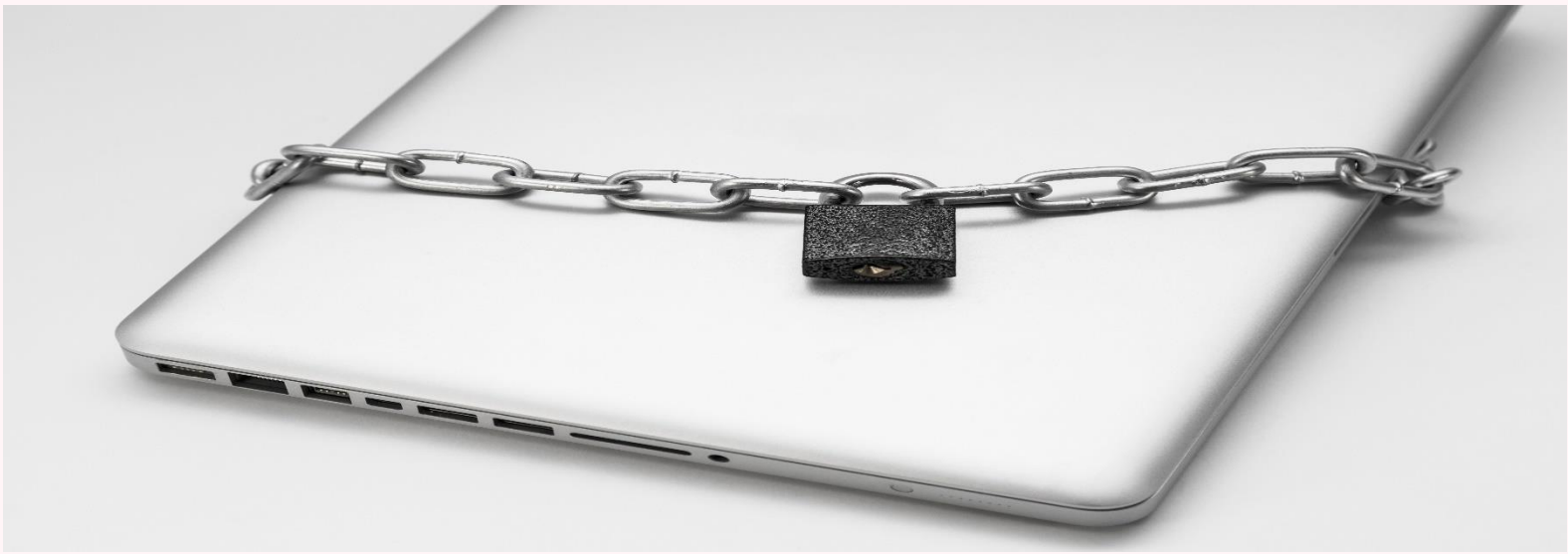
Riksrevisjonen

Revisjonsrapport for 2022 om informasjonssikkerhet og tilgjengeliggjøring av person- og helseopplysninger i helseregistre

Rapportert i Dokument 1 (2023–2024)



Forsidebilde: Kolosov/Scandinavian Stockphoto
ISBN-nummer: 978-82-8229-570-3

Revisjonen er gjennomført som en del av Riksrevisjonens kontroll av disposisjoner i henhold til

- **lov om Riksrevisjonen § 9 første ledd**
- **instruks om Riksrevisjonens virksomhet § 3b**
- **INTOSAIs standard for etterlevelsesrevisjon (ISSAI 4000)**
- **Riksrevisjonens faglige retningslinjer for etterlevelsesrevisjon**

Innhold

1 Sammendrag

1.1 Bakgrunn for revisjonen

I Norge har vi mange helseregistre som bidrar til å ivareta og forbedre helsetjenester og behandlingstilbud. Av totalt 15 sentrale offentlige helseregistre er det 11 helseregistre som er lovbestemt i lov om helseregistre og behandling av helseopplysninger (helseregisterloven).[1] Ni av de elleve lovbestemte helseregistrene er underlagt Helse- og omsorgsdepartementet.[2]

Formålet med helseregistrene er å samle person- og helseopplysninger, slik at disse kan behandles samlet og brukes til blant annet kvalitetsforbedring, forebyggende arbeid, beredskap, analyser og forskning. Helseregistrene gir informasjon om blant annet smittsomme sykdommer, bivirkninger, dødsårsaker og helse- og omsorgstjenester.

Det er Folkehelseinstituttet, Helsedirektoratet og Statens legemiddelverk som er dataansvarlig for de lovbestemte helseregistrene under Helse- og omsorgsdepartementet, og disse tre virksomhetene er dermed overordnet ansvarlig for å overholde personvernprinsippene og regelverket.

Både helseregisterloven og lov om behandling av personopplysninger (personopplysningsloven) stiller krav til håndtering av personopplysninger. De dataansvarlige virksomhetene skal behandle personopplysningene i samsvar med prinsippene i personvernforordningen (GDPR). Formålet med forordningen er å sørge for god beskyttelse av personopplysninger samtidig som personopplysninger skal kunne utveksles fritt innenfor EØS-området.[3] Den 15. juni 2018 ble det vedtatt en ny personopplysningslov som gjør forordningen til norsk rett.[4]

God informasjonssikkerhet betyr at informasjonssystemene som benyttes til å behandle informasjon, er sikret. Dette inkluderer sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene.[5]

For å ivareta sikkerheten må de dataansvarlige virksomhetene sørge for at personopplysningene

- sikres mot uautorisert utlevering og tilgang – sikre konfidensialitet
- sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer – sikre integritet
- er tilgjengelig for autoriserte personer med tjenstlig behov – sikre tilgjengelighet

I tillegg stiller personvernregelverket krav om sikring av robusthet. Robusthet betyr at programvaren som behandler personopplysninger, skal være robust mot for eksempel sårbarheter, angrep og uhell.[6]

Medisinsk og helsefaglig forskning utføres med mål om å frembringe ny kunnskap om helse og sykdom. En viktig kilde til data som kan benyttes til denne typen forskning, er data som oppbevares i de lovbestemte helseregistrene.

For at forskere skal kunne benytte data fra helseregistrene, må de sende en søknad til den virksomheten som forvalter helseregistret de ønsker data fra. Søknaden må dokumentere at forskningsprosjektet oppfyller vilkårene for å få tilgjengeliggjort person- og helsedata fra helseregistret.

[1] Kreftregisteret, helsearkivregisteret, Pasientens prøvesvar, Reseptformidleren og Forsvarets helseregister kommer i tillegg til helseregistrene under Helse- og omsorgsdepartementet. Disse er underlagt henholdsvis Oslo universitetssykehus HF, Arkivverket, Norsk helsenett, Helsedirektoratet og Forsvarsdepartementet.
[2] Kreftregisteret og Forsvarets helseregister er lovbestemt i helseregisterloven § 11.
[3] Forordningen ble innlemmet i EØS-avtalen ved vedtak i EØS-komiteen 6. juli 2018.
[4] Personopplysningsloven trådte i kraft 20. juli 2018.
[5] https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet.
[6] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf.

Vurderer virksomheten at de etterspurte helsedataene er relevante og nødvendige for forskningsprosjektets formål, skal dataene bli tilgjengeliggjort, jf. kravene i helseregisterloven.

Målet med revisjonen har vært å kontrollere om person- og helseopplysninger i lovbestemte helseregistre som inneholder personidentifiserende opplysninger og er underlagt Helse- og omsorgsdepartementet, behandles i henhold til kravene til informasjonssikkerhet, personvern og tilgjengeliggjøring i helseregisterloven og personopplysningsloven.

