen av presisjonsmedisin vil grensen mellom forskning og behandling i stadig større grad bli utydelig, med stadig økende sekundærbruk av data. Videre vil også bruk av KI bli vanskeliggjort med denne typen lovregulering, fordi sammenstilling av data er en nødvendig forutsetning for læringsprosesser ved kunstig intelligens. ELIXIR-Noreg mener det er nødvendig å tydeligere definere grensene for hva som utgjør slike sensitive datasett, og beskrive mer i detalj hvilke typer data som vil utløse de foreslåtte tiltakene.

Dersom ny lovgivning begrenser Norges mulighet til å delta på grunn av redusert tilgang til å dele data, mener ELIXIR-Noreg at dette kan true norsk deltakelse i de internasjonale samarbeidene og føre til at Norge blir isolert fra resten av Europa (og verden ellers) på disse områdene. Det er derfor viktig at ny lovgivning bare fører til begrensninger i datadeling når dette er absolutt nødvendig.

Norsk Forening for Farmakoepidemiologi mener at tilgjengeliggjøring av store aggregerte datasett med anonyme eller indirekte identifiserbare helsedata, per i dag allerede er begrenset til nødvendige opplysninger. Det er veldig uklart i forslaget hvilke kriterier som skal ivaretas for å vurdere hvilke data/datasett som kan ha betydning for nasjonale sikkerhetsinteresser. Norsk Forening for Farmakoepidemiologi mener det er sentralt å veie nøye risiko for trussel ved å ha tilgang til store datasett med kun de nødvendige opplysninger, mot nytten disse dataene har for helse i hele den norske befolkningen og andre steder i verden. Norsk Forening for Farmakoepidemiologi mener at nytten veier ut risiko i de fleste tilfeller som gjelder forskning. Norsk Forening for Farmakoepidemiologi mener det er sentralt at det i forskrift beskrives mer detaljert hvordan vurderingen skal ivaretas og gjennomføres.

Norsk Radiografforbund mener de foreslåtte endringer vil kunne begrense deling av enkelte store sett med helsedata, av hensyn til nasjonale sikkerhetsinteresser. Dette kan nok være nødvendig som forebyggende tiltak, men advarer mot endringer som vanskeliggjør tilgang på gode data, godt forskningsarbeid og samarbeid på tvers av foretak og nivåer i helsetjenesten. Tilgang til store datasett vil være av stor betydning for tilpasning og bruk av teknologi bygd på kunstig intelligens for norske forhold. Endringer bør derfor ikke legge unødvendige begrensninger for bruk av nasjonale data for utvikling og implementering av slik teknologi.

Advokatforeningen støtter departementets forslag om begrenset deling av store datasett der dette kan ha betydning for nasjonal sikkerhet, men understreker viktigheten av at en slik hjemmel ikke legger større begrensinger på blant annet forskning enn det som er absolutt nødvendig. Norge har gjennomgående små forskningsmiljøer og internasjonalt samarbeid er nødvendig. Det er derfor viktig at kriteriene i større grad utdypes og beskrives i forskriftsarbeidet og eventuelt i rundskriv. Videre mener Advokatforeningen at ansvarlig departement bør gjøre en jevnlig evaluering av om begrensningene som praktiseres fungerer etter hensikten eller ikke.

Mental Helse Ungdom påpeker at forslaget om å begrense delingen av store datasett for å beskytte nasjonale sikkerhetsinteresser er forståelig. Samtidig er det viktig at slik begrensning ikke hindrer forskning og utvikling som kan bidra til bedre helse- og omsorgstjenester. Enhver restriksjon må balanseres mot behovet for å fremme åpenhet og innovasjon i helseforskningen, særlig når det gjelder anonymiserte eller aggregerte data som kan være avgjørende for medisinsk fremgang.

Tekna mener det i proposisjonen må omtales hvem som skal vurdere hvilke innstramninger som skal gjøres, og hvem som skal gis tilgang på data til forskningsformål. Tekna har fått tilbakemeldinger om at det vil være krevende for den enkelte virksomhet å foreta vurderinger av hvilke datasett som har betydning for nasjonale sikkerhetsinteresser. De er ikke rigget for å kunne gjøre slik risiko- og sårbarhetsvurderinger.

Spekter støtter forslaget i høringen om begrensninger i tilgang til store datasett. Det vil imidlertid være krevende for den enkelte virksomhet å foreta den faktiske vurderingen av hvilke datasett som vil kunne ha betydning for nasjonale sikkerhetsinteresser. Det er derfor viktig at kriteriene utdypes og beskrives i forskriftsarbeidet og rundskriv.

Legemiddelindustrien mener det bør gjøres en grundigere vurdering av hvordan begrensinger for offentliggjøring av anonym statistikk vil kunne påvirke bruk av helsedata til forskning, helseøkonomiske analyser og metodevurderinger (HTA), samt muligheter for publisering av forskingsresultater. Legemiddelindustrien opplever at forslaget har stort potensiale til å påvirke tilgangen til og bruken av helsedata negativt, ved å gjøre det mer komplisert og tidskrevende å få tilgang. Legemiddelindustrien mener det bør gjøres en grundigere konsekvensutredning mht. hvordan endringene vil påvirke alle typer dataansvarlige som vurderer

søknader om tilgang til helsedata og alle typer mottakere av helsedata til sekundærbruk.