Rapporten ble forelagt Helse- og omsorgsdepartementet ved brev av 13. juni 2023. Departementet har i brev av 4. juli 2023 gitt kommentarer til rapporten. Kommentarene er i hovedsak innarbeidet i rapporten.

1.2 Konklusjoner

Person- og helseopplysninger i helseregistre behandles ikke i tilstrekkelig grad i henhold til kravene i helseregisterloven og personopplysningsloven.

Konklusjonen bygger på følgende hovedfunn:

- Virksomhetene har ikke oversikt over sikkerhetsarbeidet som gjøres hos leverandørene, og jobber ikke systematisk med risiko og tiltak.
- Viktige informasjonssikkerhetstiltak hos leverandørene er ikke er implementert eller fungerer ikke etter hensikten.

Helsedirektoratet og Folkehelseinstituttet overholder ikke lovpålagte frister for tilgjengeliggjøring av helseopplysninger.

2 Innledning

I Norge har vi mange helseregistre som bidrar til å ivareta og forbedre helsetjenester og behandlingstilbud. Av totalt 15 sentrale offentlige helseregistre er det 11 helseregistre som er lovbestemt i lov om helseregistre og behandling av helseopplysninger (helseregisterloven).[7] Ni av de elleve lovbestemte helseregistrene er underlagt Helse- og omsorgsdepartementet.[8] Formålet med helseregistrene er å samle person- og helseopplysninger, slik at disse kan behandles samlet og brukes til blant annet kvalitetsforbedring, forebyggende arbeid, beredskap, analyser og forskning. Helseregistrene gir informasjon om blant annet smittsomme sykdommer, bivirkninger, dødsårsaker og helse- og omsorgstjenester.

Helseregisterloven skal sikre at behandlingen av helseopplysninger foregår på en etisk forsvarlig måte, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste.

2.1 Lovbestemte helseregistre

Ifølge helseregisterloven § 11 kan enkelte helseregistre behandle opplysninger som navn, fødselsnummer og andre personidentifiserende kjennetegn uten samtykke fra den registrerte. Personopplysningene skal behandles i samsvar med prinsippene i personvernforordningen (General Data Protection Regulation – GDPR). Ifølge Datatilsynet er tilfredsstillende informasjonssikkerhet et grunnkrav som må være oppfylt for at det skal være tillatt å behandle personopplysninger.

Det er Folkehelseinstituttet, Helsedirektoratet og Statens legemiddelverk som er dataansvarlig for de lovbestemte helseregistrene under Helse- og omsorgsdepartementet, og disse tre virksomhetene er dermed overordnet ansvarlig for å overholde personvernprinsippene og regelverket. Figur 1 viser de lovbestemte helseregistrene som inneholder personidentifiserende opplysninger og er underlagt Helse- og omsorgsdepartementet, og hvilke virksomheter som er dataansvarlig for disse registrene.

Faktaboks 1 Dataansvarlig

Den dataansvarlige er det primære pliktsubjektet etter personvernforordningen (GDPR) og overordnet ansvarlig for å overholde personvernprinsippene og regelverket.

Personvernforordningen benytter begrepet *behandlingsansvarlig*. I helselovgivningen benyttes i stedet begrepet *dataansvarlig*, ettersom *behandlingsansvarlig* har et annet innhold i helsesektoren.

Kilde: Datatilsynet og Helse- og omsorgsdepartementet

[7] Kreftregisteret, helsearkivregisteret, Pasientens prøvesvar, Reseptformidleren og Forsvarets helseregister kommer i tillegg til helseregistrene under Helse- og omsorgsdepartementet. Disse er underlagt henholdsvis Oslo universitetssykehus HF, Arkivverket, Norsk helsenett, Helsedirektoratet og Forsvarsdepartementet.
[8] Kreftregisteret og Forsvarets helseregister er lovbestemt i helseregisterloven § 11.

Figur 1 Lovbestemte helseregistre som inneholder personidentifiserende opplysninger og er underlagt Helse- og omsorgsdepartementet

Helseregister	Dataansvarlig	Lov
Dødsårsaksregisteret	Folkehelseinstituttet	Helseregisterloven § 11 a
Medisinsk fødselsregister		Helseregisterloven § 11 c
Meldingssystem for smittsomme sykdommer (MSIS)		Helseregisterloven § 11 d
System for vaksinasjonskontroll (SYSVAK)		Helseregisterloven § 11 e
Nasjonalt register over hjerte- og karlidelser		Helseregisterloven § 11 j
Legemiddelregisteret		Helseregisterloven § 11 k
Norsk pasientregister	Helsedirektoratet	Helseregisterloven § 11 g
Kommunalt pasient- og brukerregister		Helseregisterloven § 11 h
System for bivirkningsrapportering	Statens legemiddelverk	Helseregisterloven § 11 i

Kilde: Helseregisterloven § 11

I løpet av 2016 fikk Norsk helsenett i oppdrag å opprette et sentralt tjenestesenter for alle virksomheter under Helse- og omsorgsdepartementet. Senteret skulle levere tjenester innenfor IKT, anskaffelser og arkiv- og dokumentforvaltning. I forbindelse med opprettelsen ble det overført ressurser fra virksomhetene til senteret.

Folkehelseinstituttet og Helsedirektoratet har inngått en avtale med Norsk helsenett om drift av infrastrukturen i de helseregistrene som omfattes av revisjonen. Statens legemiddelverk har tidligere hatt en databehandleravtale med Advania om drift av IT-systemene, men denne databehandleravtalen ble overdratt til Norsk helsenett 1. januar 2017. Norsk helsenett har gjennom databehandleravtalen med Statens legemiddelverk overtatt ansvaret for oppfølgingen av avtalen med Advania.

Faktaboks 2 Databehandler

Databehandleren er den som behandler personopplysninger på vegne av den dataansvarlige. Den dataansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den behandlingsansvarlige. Databehandleren kan derfor bare behandle personopplysninger etter instruks fra den behandlingsansvarlige.

Kilde: Artikkel 4 i personvernforordningen

Helse- og omsorgsdepartementet

Helse- og omsorgsdepartementet har det overordnede ansvaret for at befolkningen skal få gode og likeverdige helse- og omsorgstjenester, og etatsstyringsansvaret for de virksomhetene som er dataansvarlig for helseregistrene som omfattes av denne revisjonen. Helse- og omsorgsdepartementet har også ansvaret for statens eierskap og er ansvarlig for eierstyringen av Norsk helsenett.

Folkehelseinstituttet

Folkehelseinstituttet har en sentral rolle i den nasjonale og globale helseberedskapen og er en sentral kunnskapsprodusent i helsesystemet. Instituttet skal følge med på utviklingen i folkehelsen og helse- og omsorgstjenestene, bidra til utdanning innenfor instituttets fagområder, drive omfattende

kunnskapsformidling, delta i internasjonalt arbeid på instituttets fagområder og så videre.[9] Instituttet er delt inn i fem områder: *smittevern*, *psykisk og fysisk helse*, *helsedata og digitalisering*, *helsetjenester* og *klima og miljø*. Innenfor området for helsedata og digitalisering er det avdelingen for helseregister som har ansvaret for dødsårsaksregisteret. Fra område for smittevern er det avdeling for smittevernregistre som har ansvaret for meldingssystemet for smittsomme sykdommer.

Helsedirektoratet

Helsedirektoratet skal styrke hele befolkningens helse gjennom helhetlig og målrettet arbeid på tvers av tjenester, sektorer og forvaltningsnivåer.[10] Som faglig rådgiver har Helsedirektoratet ansvar for å følge med på forhold som påvirker folkehelsen og utviklingen i helse- og omsorgstjenestene. Direktoratet skal sammenstille kunnskap og erfaringer og utarbeide nasjonale normer på ulike områder.

Helsedirektoratet er delt opp i fem divisjoner: *folkehelse og forebygging, kvalitet og forløp, helseøkonomi og kompetanse, analyse og samfunn* og *digitalisering og helseregistre.* Divisjonen for digitalisering og helseregistre er delt opp i tre avdelinger: *prosjekt og tjenestedesign, utvikling og digitale kanaler* og *helseregistre.* Avdelingen for helseregistre har ansvaret for kommunalt pasient- og brukerregister.

Statens legemiddelverk

Statens legemiddelverk skal sikre at legemiddelbehandlingen er av god kvalitet, og at legemidlene har lavest mulig pris. Legemiddelverket skal sørge for at befolkningen får likeverdig og rask tilgang til effektive legemidler, og være fag- og tilsynsmyndighet for medisinsk utstyr. De skal også legge til rette for forskning og innovasjon på disse områdene.[11]

Statens legemiddelverk har ansvaret for sikkerhetsinformasjon om legemidler, vurdering av risikominimeringstiltak og overvåking av bivirkningsmeldinger og signaler, i tillegg til å være forvalter av den nasjonale bivirkningsdatabasen. Statens legemiddelverk har ansvaret for systemet for bivirkningsrapportering (bivirkningsregisteret).

2.2 Helseregistrene som omfattes av revisjonen

Ved valg av helseregistre til denne revisjonen har vi vurdert omfanget av sensitive data i registrene, antallet utleveringer av data og resultatene fra risikovurderinger og personvernkonsekvensvurderinger (Data Protection Impact Assessment – DPIA). Vi har vurdert innspill fra Datatilsynet og virksomhetenes egne internrevisjoner. I tillegg var det ønskelig å inkludere alle virksomhetene som er dataansvarlig for de lovbestemte helseregistrene.[12] Datatilsynet fremhever kommunalt pasient- og brukerregister på grunn av mengden av sensitive data og meldingssystemet for smittsomme sykdommer på grunn av de mange endringene på dette området de siste årene. Vi har valgt ut systemet for bivirkningsrapportering for å inkludere Statens legemiddelverk, og vi har valgt ut dødsårsaksregisteret for å inkludere både avdelingen for smittevernregistre og avdelingen for helseregistre hos Folkehelseinstituttet.

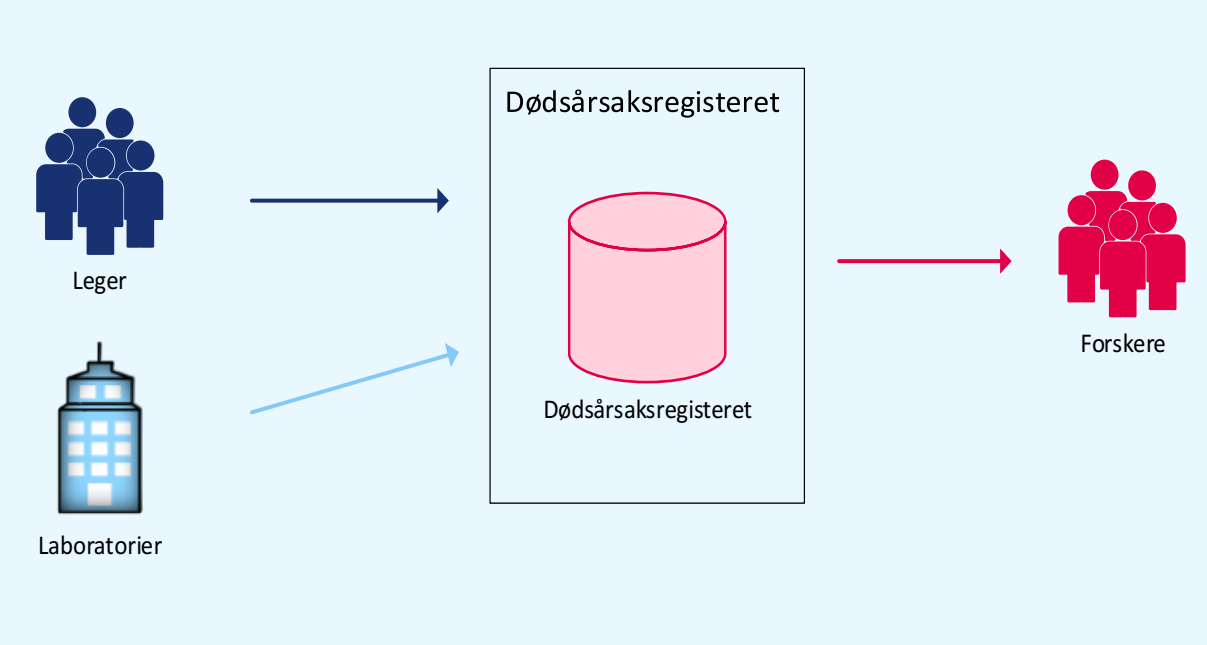
Dødsårsaksregisteret

Formålet med dødsårsaksregisteret er å overvåke dødsårsaker i befolkningen, belyse endringer i dødsårsaker over tid og utarbeide nasjonal, regional og lokal statistikk over dødsårsaker. Registeret inneholder data om dødsårsaker i Norge og skal gi grunnlag for planlegging, kvalitetssikring og kvalitetsutvikling i helse- og omsorgstjenesten og helse- og omsorgsforvaltningen. Figur 2 viser en

[9] fhi.no/om fhi, 9. august 2022.
[10] https://www.helsedirektoratet.no/om-oss/dette-gjor-helsedirektoratet.
[11] legemiddelverket.no, 9. august 2022.
[12] Se figur 1.

forenklet dataflyt for dødsårsaksregisteret. Det er flere mottakere av data fra registeret, jf. kapittel 2.5. I figuren vises kun forskere.