Legemiddelindustrien mener et legemiddelfirma eller en leverandør av forskningstjenester som søker tilgang til datasett med helseopplysninger for forskningsformål dermed vil kunne omfattes av kravet om bakgrunnssjekk. Videre er det ikke definert i lovteksten hva en «mottaker» er. I dag vil en mottaker i praksis kunne være en enkeltperson eller en organisasjon. Bakgrunnssjekk av en organisasjon er imidlertid ikke omtalt i lovforslaget. Det bør derfor utypes hva en mottaker er enten i lovteksten eller i forarbeidet.

Legemiddelindustrien mener det er nødvendig med en videre konsekvensutredning sammen med klargjøring av vilkårene for bakgrunnssjekk for tilgang til helsedata for sekundærbruk.

Fürst Medisinsk Laboratorium mener det er mangler ved beskrivelsen av hva som menes med deling av store helsedatasett og hvorvidt et datasett har betydning for «nasjonale sikkerhetsinteresser». Foruten å berøre risikomomenter for forskjellig praksis, samt kompetanse- og ressursproblemer nevnt i tilknytning bakgrunnssjekk, etterlyser Fürst Medisinsk Laboratorium en tydeligere avveining av den betydning dette kan få for den løpende forskning på helseområdet.

4.4 Departementets vurderinger

4.4.1 Hovedinnhold

Departementet foreslår endringer i helsepersonelloven og helseregisterloven, som presiserer at det ikke skal gis unntak fra taushetsplikten for tilgjengeliggjøring av helseopplysninger som kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare. Videre foreslås et unntak fra plikten til å utarbeide statistikk etter helseregisterloven § 19 når anonyme datasett kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare.

I høringsnotatet foreslo departementet at krav om bakgrunnssjekk av personell hos mottaker, kan være et alternativ til å nekte tilgjengeliggjøring. Departementet vil på bakgrunn av innspill i høringen, ikke foreslå at bakgrunnssjekk kan være et alternativ.

Forskning på og analyse av helsedata er svært viktig for å vurdere hvordan det står til med helsen i den norske befolkningen, hvordan pasientsikkerheten er, og om kvaliteten på tjenestene er god nok. Helsedata brukes både til å administrere og yte helsehjelp (primærbruk) og til å holde oversikt over helsetilstanden i befolkningen, over aktivitet og ressursbruk i helse- og omsorgstjenesten, til å forstå hva som påvirker helsen i befolkningen, til å planlegge framtidens behov for helsetjeneste og til å utvikle kunnskap om forebygging, diagnostikk, behandling og effekter av behandlingen (sekundærbruk).

Tilgang til helsedata er nødvendig for legemiddelutvikling og i utvikling av produkter og løsninger for helse- og omsorgstjenesten og bidrar samtidig til innovasjon, kommersialisering og økt verdiskaping. God forskning og analyse forutsetter at helsedata er tilgjengelig for disse formålene.

I Norge har vi stor grad av åpenhet, med offentlig deling og publisering av store datasett med aggregerte (anonyme) helsedata. Dette er en utviklingsretning som i stor grad også følger av våre EØS-rettslige forpliktelser, bl.a. gjennom datadelingsregelverket. Personvernforordningen kommer ikke til anvendelse på anonyme data. Departementet presiserer at sikkerhetsloven vil kunne komme til anvendelse for datasett med aggregerte (anonyme) helsedata. Dette er dersom datasettet vurderes som skjermingsverdig, altså informasjon som kan skade nasjonale sikkerhetsinteresser, dersom informasjonen blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig, jf. sikkerhetsloven § 5-1.

På bakgrunn av endringer i den sikkerhetspolitiske situasjonen og risikobildet, er det nødvendig med en unntaksbestemmelse som gir mulighet for også å unnta ikke-personidentifiserbare helsedata, som ikke er omfattet av sikkerhetslovens bestemmelser, fra deling.

4.4.2 Formål og virkeområde

Formålet med forslaget er å ha et rettslig grunnlag for å kunne unnlate å dele datasett med helsedata, som kan ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Dette gjelder også aggregerte (anonyme) data.

Departementet foreslår endringer i helseregisterloven §§ 19, 19 a, 19 b, 19 e og helsepersonelloven § 29. Dette betyr at forslagene er begrenset av virkeområdet til disse lovene. Se punkt 3.2.

Departementet har merket seg Helsedirektoratets forslag om også å hjemle unntaket i folketrygdloven, slik at det også vil være dekkende for informasjonskilder knyttet til helserefusjoner. Et slikt forslag har ikke vært på høring og departementet finner det i denne omgang ikke mulig å følge opp.

«Helsedata» er et vidt begrep som kan omfatte alle typer opplysninger om helse, enten de frembringes i helse- og omsorgstjenestene, gjennom de store befolkningsundersøkelsene eller på andre måter. Begrepet helsedata favner videre enn begrepet helseopplysninger slik det er definert i personvernforordningen. Helsedata kan være anonyme, direkte identifiserbare eller indirekte identifiserbare.

Folkehelseinstituttet påpeker at departementet i høringsnotatet har benyttet begrepet «aggregert» i betydningen «samling», og ikke relatert til aggregert anonym statistikk slik det vanligvis brukes for å indikere at statistikken faktisk er anonym. Innenfor forskning er det sjelden at store datasett med individdata kan klassifiseres som «anonyme». Departementet vil presisere at begrepet «aggregert» i forslaget her er relatert til aggregert anonym statistikk.