Figur 2 Dataflyt for dødsårsaksregisteret



Kilde: Riksrevisjonen, basert på informasjon fra Folkehelseinstituttet

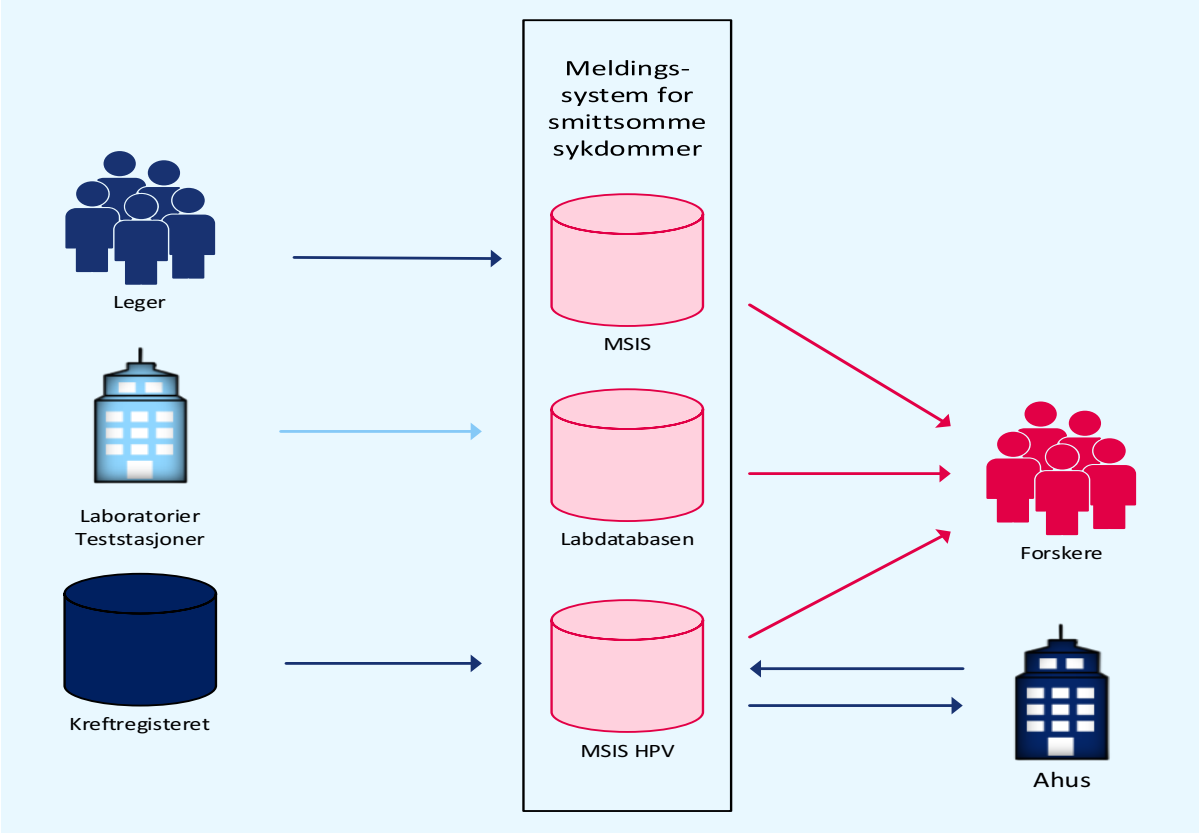
Folkehelseinstituttet har opprettet egen løsning for elektronisk dødsmelding. Den 1. januar 2022 ble det obligatorisk å sende dødsmeldinger elektronisk. Alle leger som er tilkalt til en døende eller til en som er død, har plikt til å melde inn dødsfall. Alle leger som har godkjent HPR-nummer, har tilgang til å melde dødsfall elektronisk. Løsningen bruker HelseID til pålogging. Legene sender inn den elektroniske dødsmeldingen til folkeregisteret og til Folkehelseinstituttet/dødsårsaksregisteret med opplysninger om dødsårsak. Dataene i registret kommer fra elektroniske dødsmeldinger, obduksjonsresultat på papir og svar på spørsmål som Folkehelseinstituttet har stilt til leger og institusjoner.[13]

Meldingssystemet for smittsomme sykdommer

Formålet med registret er å følge med på smittsomme sykdommer hos mennesker i Norge gjennom fortløpende og systematisk innsamling, analyse, tolking og rapportering av opplysninger om forekomst av smittsomme sykdommer. Dette skal legge grunnlaget for å beskrive forekomsten av smittsomme sykdommer over tid etter geografiske og demografiske forhold. Registret skal også legge grunnlaget for å oppdage og oppklare utbrudd av smittsomme sykdommer, det skal gi råd til publikum, helsepersonell og forvaltningen om smitteverntiltak, og det skal evaluere virkningene av smittevernstiltak og behandlingstiltak. Figur 3 viser en forenklet dataflyt for meldingssystemet for smittsomme sykdommer (MSIS). Data fra MSIS brukes til blant annet overvåking, nasjonal og internasjonal rapportering i tillegg til forskning, jf. kapittel 2.5. I figuren vises meldinger til og fra Akershus universitetssykehus, og utlevering til forskning.

[13] Verifisert referat fra intervju med avdeling for helseregistre i Folkehelseinstituttet 26. januar 2023.

Figur 3 Dataflyt for meldingssystemet for smittsomme sykdommer



Kilde: Riksrevisjonen, basert på informasjon fra Folkehelseinstituttet

Personidentifiserende opplysninger i registeret meldingssystem for smittsomme sykdommer blir kryptert. Registret består av tre saksbehandlingssystemer eller registerapplikasjoner: *MSIS, MSIS HPV* og *Labdatabasen.*

Registerapplikasjonen *MSIS* mottar meldinger fra fastleger, kommuneleger og sykehusleger. Informasjonen sendes inn til databasen gjennom klinikermeldinger. Noe informasjon kan overføres automatisk, mens noe må legges inn manuelt fra selve meldingen. Ved hjelp av koding kontrolleres det fortløpende at meldingene stemmer overens med opplysninger i folkeregisteret. Om nødvendig kan meldingene også avklares med den sykdomsansvarlige.

Registerapplikasjonen *Labdatabasen* mottar meldinger elektronisk fra laboratorier og teststasjoner. Innsending skjer gjennom mikrobiologisk svarrapport. Applikasjonen henter automatisk ut relevante data fra meldingene og legger informasjon i databasen.

Registerapplikasjonen *MSIS HPV* mottar data fra kreftregisteret, som har meldeplikt til meldingssystemet for smittsomme sykdommer. Meldingene sendes elektronisk og de går rett inn i applikasjonen. Data om alle tilfeller av kreft og et utvalg tilfeller med forstadier til kreft analyseres for humant papillomavirus (HPV) ved referanselaboratoriet ved Akershus universitetssykehus. HPV-analysene meldes fra Akershus universitetssykehus til MSIS HPV databasen.[14]