Terminologien «nasjonale sikkerhetsinteresser» er i høringsnotatet benyttet på en måte som favner noe videre enn legaldefinisjonen i sikkerhetsloven § 1-5. Informasjonssystemet og informasjonen det lovforslaget gjelder, har et skadepotensiale som er løsere eller mer indirekte knyttet til nasjonale sikkerhetsinteresser, slik at det ikke direkte kan sies å falle inn under sikkerhetslovens regler om beskyttelse av informasjon. Skadepotensialet vil være noe mindre enn ved kompromittering av objekter som er skjermet etter sikkerhetsloven, men samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare vil likevel rammes. Flere høringsinstanser mener derfor det er uheldig å bruke begrepene fra sikkerhetsloven. Basert på innspill i høringsprosessen, benytter departementet i forslaget her terminologien «som kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare», ikke «nasjonale sikkerhetsinteresser».

Departementet vil presisere at forslaget ikke gjelder helsedata med et skadepotensiale som faller inn under sikkerhetslovens regler om beskyttelse av informasjon. Dette skal fremdeles reguleres av sikkerhetsloven.

4.4.3 «Offentlig sikkerhet» og EØS-avtalen

Unntak for deling av sett med helsedata som kan true samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare (samfunnssikkerhet), er etter departementets oppfatning i samsvar med EØS-avtalen. EUs forordninger og direktiver om datadeling, har unntak for deling som er berettiget av hensyn til offentlig sikkerhet («public security»). Dette gjelder bl.a. EUs forordning (EU) 2018/1807 om en ramme for fri flyt av andre opplysninger enn personopplysninger i EU, datastyringsforordningen (Data Governance Act (EU) 2022/868) og forslag til dataforordning (Data Act). De aktuelle EU-rettsaktene er, eller vil bli implementert i annet regelverk.

Etter det departementet forstår, legger nevnte EU-regelverk til grunn forståelsen av «offentlig sikkerhet», slik det er definert i EU-retten og særlig traktaten om Den europeiske unions virkemåte (TFEU) artikkel 52. Begrepet «offentlig sikkerhet» dekker både den interne og den eksterne sikkerheten i en medlemsstat, samt spørsmål om samfunnssikkerhet. «Offentlig sikkerhet» forutsetter at det foreligger en reell og tilstrekkelig alvorlig trussel som påvirker en av de grunnleggende samfunnsinteressene, for eksempel en trussel mot institusjoners og grunnleggende offentlige tjenesters virkemåte og befolkningens overlevelse, samt risikoen for en alvorlig forstyrrelse av internasjonale relasjoner eller nasjoners fredelige sameksistens, eller en trussel mot militære interesser.

I Meld. St. 10 (2016–2017) *Risiko i et trygt samfunn – Samfunnssikkerhet,* brukes følgende definisjon av begrepet samfunnssikkerhet:

> Samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger.

Samfunnssikkerhetsbegrepet brukes bredt. Det dekker beskyttelse mot alle alvorlige situasjoner i hele spekteret av utfordringer, fra ulykker i fredstid, til situasjoner som truer rikets sikkerhet og selvstendighet.

Departementet oppfatter at samfunnssikkerhet slik det er benyttet i denne lovproposisjonen, er omfattet av begrepet «offentlig sikkerhet» i EU-regelverket.

4.4.4 Samfunnssikkerhet

I helseretten er det uklart i hvilken grad det er adgang til å unnta deling av datasett med helseinformasjon, med den begrunnelse at det kan ha betydning for samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare. Dette gjelder blant annet opplysnin-

ger som er unntatt fra taushetsplikten på grunnlag av samtykke fra den opplysningene gjelder. Departementet mener at det er nødvendig å ha mulighet til å kunne begrense tilgang til denne type datasett og at dette bør fremgå av helseregisterloven og helsepersonelloven.

Departementet vil presisere at den klare hovedregelen fortsatt bør være tilgjengeliggjøring, herunder til forskning og analyse, når de øvrige vilkårene er oppfylt.

Departementet merker seg at det ikke er enighet om forslaget blant høringsinstansene. UiT Norges Arktiske Universitet, Norges teknisk-naturvitenskapelige universitet og Universitetet i Bergen mener forslaget kan påvirke helseforskning og forskningssamarbeid negativt. Helseforskning er et område med mye internasjonalt samarbeid, forskning på tvers av landegrenser og forskning med store datasett. Departementet er godt kjent med viktigheten av at data deles og at større internasjonale kohorter ofte vil være en forutsetning for forskningen. Det er likevel slik at samfunnets behov for verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare, også må vektes høyt.

Norges teknisk-naturvitenskapelige universitet m.fl. uttaler at bruk av anonymiserte data er vanlig i forskning, og en viktig del av åpen vitenskap og deling av data. Disse påpeker at anonymiserte data ikke er sensitive eller omfattet av personvernforordningen, og ikke bør omfattes. Til dette vil departementet bemerke at endringene i den sikkerhetspolitiske situasjonen og det tekniske mulighetsrommet, har endret risikobildet knyttet til tilgjengeliggjøring av store aggregerte datasett. Det er grunn til å tro at tilgjengeliggjøring av store datasett med aggregert anonym helseinformasjon, også kan ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Ifølge NSMs trusselvurdering må vi regne med at skjerpet risikobilde er en vedvarende situasjon.

Departementet har imidlertid justert noe på forslaget til endringer i helseregisterloven § 19 om utarbeidelse av statistikk. Departementet mener endringen i første omgang bør formuleres som en adgang for dataansvarlig til å nekte utarbeidelse av statistikk, i stedet for en plikt. Anonyme datasett (statistikk) vil som det klare utgangspunkt ikke utgjøre en trussel mot samfunnssikkerheten, men tvert imot være et gode for samfunnet gjennom mer tilgjengelig kunnskap. Den dataansvarlige bør derfor ha frihet til å innrette praksis slik at det bare er de åpenbare tilfellene som det er nødvendig å vurdere opp mot hensynet til samfunnssikkerhet. Departementet vil følge med på praksis, og eventuelt vurdere om det senere bør innføres en plikt til å avslå søknader om statistikk når samfunnssikkerheten er truet.

Etter offentlighetsloven § 21 kan det «gjerast unntak frå innsyn for opplysningar når det er påkravd av nasjonale tryggingsomsyn eller forsvaret av landet», se punkt 3.5. Departementet mener unntaket etter offentlighetsloven er viktig. I forbindelse med tilgjengeliggjøring av helsedata etter helsepersonelloven- og helseregisterlovens bestemmelser fremstår imidlertid ikke unntaket som tilstrekkelig for å ivareta samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare med et sammensatt trussel- og utfordringsbilde. Departementet mener det er nødvendig at et unntak har samme virkeområde som helsepersonelloven og helseregisterloven, og ikke er begrenset til virksomheter som er omfattet av offentlighetslovens virkeområde.

4.4.5 Konkret vurdering

Kompetanse og kunnskap om risiko, trusler, sårbarheter og effektive mottiltak er en forutsetning for å kunne beskytte våre verdier mot uønskede hendelser. Det er derfor viktig at de aktuelle virksomhetene setter seg i stand til å kunne identifisere denne type utfordringer og fatte beslutninger om begrenset deling. I samsvar med forholdsmessighetsprinsippet bør unntak som er begrunnet ut fra hensynet til samfunnssikkerhet, være egnet til å sikre at det fastsatte målet nås, og ikke gå lenger enn det som er nødvendig for å nå dette målet.

Folkehelseinstituttet påpeker at det er vanskelig å vurdere hva som bør få «varslingslampene» til å lyse. Folkehelseinstituttet mener at særlige sensitive variabler i seg selv kan utgjøre en risiko, men det kan også være omfanget av data, eller kombinasjonen. Disse vurderingene må skje før tilgang gis. For vedtaksmyndighetene (bl.a. Helsedataservice ved Folkehelseinstituttet) ville det måtte skje som ledd i saksbehandlingen, og vurderinger etter de foreslåtte endringene i §§ 19 a, 19 b og 19 e vil i enkelte tilfeller kunne bli tidkrevende.

Norsk Forening for Farmakoepidemiologi mener det er sentralt å veie risiko ved å ha tilgang til store datasett, mot nytte disse dataene har for helse i hele den norske befolkningen og andre steder i verden. Foreningen mener at nytten veier

opp for risikoen i de fleste tilfeller som gjelder forskning. Departementet er enig i at nytten av forskning er meget høy, og vil påpeke at behovet for skjerming ikke gjelder alle store datasett og at den klare hovedregelen fortsatt skal være tilgjengeliggjøring.

Unntak fra deling med begrunnelse at slik deling antas å ville ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare, må vurderes konkret. Departementet mener sikkerhetslovens metodikk for hvordan nasjonale verdier skal kartlegges, også vil kunne benyttes for å identifisere datasett det kan være aktuelt å underlegge begrenset deling. Metoden er egnet for å gi god oversikt over verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for kritiske samfunnsfunksjoner. Samtidig må en oversikt over verdier ses i sammenheng med trussel- og risikobildet, for å forstå egne sårbarheter og for å kunne ivareta egen sikkerhet.

Den faktiske vurderingen av hvilke datasett som vil kunne ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare, vil kunne være krevende for de enkelte virksomhetene å foreta. Det er i utgangspunktet heller ikke vurderinger som virksomhetene er «rigget» for å foreta. Departementet har derfor forståelse for Helsedirektoratet og Folkehelseinstituttets m.fl. anførsel om at vurderingen av hvilke datasett som vil kunne utgjøre en trussel ved tilgjengeliggjøring, og til hvem, vil kunne være krevende, og forutsetter at man i noen grad ser det litt større bildet.

Departementet antar imidlertid at det i de fleste saker om tilgjengeliggjøring ikke er nødvendig med en særskilt vurdering av hensynet til samfunnssikkerheten. Behovet for slike vurderinger vil trolig være forbeholdt noen få saker med tilgang til store datasett.

Det er også en forutsetning at det er tett dialog mellom virksomhetene som skal forestå disse vurderingene og de nasjonale instansene med særskilt kompetanse på samfunnssikkerhet. Dette vil kunne bidra til at de ulike virksomhetene i størst mulig grad tolker like saker likt og at tilgang til datasettene ikke blir begrenset i for stor grad.

5 Forslag til endringer i pasientjournalloven § 22 og helseregisterloven § 21

5.1 Bakgrunn

Pasientjournalloven § 22 og helseregisterloven § 21 regulerer informasjonssikkerhet ved behandling av personopplysninger. Paragrafenes virkeområde er begrenset gjennom henvisning til personvernforordningen artikkel 32. Dette ivaretar ikke andre sikkerhetsutfordringer som er aktualisert etter endringene i den sikkerhetspolitiske situasjonen, se omtale i punkt 2.1.

5.2 Høringsforslaget

Departementet foreslo å endre pasientjournalloven § 22 og helseregisterloven § 21, slik at det tydelig fremgår at bestemmelsene også dekker andre sikkerhetsutfordringer enn det som er knyttet til personvernforordningen. Det ble foreslått at det også inntas en plikt til å gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenester etter disse to lovene. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, ble det foreslått at det blant annet skal ses hen til den teknologiske utviklingen og nasjonale sikkerhetsinteresser. Departementet foreslo derfor at lovbestemmelsens overskrift endres til «Tekniske og organisatoriske sikkerhetstiltak». Departementet foreslo videre at det i pasientjournalloven § 22 og helseregisterloven § 21 presiseres at det i forskrift kan fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.