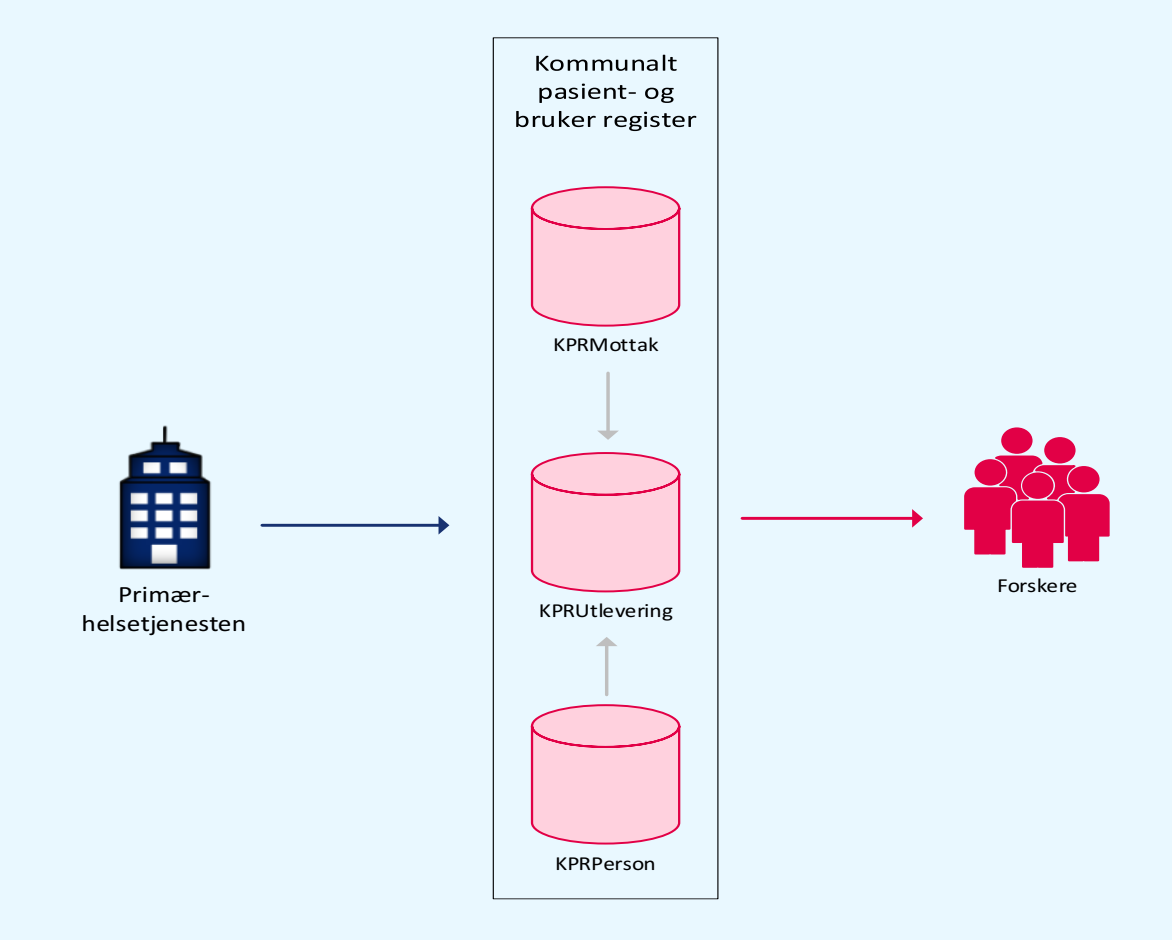
Kommunalt pasient- og brukerregister

Kommunalt pasient- og brukerregister (KPR) inneholder opplysninger om de som har søkt om, mottar eller har mottatt helse- og omsorgstjenester fra kommunene. Formålet med registret er å gi grunnlag for forskning, kvalitetssikring, planlegging, utvikling og styring av helse- og omsorgstjenesten. Figur 4

[14] Verifisert intervju med avdelingen for smittevernregistre i Folkehelseinstituttet 11. januar 2023.

viser en forenklet dataflyt for KPR. Forskere er kun en av målgruppene for KPR, jf. kapittel 2.5. I figuren vises kun forskere.

Figur 4 Dataflyt for kommunalt pasient- og brukerregister



Kilde: Riksrevisjonen, basert på informasjon fra Helsedirektoratet

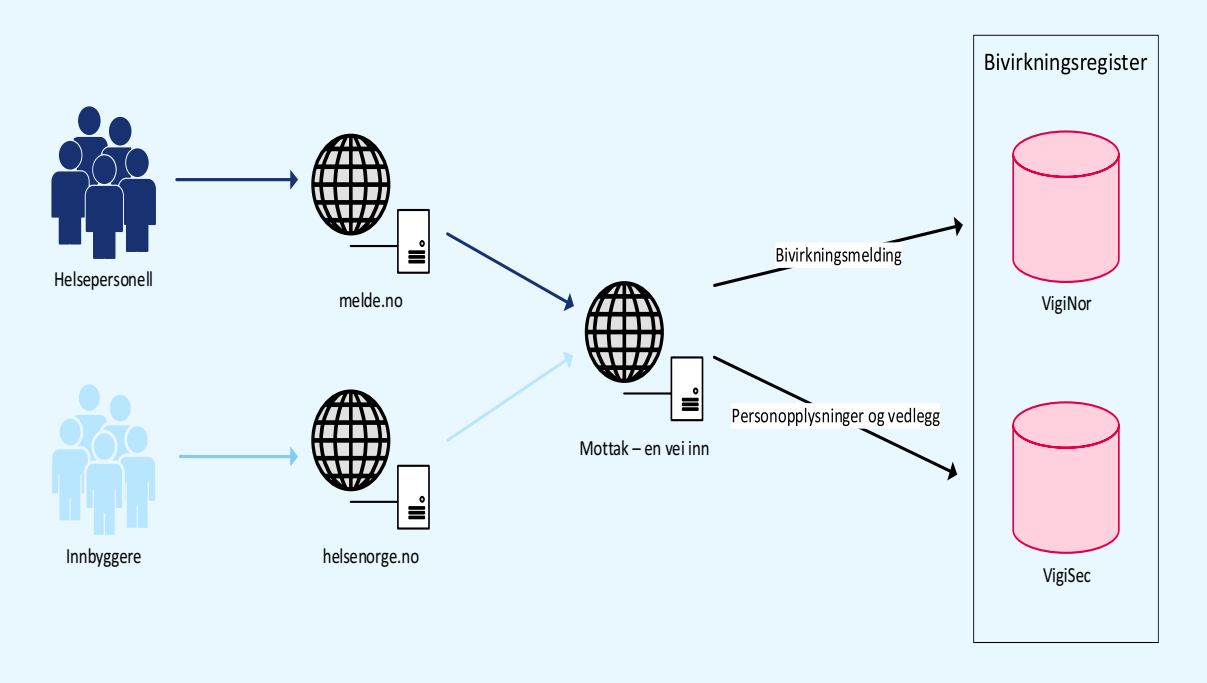
Helsedirektoratet innhenter data til KPR automatisk. Datakildene er eksempelvis offentlige og private sykehus, fastleger og legevakter og avtalespesialister. Det arbeides for tiden med å få inn fastlegedata og tannhelsedata. For at Helsedirektoratet skal få inn mest mulig komplette data med kjent og dokumentert kvalitet, er det et tett samarbeid med de rapporterende enhetene og systemleverandørene deres. Det er viktig og nødvendig at enhetene har systemstøtte som sikrer at alle data kommer inn i den elektroniske pasientjournalen.[15]

Bivirkningsregisteret

Bivirkningsregisteret inneholder meldinger om mistenkte bivirkninger av legemidler, inkludert vaksiner, fra helsepersonell og innbyggere i Norge. Registret skal bidra til sikker og effektiv legemiddelbruk gjennom fortløpende og systematisk innsamling, behandling og analysering av opplysninger om mistenkte bivirkninger av legemidler. Opplysningene i registret kan tilgjengeliggjøres til styring planlegging av legemiddelbruk, til kvalitetsforbedring av legemidler og til forskningsformål. Figur 5 viser en forenklet dataflyt for bivirkningsregisteret.

[15] Verifisert referat fra møte med Helsedirektoratet 17. januar 2023.

Figur 5 Dataflyt for bivirkningsregisteret



Kilde: Riksrevisjonen, basert på informasjon fra Statens legemiddelverk

Systemene *VigiNor* og *VigiSec* utgjør til sammen bivirkningsregisteret. Innrapporteringene til bivirkningsregisteret skjer i hovedsak ved at helsepersonell rapporterer bivirkninger på melde.no, eller ved at pasienter og pårørende rapporterer inn bivirkninger på helsenorge.no.