I tilknytning til forslaget om bakgrunnssjekk av personell med privilegerte tilganger til IKT-systemene, foreslo departementet krav om å legge fram uttømmende og utvidet politiattest.

5.3 Høringsinstansenes syn

Helsedirektoratet støtter i all hovedsak de foreslåtte tiltakene, og slutter seg til departementets beskrivelse av utfordringsbildet. Direktoratets vurdering er at det er viktig å iverksette tiltak for å redusere sårbarheter og øke motstandskraften mot trusselaktører. Når det gjelder uttømmende og utvidet politiattest, mener Helsedirektoratet hjemmel for å få tilgjengeliggjort opplysningene direkte fra politiets registre kunne være mer hensiktsmessig, eksempelvis på tilsvarende måte som etter klareringsforskriften § 8 med hensyn til personkontrollen som utføres i forbindelse med en sikkerhetsklarering. I sikkerhetsloven § 8-5 niende ledd er det fastsatt at «Behandlingsansvarlige for relevante registre skal legge til rette for digitalisert overføring av registeropplysninger til sikkerhetsmyndigheten». Etter direktoratets oppfatning vil de aktuelle opplysningene da kunne innhentes på en måte som bedre ivaretar prinsippet om dataminimering, fremfor at den enkelte selv innhenter og videreformidler politiattest.

Også *Helse Vest RHF, Vestre Viken HF, Fürst Medisinsk Laboratorium* og *Visma Flyt AS* støtter i all hovedsak departementets vurderinger og forslag til lovendringer. *Oslo universitetssykehus HF* støtter vurderingene av de sikkerhetsmessige utfordringene og er grunnleggende positiv til de foreslåtte lovendringer.

Datatilsynet mener endringene medfører at bestemmelsene er bedre tilpasset innholdet i personvernforordningen artikkel 32. Artikkel 32 omhandler personopplysningssikkerhet, som er noe mer enn kun informasjonssikkerhet, jf. den nåværende overskriften i pasientjournalloven § 22 og helseregisterloven § 21. Speilingen av ordlyden i artikkel 32, så vel som en konkretisering av lovkravene, ser Datatilsynet som positivt. Datatilsynet ser også positivt på en forskriftshjemmel der sikkerhetstiltakene kan utdypes og konkretiseres ytterligere.

Helse Sør-Øst RHF anbefaler at endringer i helseregisterloven § 21 og pasientjournalloven § 22 avventes til CER-direktivet og NIS/NIS II er gjennomført i norsk rett. Helse Sør-Øst RHF mener dagens regelverk fungerer godt, og forslagene gir fare for at oppmerksomheten vris fra områdene med størst risiko til dem som omtales i bestem-

melsen. Videre påpekes at helseforetakene behandler en rekke opplysninger som ikke er knyttet til personer, for eksempel opplysninger om medisiner, bygg o.a. Informasjonssikkerhetsbrudd for slike opplysninger vil kunne ha betydelige konsekvenser. Endring av sikkerhetskrav for annet enn personopplysninger (herunder anonymiserte datasett) bør etter Helse Sør-Øst RHF syn knyttes til annet regelverk enn pasientjournalloven/helseregisterloven.

Politidirektoratet uttaler at det for politiet vil være kostnader knyttet til utstedelse av politiattester og eventuell annen utlevering av opplysninger. *Politiets enhet for vandelskontroll og politiattester* (vandelsenheten) opplever at kommuner, helseforetak mv. forsøker å innhente politiattest av personer der det etter det aktuelle hjemmelsgrunnlaget ikke er hjemmel til dette. For eksempel av personell som ikke yter spesialisthelsetjenester eller tannhelsetjenester til barn jf. helsepersonelloven § 20 a. Det bør derfor være klart presisert i loven eller forskriften når kravet faktisk kan inntre. Videre uttaler Vandelsenheten at det kommer stadig flere lovendringer som gir nye hjemler for krav om politiattest, eller som utvider personkretsen i eksisterende hjemler. I sum kan dette medføre en større belastning for enheten. En saksbehandler ved vandelsenheten behandler i gjennomsnitt ca. 20 000 politiattester per år.

Advokatforeningen støtter forslaget om å lovfeste plikten til å utføre tekniske og organisatoriske sikkerhetstiltak i pasientjournalloven mv., herunder henvisningen til nasjonale sikkerhetsinteresser.

5.4 Departementets vurderinger

Departementet mener den teknologiske utviklingen gjør det nødvendig med endringer i bestemmelsene om informasjonssikkerhet i pasientjournalloven og helseregisterloven. Truslene mot viktige samfunnsfunksjoner er i stor grad av sofistikerte angripere med høy evne og kapasitet. Aktørene kan være statlige eller statsfinansierte grupper som bryter seg inn i IKT-systemer for å påføre skade eller hente informasjon som kan benyttes for å nå økonomiske, politiske eller militære mål. Statlige aktører kan være andre staters etterretnings- og sikkerhetstjenester, inkludert aktører engasjert av disse. Motivene kan i ytterste konsekvens være forberedelser til fremtidige sabotasjeoperasjoner, terrorisme eller krig. Utsatte grupper er leverandører, utviklere og operatører knyttet til kritisk infrastruktur, for eksempel i forbindelse med plassering av digitale bakdører og utro tjenere.

Høringsinstansene deler i hovedsak departementets syn på risikobildet og sikkerhetsutfordringene helse- og omsorgstjenesten står overfor. Departementet oppfatter at det også er bred enighet om behovet for økt bevissthet om oppdaterte og effektive sikkerhetstiltak. Departementet merker seg imidlertid at få av høringsinstansene uttaler seg konkret om denne delen av forslaget.

Etter gjeldende rett regulerer pasientjournalloven § 22 og helseregisterloven § 21 informasjonssikkerhet ved behandling av personopplysninger. Bestemmelsene er begrenset til å gjelde ved behandling av personopplysninger gjennom henvisning til personvernforordningen artikkel 32. Etter departementets syn ivaretar dette ikke andre sikkerhetsutfordringer knyttet til ivaretakelse av kritiske samfunnsfunksjoner og helse- og omsorgstjenestens evne til å ivareta sine oppgaver.

Departementet foreslår på denne bakgrunn at bestemmelsenes ordlyd endres slik at det tydelig fremgår at bestemmelsene også dekker andre sikkerhetsutfordringer. Det foreslås en plikt til å gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenester etter disse to lovene. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, kritiske samfunnsfunksjoner, helse- og omsorgstjenestens evne til å ivareta sine oppgaver og den teknologiske utviklingen. Dataansvarlige og databehandleren skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Tiltakene skal sikre kontinuitet i tjenesteleveransen. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. Dette omfatter tiltak som blant annet tilgangsstyring, logging og etterfølgende kontroll.

Departementet opprettholder også forslaget om en hjemmel for å kunne kreve uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2, for personell som skal ha privilegerte tilganger til IKT-systemene. Forslaget innebærer en adgang til å kreve politiattest fra personer som skal tilsettes i stillinger som skal ha slik tilgang eller annet personell som skal gis slik tilgang, for eksempel innleide konsulenter eller personell tilsatt i andre virksomheter som yter tjenester til helse- og omsorgstjenesten. Forslaget overlater således til virksomheten å avgjøre om det skal innhentes politiattest i det enkelte tilfelle. Hjemmelen har ikke tilbakevirkende kraft, slik at det ikke kan kreves attest av personell som allerede har privilegert tilgang. Dette betyr også at personer som allerede

er ansatt uten privilegerte tilganger, kan avkreves politiattest dersom de skal få slike tilganger.

Med privilegert tilgang menes tilgang med spesielle rettigheter og tillatelser som er nødvendige for å utføre administrative eller sensitive oppgaver, som ikke er tilgjengelige for vanlige brukere. Dette kan inkludere tilgang til kritiske systemer, konfigurasjonsendringer og administrasjon av sikkerhetsinnstillinger. Tilgangene gis ut fra tjenstlige behov, men kan misbrukes dersom feil person gis disse tilgangene. Potensiale for skade er stort, og misbruk vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver og befolkningens helse og sikkerhet, og derigjennom kunne skade kritiske samfunnsfunksjoner.

Departementet foreslår videre at det i pasientjournalloven § 22 og helseregisterloven § 21 presiseres at departementet i forskrift kan fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.

Departementet foreslår derfor også at lovbestemmelsenes overskrift endres til «Tekniske og organisatoriske sikkerhetstiltak». Dette vil gi et bedre bilde av hva bestemmelsen regulerer. Etter gjeldende rett er forskriftshjemmelen begrenset til å «fastsette nærmere krav til informasjonssikkerhet» ved behandling av helseopplysninger.

Departementet merker seg at Datatilsynet uttaler at endringene i pasientjournalloven § 22 og helseregisterloven § 21, medfører at de er bedre tilpasset innholdet i personvernforordningen artikkel 32. Speilingen av ordlyden i artikkel 32, så vel som en konkretisering av lovkravene, ser Datatilsynet som positivt. Datatilsynet ser også positivt på en forskriftshjemmel som gjør at sikkerhetstiltakene kan utdypes og konkretiseres ytterligere.

Departementet merker seg videre at Helse Sør-Øst RHF er negativ til forslaget, og anbefaler at endringer i sektorregelverket avventes til CER-direktivet og NIS/NIS II er gjennomført i norsk rett. Helse Sør-Øst RHF påpeker videre at dagens regelverk fungerer godt, og forslagene gir fare for at oppmerksomheten vris fra områdene med størst risiko til de områdene som omtales i bestemmelsen. Helseforetakene er underlagt en rekke regelverk, og disse stiller dels eksplisitt og dels forutsetningsvis krav til god risikostyring.

Departementet har forståelse for innspillet til Helse Sør-Øst RHF, men mener det er viktig at kravene presiseres i disse to lovene. Regelverket er fragmentert og det er ønskelig å synliggjøre helheten i kravene i helselovgivningen.

6 Økonomiske og administrative konsekvenser

Forslagene om å begrense delingen av store datasett ved tilgjengeliggjøring fra helseregistre, vil kunne ha noe administrative og økonomiske konsekvenser for dataansvarlig for registrene. De enkelte virksomhetene må i enkelte saker gjøre tilleggsvurderinger av om tilgjengeliggjøring kan true samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare.

Endringen i sikkerhetsbestemmelsene i helseregisterloven og pasientjournalloven vil kunne medføre merarbeid av begrenset karakter for aktørene som er omfattet av regelverket. Kravet om politiattest vil innebære noe økte kostnader for politiet.

Konsekvensene antas i all hovedsak å gjelde statlige aktører, og merutgiftene dekkes innenfor gjeldende budsjettrammer.

7 Merknader til de enkelte bestemmelsene

Til endringer i helsepersonelloven

Til helsepersonelloven § 29

Formålet med forslaget er å ha et rettslig grunnlag for å kunne unnlate å dele datasett med helsedata, som kan ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Dette gjelder også aggregerte (anonyme) data.