For å belyse saken kan man sende inn vedlegg, for eksempel journalposter, bilder, obduksjonsrapporter og så videre. Vedleggene kan ha ulike formater og vil i mange tilfeller inneholde personidentifiserende opplysninger. Innrapporterte opplysninger sendes videre til *Mottak – en vei inn*. Denne løsningen splitter deretter fødselsnummer, kontaktopplysninger og vedlegg lagrer dem i *VigiSec* (i sikker sone). Selve bivirkningsmeldingen blir lagret i *VigiNor*.[16]

Før 30. april 2020 hadde ikke registret personidentifiserende opplysninger, og derfor var det ikke aktuelt å sammenstille dataene fra dette registret med data fra andre registre. Bivirkningsregisteret inkludert personidentifiserende opplysninger, er et ungt register som foreløpig ikke har et dataomfang som gjør det interessant å hente ut data fra det. Hittil har Statens legemiddelverk mottatt kun to forespørsler om slik utlevering. Ingen av forespørslene har vært til bruk i forskning. Skriftlige rutiner for utlevering av data er under utarbeidelse.

2.3 Personvern og informasjonssikkerhet

Både helseregisterloven og lov om behandling av personopplysninger (personopplysningsloven) stiller krav til håndtering av personopplysninger. De dataansvarlige virksomhetene skal behandle personopplysningene i samsvar med prinsippene i personvernforordningen (GDPR). Formålet med forordningen er å sørge for god beskyttelse av personopplysninger samtidig som personopplysninger skal kunne utveksles fritt innenfor EØS-området.[17] Den 15. juni 2018 ble det vedtatt en ny personopplysningslov som gjør forordningen til norsk rett.[18]

Ifølge Datatilsynet er tilfredsstillende informasjonssikkerhet et grunnkrav som må være oppfylt for at det skal være tillatt å behandle personopplysninger. Å ivareta strenge krav til konfidensialitet er én

[16] Verifisert referat fra møte med Statens legemiddelverk 5. januar 2023.
[17] Forordningen ble innlemmet i EØS-avtalen ved vedtak i EØS-komiteen 6. juli 2018.
[18] Personopplysningsloven trådte i kraft 20. juli 2018.

side av saken, men det er også viktig å sikre at personopplysningene i helseregistrene er tilgjengelige til det formålet de er samlet inn for, og at de er og fortsetter å være korrekte og ikke endres eller manipuleres av uvedkommende.[19]

God informasjonssikkerhet betyr at informasjonssystemene som benyttes til å behandle informasjon, er sikret. Dette inkluderer sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene.[20]

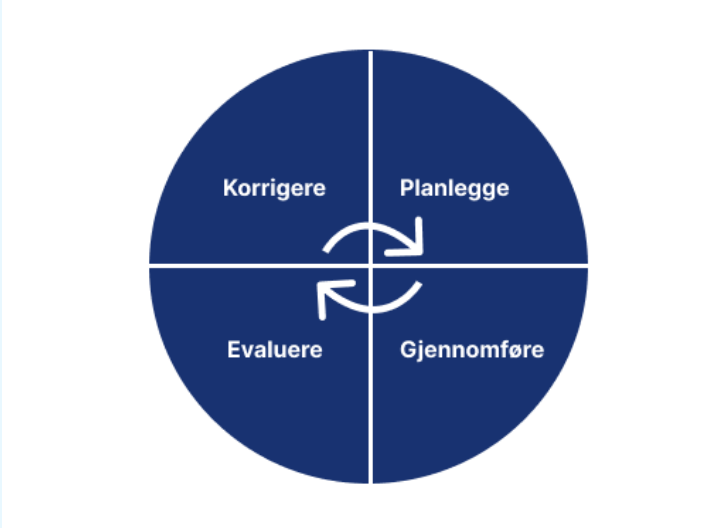
For å ivareta sikkerheten må de dataansvarlige virksomhetene sørge for at personopplysningene

- sikres mot uautorisert utlevering og tilgang – sikre konfidensialitet
- sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer – sikre integritet
- er tilgjengelig for autoriserte personer med tjenstlig behov – sikre tilgjengelighet

I tillegg stiller personvernregelverket krav om sikring av robusthet. Robusthet betyr at programvaren som behandler personopplysninger, skal være robust mot for eksempel sårbarheter, angrep og uhell.[21]

Den dataansvarlige skal dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernforordningen. Et styringssystem er en formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer, kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.[22] Figur 6 viser hvordan et styringssystem kan fremstilles.

Figur 6 Et styringssystem kan fremstilles som en syklus



Kilde: Direktoratet for e-helse: Veileder om internkontroll for informasjonssikkerhet og personvern

Styringssystemet for informasjonssikkerhet og personvern skal sikre at arbeidet med personvern og informasjonssikkerhet blir en kontinuerlig prosess. Det betyr at virksomheten hele tiden bør prøve å forbedre seg og videreutvikle systemet i takt med endringer som påvirker informasjonssikkerheten og personvernet i virksomheten.[23]

[19] Brevkontroll med sentrale helseregistre – Datatilsynets oppsummering https://www.datatilsynet.no/contentassets/839c29c829e240a39965b1d56f9b9bc1/rapport---brevkontroll-med-sentrale-helseregistre.pdf.
[20] https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet.
[21] https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/innebygd-personvern/02-sjekkliste_krav_250817.pdf.
[22] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, versjon 6.0, vedtatt 4. februar 2020.
[23] Direktoratet for e-helse. (2021). *Veileder om internkontroll for informasjonssikkerhet og personvern versjon 1.0,* datert 2. desember 2021.

2.4 Trussel- og risikobildet

Datatilsynets oppgave er å kontrollere at personvernregelverket etterleves, og medvirke til at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.[24] Datatilsynet opplyser at de gjennom sitt arbeid ser at det fortsatt er høy risiko for at kravene i personvernforordningen ikke blir etterlevd, og trekker spesielt frem kommunalt pasient- og brukerregister fordi det inneholder omfattende helse- og personopplysninger. Ifølge Datatilsynet ble kravene til kryptering redusert da data fra tidligere IPLOS (individbasert pleie- og omsorgsstatistikk) ble tatt inn i kommunalt pasient- og brukerregister.[25]

Datatilsynet opplyste videre at deres generelle inntrykk var at behovet for at det skal være enkelt å koble data, går foran sikkerheten. Datatilsynet nevner ellers meldesystem for smittsomme sykdommer, der det har vært store endringer de siste årene på grunn av pandemien.

Ifølge Datatilsynet er det nødvendig å kontrollere at virksomhetenes risikovurderinger er oppdaterte, og at en identifisert risiko faktisk blir fulgt opp med tiltak og ikke bare blir liggende i en tiltaksplan. Videre er det viktig å se på tilgangsstyringen, inkludert terminering av tilganger og bruk av tilgangsroller. Logging er et viktig tiltak. Virksomhetene må ha en god sikkerhetsarkitektur og evnen til å fange opp forsøk på uautorisert tilgang og eventuelle sårbarheter og hull, slik at eksterne angrep kan forhindres. Her nevnes også oppbevaring av krypteringsnøkler. Virksomhetene bør ha en oversikt over forsøk på angrep, avvik og hendelser.