«Helsedata» er et vidt begrep som kan omfatte alle typer opplysninger om helse, enten de frembringes i helse- og omsorgstjenestene, gjennom de store befolkningsundersøkelsene eller på andre måter. Begrepet helsedata favner videre enn begrepet helseopplysninger slik det er definert i personvernforordningen artikkel 4 nr. 15. Helsedata kan være anonyme, direkte identifiserbare eller indirekte identifiserbare.

Helsedata brukes både til å administrere og yte helsehjelp (primærbruk) og til å holde oversikt over helsetilstanden i befolkningen, over aktivitet og ressursbruk i helse- og omsorgstjenesten, til å forstå hva som påvirker helsen i befolkningen, til å planlegge framtidens behov for helsetjeneste og til å utvikle kunnskap om forebygging, diagnostikk, behandling og effekter av behandlingen (sekundærbruk).

Unntak fra deling med begrunnelse av at slik deling antas å ville ha betydning for samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare, må vurderes konkret. Departementet antar imidlertid at det i de fleste saker om tilgjengeliggjøring ikke er nødvendig med en særskilt vurdering av hensynet til samfunnssikkerheten. Behovet for slike vurderinger vil trolig være forbeholdt noen få saker med tilgang til store datasett.

Departementets presiserer at helsedata med et skadepotensiale som faller inn under sikkerhetslovens regler om beskyttelse av informasjon, skal reguleres av sikkerhetsloven.

Bestemmelsen må ses i sammenheng med forslag til endringer i helseregisterloven §§ 19, 19 a, 19 b og 19 e.

Det vises til de alminnelige merknadene i punkt 4.4.

Til endringer i pasientjournalloven

Til pasientjournalloven § 22

Det følger av forslaget at det ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, også skal tas hensyn til den teknologiske utviklingen og kritiske samfunnsfunksjoner. Departementet foreslår videre at det presiseres at departementet i forskrift kan fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.

Departementet foreslår videre at paragrafens ordlyd endres slik at det tydelig fremgår at bestemmelsen også dekker andre sikkerhetsutfordringer. Det foreslås derfor at det også inntas en plikt til å gjennomføre en risikovurdering av nettverks- og informasjonssystemer som benyttes for å levere tjenester etter pasientjournalloven. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, kritiske samfunnsfunksjoner, helse- og omsorgstjenestens evne til å ivareta sine oppgaver og den teknologiske utviklingen.

Dataansvarlige og databehandleren skal iverksette proporsjonale tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Tiltakene skal sikre kontinuitet i tjenesteleveransen. Tiltakene skal samlet sørge for et sikkerhetsnivå som er tilpasset risikoen. Dette omfatter tiltak som blant annet tilgangsstyring, logging og etterfølgende kontroll. Bestemmelsen inneholder også en hjemmel for å kreve uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2, for personer som skal ha privilegerte tilganger til nettverks- og informasjonssystemer. Hjemmelen har ikke tilbakevirkende kraft, slik at det ikke kan kreves attest av personell som allerede har privilegert tilgang. Med privilegert tilgang menes tilgang med spesielle rettigheter og tillatelser som er nødvendige for å utføre administrative eller sensitive oppgaver, som ikke er tilgjengelige for vanlige brukere. Dette kan inkludere tilgang til kritiske systemer, konfigurasjonsendringer og administrasjon av sikkerhetsinnstillinger. Tilgan-

gene gis ut fra tjenstlige behov, men kan misbrukes dersom feil person gis disse tilgangene. Potensiale for skade er stort, og misbruk vil kunne true helse- og omsorgstjenestens evne til å ivareta sine oppgaver og befolkningens helse og sikkerhet, og derigjennom kunne skade kritiske samfunnsfunksjoner.

Det vises til de alminnelige merknadene i punkt 5.4.

Til endringer i helseregisterloven

Til helseregisterloven § 19 nytt femte ledd

I forslaget presiseres det at plikten til å utarbeide statistikk ikke gjelder anonyme datasett som kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare.

Det vises til de spesielle merknadene i omtalen av endringene i helsepersonelloven § 29 og de alminnelige merknadene i punkt 4.4.

Til helseregisterloven § 19 a nytt åttende ledd

I bestemmelsen presiseres at helseopplysninger som kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare, ikke skal gjøres tilgjengelig.

Forslaget må ses i sammenheng med tilsvarende endringer i §§ 19, 19 b, 19 e og helsepersonelloven § 29. Det vises til de spesielle merknadene i omtalen av endringene i helsepersonelloven § 29 og de alminnelige merknadene i punkt 4.4.

Til helseregisterloven § 19 b nytt andre ledd

Bestemmelsen er identisk med § 19 a nytt åttende ledd og presiserer at helseopplysninger som kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare, ikke skal gjøres tilgjengelig. Forslaget må også ses i sammenheng med tilsvarende endringer i §§ 19, 19 e og helsepersonelloven § 29.

Det vises til de spesielle merknadene i omtalen av endringene i helsepersonelloven § 29 og de alminnelige merknadene i punkt 4.4.

Til helseregisterloven § 19 e fjerde ledd

Av forslaget følger at det ikke kan gis dispensasjon fra taushetsplikt, når tilgjengeliggjøring vil true samfunnets evne til å verne grunnleggende verdier og funksjoner eller sette liv og helse i fare. Dette kommer i tillegg til om tilgjengeliggjøringen er ubetenkelig ut fra etiske, medisinske og helsefaglige hensyn.

Forslaget må ses i sammenheng med tilsvarende endringer i §§ 19, 19 a, 19 b og helsepersonelloven § 29.

Det vises til de spesielle merknadene i omtalen av endringene i helsepersonelloven § 29 og de alminnelige merknadene i punkt 4.4.