I internrevisjoner som er gjennomført i Helsedirektoratet og Folkehelseinstituttet, er det observert risiko for at det ikke jobbes systematisk med internkontrollen av personvern og informasjonssikkerhet. Videre er det risiko for at virksomhetene har manglende risikostyring og risikohåndtering.[26] Personvernombudene i virksomhetene mener at det er risiko knyttet til datautlevering og leverandøroppfølging.[27]

Nasjonal sikkerhetsmyndighet (NSM) er Norges direktorat for nasjonal forebyggende sikkerhet. Dette direktoratet gir råd og gjennomfører tilsyn og andre kontrollaktiviteter på sivil og militær side. Direktoratets arbeid dreier seg om sikring av informasjon, systemer, objekter og infrastruktur av nasjonal betydning. Ifølge en rapport som ble utgitt av NSM i 2022, er det høy risiko for alvorlige cyberoperasjoner, og risikoen øker blant annet i virksomheter som driver forskning og utvikling innenfor helse.[28] I tillegg har innføringen av nye digitale løsninger akselerert hos mange virksomheter under pandemien. Med nye løsninger følger nye sårbarheter og behov for nye risikoreduserende tiltak.[29]

Lav bevissthet om hva som står på spill, og hvilke sårbarheter som kan utnyttes, påvirker vurderinger av risiko i den enkelte virksomhet, privat som offentlig. Dette kan føre til at sårbarheter ikke blir avdekket, og at nødvendige sikkerhetstiltak ikke blir iverksatt. Fravær av risikostyring og tilstrekkelig gode avtaler mellom virksomhetene gir grensesnittutfordringer som kan ha konsekvenser for både de involverte virksomhetene og den nasjonale sikkerheten.[30]

Det er i mange tilfeller enklere å få tilgang til en virksomhets teknologi eller bedriftshemmeligheter eller annen sensitiv informasjon ved å utnytte en leverandør eller underleverandør enn ved å ramme virksomheten direkte. Hendelser hos store leverandører av IT-tjenester eller programvare vil kunne få konsekvenser for svært mange virksomheter.[31] Uoversiktlige verdikjeder gjør det vanskeligere å

[24] https://www.datatilsynet.no/om-datatilsynet/oppgaver/.
[25] Kartleggingsmøte med Datatilsynet 12. oktober 2022.
[26] Rapport fra Helsedirektoratets internrevisjon juni/2020, årsrapport for 2021 fra Folkehelseinstituttets internrevisjon.
[27] Kartleggingsmøte med personvernombud og sikkerhetskoordinator for helseregistre i Helsedirektoratet samt personvernombud i Folkehelseinstituttet.
[28] NSMs rapport «Risiko 2022» s. 9.
[29] NSMs rapport «Risiko 2022» s. 27.
[30] NSMs rapport «Risiko 2022» s. 23.
[31] NSMs rapport «Risiko 2022» s. 20.

beskytte viktige nasjonale verdier. Verdikjedene må kartlegges, og sikkerhetsstyringen av leverandører og underleverandører må prioriteres høyere.[32]

Det viktigste budskapet fra nasjonal sikkerhetsmyndighet for 2022 var at toppledere må prioritere å beskytte seg og samfunnet enda bedre i tiden fremover. Forståelsen for trussel- og risikobildet må økes, og tiltak må iverksettes nå.

Ifølge rapporten fra NSM er det generelle sikkerhetsnivået i IKT-systemer hos norske virksomheter for lavt. I de fleste tilfeller er det tekniske sårbarheter som utnyttes til å kompromittere systemene. De aller fleste cyberhendelser som rammer norske virksomheter og myndighetsorganer, kunne vært unngått eller fått langt mindre alvorlige konsekvenser dersom Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet ble fulgt.[33]

Mange virksomheter sikrer seg mot driftsforstyrrende hendelser som innbrudd eller nedetid på systemene, men disse sikringstiltakene beskytter ikke nødvendigvis mot målrettede trusselaktører. Et tilstrekkelig sikkerhetsnivå avhenger av at virksomheter oppdaterer kunnskapen sin, blir mer sikkerhetsbevisste og tilpasser sikringstiltakene etter endringer i trusselbildet.[34]

Selv om flere tar innover seg alvoret i det digitale trussel- og risikobildet, går den teknologiske utviklingen og endringene i sårbarhetsbildet så raskt at den digitale risikoen stadig blir høyere. Sikkerheten i IKT-systemene i norske virksomheter må derfor styrkes. NSMs grunnprinsipper er et godt utgangspunkt for IKT-sikkerhetsarbeidet.[35]

2.5 Tilgjengeliggjøring av helseopplysninger

Medisinsk og helsefaglig forskning utføres med mål om å frembringe ny kunnskap om helse og sykdom. En viktig kilde til data som kan benyttes til denne typen forskning, er data som oppbevares i de lovbestemte helseregistrene som er beskrevet i kapittel 2.1.

For at forskere skal kunne benytte data fra helseregistrene, må de sende en søknad til den virksomheten som forvalter helseregistret de ønsker data fra. Søknaden må dokumentere at forskningsprosjektet oppfyller vilkårene for å få tilgjengeliggjort person- og helsedata fra helseregistret. Vurderer virksomheten at de etterspurte helsedataene er relevante og nødvendige for forskningsprosjektets formål, skal dataene bli tilgjengeliggjort, jf. kravene i helseregisterloven.

Foruten til forskere utleverer helseregistrene data til

- forvaltningen
- myndighetene
- internasjonale organisasjoner
- andre helseregistre på grunn av kvalitetssikring
- mediene

[32] NSMs rapport «Risiko 2022» s. 8.
[33] NSMs rapport «Risiko 2022» s. 27.
[34] NSMs rapport «Risiko 2022» s. 9.
[35] NSMs rapport «Risiko 2022» s. 9.

3 Mål og problemstillinger

3.1 Målet med revisjonen

Målet med revisjonen har vært å kontrollere om person- og helseopplysninger i lovbestemte helseregistre som inneholder personidentifiserende opplysninger og er underlagt Helse- og omsorgsdepartementet, behandles i henhold til kravene til informasjonssikkerhet, personvern og tilgjengeliggjøring i helseregisterloven og personopplysningsloven.

3.2 Problemstilling 1: risikostyring og leverandøroppfølging

Har virksomhetene gjennomført risikostyring og leverandøroppfølging slik at de kan iverksette tiltak som er egnet for at virksomhetene skal oppnå et akseptabelt sikkerhetsnivå?

3.3 Problemstilling 2: informasjonssikkerhetstiltak

Har virksomhetene gjennomført informasjonssikkerhetstiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen?

3.4 Problemstilling 3: tilgjengeliggjøring

Tilgjengeliggjør virksomhetene helseopplysninger fra lovbestemte helseregistre i henhold til regelverket?

3.5 Avgrensninger

Denne revisjonen er avgrenset til å gjelde følgende helseregistre:[36]

- dødsårsaksregisteret
- meldingssystemet for smittsomme sykdommer
- kommunalt pasient- og brukerregister
- systemet for bivirkningsrapportering

Virksomhetene som er dataansvarlig for disse helseregistrene, er Folkehelseinstituttet, Helsedirektoratet og Statens legemiddelverk. Leverandørenes interne systemer har ikke vært en del av revisjonen.

Dataene ble samlet i perioden juni 2022 til mai 2023.

I problemstilling 3 vil vi ta utgangspunkt i forskningsprosjekter som er blitt sendt til forhåndsgodkjenning hos regionale komiteer for medisinsk og helsefaglig forskningsetikk, og som inneholder data som direkte eller indirekte er personidentifiserende. Vi tar utgangspunkt i data fra 2020–2022.

[36] Jf. kapittel 2.2.

4 Revisjonskriterier

4.1 Formål med og prinsipper for behandling helse- og personopplysninger

Både helseregisterloven og personopplysningsloven stiller krav til virksomhetenes håndtering av person- og helseopplysninger i helseregistrene.

Helseregisterlovens formål er å legge til rette for innsamling og annen behandling av helseopplysninger for å fremme helse, forebygge sykdom og skade og forbedre helse- og omsorgstjenestene. Loven skal sikre at behandlingen er etisk forsvarlig, ivaretar den enkeltes personvern og brukes til individets og samfunnets beste.[37]

I henhold til personopplysningsloven § 1 gjelder personvernforordningen[38] som lov med de tilpasningene som følger av vedlegg XI, protokoll 1 og avtalen for øvrig.