Til helseregisterloven § 21

Forslaget tilsvarer forslaget til endringer i pasientjournalloven § 22. Det vises derfor til omtalen av denne.

Det vises til de alminnelige merknadene i punkt 5.4.

Helse- og omsorgsdepartementet

t i l r å r :

At Deres Majestet godkjenner og skriver under et framlagt forslag til proposisjon til Stortinget om endringer i helselovgivningen (tilgjengeliggjøring av helsedata og krav til tekniske og organisatoriske sikkerhetstiltak).

Vi HARALD, Norges Konge,

s t a d f e s t e r :

Stortinget blir bedt om å gjøre vedtak til lov om endringer i helselovgivningen (tilgjengeliggjøring av helsedata og krav til tekniske og organisatoriske sikkerhetstiltak) i samsvar med et vedlagt forslag.

Forslag

til lov om endringer i helselovgivningen (tilgjengeliggjøring av helsedata og krav til tekniske og organisatoriske sikkerhetstiltak)

I

I lov 2. juli 1999 nr. 64 om helsepersonell m.v. skal § 29 fjerde ledd, nytt tredje punktum lyde:

Dersom tilgjengeliggjøring av opplysninger kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare, skal opplysningene ikke gjøres tilgjengelig.

II

I lov 20. juni 2014 nr. 42 om behandling av helseopplysninger ved ytelse av helsehjelp gjøres følgende endringer:

§ 22 skal lyde:

§ 22 *Tekniske og organisatoriske sikkerhetstiltak*

Den dataansvarlige og databehandleren skal gjennomføre *nødvendige* tekniske og organisatoriske tiltak for å *ivareta sikkerheten ved behandling av personopplysninger. Tiltakene skal være egnet med hensyn til risikoen ved behandlingen av personopplysningene,* jf. personvernforordningen artikkel 32. *Den dataansvarlige og databehandleren skal også gjennomføre risikovurderinger av nettverks- og informasjonssystemene som benyttes for å levere tjenester i henhold til denne loven.*

Sikkerhetstiltakene skal være proporsjonale og tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, kritiske samfunnsfunksjoner, helse- og omsorgstjenestens evne til å ivareta sine oppgaver og den teknologiske utviklingen.

Den dataansvarlige og databehandleren skal iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Dette omfatter tiltak som blant annet tilgangsstyring, logging og etterfølgende kontroll. Den dataansvarlige og databehandleren kan kreve uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2, fra personer som skal ha privilegerte tilganger til nettverks- og informasjonssystemer.

Departementet kan i forskrift fastsette nærmere krav til tekniske og organisatoriske sikkerhetstiltak.

III

I lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger gjøres følgende endringer:

§ 19 nytt femte ledd skal lyde:

Plikten til å utarbeide statistikk etter andre og tredje ledd gjelder ikke dersom tilgjengeliggjøring av opplysningene kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare.

§ 19 a nytt åttende ledd skal lyde:

Dersom tilgjengeliggjøring av helseopplysninger kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare, skal opplysningene ikke gjøres tilgjengelig.

§ 19 b nytt andre ledd skal lyde:

Dersom tilgjengeliggjøring av helseopplysninger kan true samfunnets evne til å verne grunnleggende verdier og funksjoner og sette liv og helse i fare, skal opplysningene ikke gjøres tilgjengelig.

§ 19 e fjerde ledd første punktum skal lyde:

Det kan bare gis dispensasjon dersom tilgjengeliggjøringen er ubetenkelig ut fra etiske, medisinske og helsefaglige hensyn *og ikke vil true samfunnets evne til å verne grunnleggende verdier og funksjoner og ikke sette liv og helse i fare.*

§ 21 skal lyde:

§ 21 *Tekniske og organisatoriske sikkerhetstiltak*

Den dataansvarlige og databehandleren skal gjennomføre *nødvendige* tekniske og organisatoriske tiltak for å *ivareta sikkerheten ved behandlingen av personopplysninger. Tiltakene skal være egnet med hensyn til risikoen ved behandlingen av personopplysningene*, jf. personvernforordningen

artikkel 32. I registre som er etablert med hjemmel i §§ 10 eller 11, skal navn, fødselsnummer og andre personidentifiserende kjennetegn lagres kryptert. *Den dataansvarlige og databehandleren skal også gjennomføre risikovurderinger av nettverks- og informasjonssystemene som benyttes for å levere tjenester i henhold til denne loven.*

Sikkerhetstiltakene skal være proporsjonale og tilpasset risikoen. Ved vurderingen av hva som er et forsvarlig sikkerhetsnivå, skal det tas hensyn til den enkeltes personvern, kritiske samfunnsfunksjoner, helse- og omsorgstjenestens evne til å ivareta sine oppgaver og den teknologiske utviklingen.

Den dataansvarlige og databehandleren skal iverksette tiltak for å forebygge, avdekke og redusere konsekvensene av skadelige hendelser. Dette omfatter tiltak som blant annet tilgangsstyring, logging og etterfølgende kontroll. Den dataansvarlige og databehandleren kan kreve uttømmende og utvidet politiattest, jf. politiregisterloven § 41 nr. 2, fra personer som skal ha privilegerte tilganger til nettverks- og informasjonssystemer.

Departementet kan i forskrift fastsette nærmere krav til *tekniske og organisatoriske sikkerhetstiltak*.

IV

Loven gjelder fra den tiden Kongen bestemmer. Kongen kan sette i kraft de enkelte bestemmelsene til forskjellig tid.

Trykksak
2041 0446

Departementenes sikkerhets- og serviceorganisasjon