I henhold til personvernforordningens prinsipper[39] skal personopplysninger

- behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»)
- samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenelig med de opprinnelige formålene («formålsbegrensning»)
- være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»)
- behandles på en måte som gir tilstrekkelig sikkerhet for personopplysningene, inkludert vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)

Den dataansvarlige[40] er ansvarlig for at prinsippene overholdes, og skal kunne påvise det.

Forskrift om standarder og nasjonale e-helseløsninger skal bidra til at virksomheter i helse- og omsorgstjenesten bruker standarder, standardsystemer, godkjent programvare, kodeverk, klassifikasjonssystemer og nasjonale e-helseløsninger for å fremme sikker og effektiv samhandling og bruk av IKT. Forskriften gjelder for virksomheter som forvalter og tilgjengeliggjør helseopplysninger for helseregistre med hjemmel i helseregisterloven §§ 9 til 11.

Av forskriftens § 7 *Katalog over standarder* fremgår det at Direktoratet for e-helse gir ut en katalog med oversikt over obligatoriske og anbefalte standarder.

Direktoratets referansekatalog for e-helse gjelder alle virksomheter i helse- og omsorgstjenesten og leverandørene. Av referansekatalogen fremgår det at alle virksomheter som er tilknyttet helsenettet[41], er forpliktet til å følge norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (normen) inkludert vedlegg.[42]

[37] Helseregisterloven § 1.
[38] EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679) (GDPR) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger.
[39] Artikkel 5 i personvernforordningen.
[40] Den dataansvarlige bestemmer over personopplysningene, mens databehandleren opptrer på vegne av den dataansvarlige. Dataansvarlige for helseregistrene som er underlagt Helse- og omsorgsdepartementet, er Folkehelseinstituttet, Helsedirektoratet og Statens legemiddelverk.
[41] Norsk helsenett utvikler forvalter og drifter helsenettet
[42] Referansekatalogen for e-helse, https://www.ehelse.no/standardisering/om-standardisering/referansekatalogen-for-e-helse.

Normen er en bransjenorm som er utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren. Kravene i normen utdyper og supplerer gjeldende regelverk. Overholdelse av kravene i normen kan brukes til å påvise at virksomhetene etterlever de forpliktelsene de har etter regelverket.

Basert på dette legger vi til grunn at kravene i normen med tilhørende veiledning kan benyttes som en del av revisjonskriteriene i denne revisjonen.

Normen beskriver krav til ledelse og ansvar samt risikostyring og informasjonssikkerhet. Det fremgår av normen at informasjonssikkerhet handler om å håndtere risiko forbundet med informasjon og behandling av personopplysninger. Helseopplysninger skal behandles i samsvar med prinsippene i personvernforordningen og på en måte som sikrer informasjonens integritet, tilgjengelighet og konfidensialitet. Lovverket stiller krav til at relevante og nødvendige helseopplysninger på en rask og effektiv måte blir tilgjengelige, samtidig som opplysningene vernes mot innsyn fra uvedkommende.[43]

Det fremgår av kapittel 2.4 i normen at alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern (internkontroll). Med styringssystem menes formalisering av hvordan virksomheten planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelse av relevant regelverk, krav og avtaler.

Informasjonssikkerhet og personvern bør inngå i det totale styringssystemet i virksomheten. Styringssystemet skal tilpasses virksomhetens størrelse, risiko, egenart og aktiviteter og informasjonsbehandlingens art, omfang, formål og sammenhengen den utføres i.

Styringssystemet skal dokumenteres. Dokumenter som er angitt i styringssystemet, skal holdes oppdatert og arkiveres på det tidspunktet da de erstattes med en ny gjeldende versjon. Dette kan for eksempel være rutiner for sikkerhetsrevisjoner, risikovurderinger, driftsrutiner, avvik og hvordan de håndteres, ledelsens gjennomgang, databehandleravtaler mv.

4.1.1 Ledelse og ansvar

Krav til ledelse og ansvar fremgår av kapittel 2 i normen. Virksomhetens øverste ledelse skal etablere roller og funksjoner med tilstrekkelige ressurser og kompetanse til å gjennomføre de oppgavene som er nødvendige for at ansvaret skal være ivaretatt. Alle skal være kjent med hvilke oppgaver de har, i tillegg til å ha tilstrekkelig kunnskap om andres relevante ansvar og oppgaver, og hvem som har myndighet til å ta beslutninger.

Den dataansvarlige skal

- delegere myndighet og oppgaver (jf. kapittel 2.1)
- etablere og etterleve styringssystemet (jf. kapittel 2.4)
- gjennomføre risikovurderinger og personvernkonsekvensvurderinger der det er nødvendig (jf. kapittel 3)
- sikre den registrertes rettigheter (jf. kapittel 4)
- etablere og dokumentere tekniske og organisatoriske tiltak (jf. kapittel 5)
- inngå og følge opp avtaler (jf. kapittel 5.7)
- håndtere avvik (jf. kapittel 5.8)[44]

Den dataansvarlige skal dokumentere at virksomheten har gjennomført tiltak for å etterleve personvernforordningen.

[43] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, versjon 6.0, vedtatt 4. februar 2020.
[44] Norm for informasjonssikkerhet og personvern i Helse- og omsorgssektoren, kapittel 2.2.

Databehandleren skal

- bare behandle helse- og personopplysninger etter instruks fra den dataansvarlige
- ikke bruke underdatabehandler uten at det er godkjent av den dataansvarlige
- være ansvarlig for at underleverandører oppfyller sine forpliktelser
- bistå den dataansvarlige med å sikre at virksomheten overholder forpliktelser som gjelder informasjonssikkerhet[45]

Databehandleren skal bistå den dataansvarlige med personvern og informasjonssikkerhet slik at risikoen blir akseptabel.

4.2 Problemstilling 1: risikostyring og leverandøroppfølging

I henhold til helseregisterloven § 22 og artikkel 24 i personvernforordningen skal den dataansvarlige gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, personopplysningsloven og helseregisterloven. Nevnte tiltak skal gjennomgås jevnlig og oppdateres ved behov.

4.2.1 Plikt til internkontroll

Hvert lovbestemte helseregister har egen forskrift til helseregisterloven. Seks av de ni forskriftene har bestemmelser om *plikt til internkontroll* og krav til *internkontrollens innhold*.

Av forskriftene fremgår det at databehandlere som behandler helseopplysninger på vegne av dataansvarlige, skal behandle opplysningene i samsvar med rutiner den dataansvarlige har innført. Forskriftene viser videre til at internkontrollen innebærer at den dataansvarlige skal ha kunnskap om gjeldende regler for behandling av helseopplysninger og tilstrekkelig og oppdatert dokumentasjon på gjennomføring av rutiner, i tillegg til å ha denne dokumentasjonen tilgjengelig for de som den måtte angå. Internkontrollen skal blant annet inneholde rutiner virksomheten følger dersom avvik oppstår, og opplysninger om hvem som er ansvarlig. Videre skal virksomheten dokumentere rutiner som skal følges for at avvik ikke skal gjenta seg.

4.2.2 Risikostyring

Risikostyring er koordinerte aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko. Dette innebærer å få oversikt over informasjon og teknologi i virksomheten og å identifisere trusler, sårbarheter og konsekvenser ved mulige uønskede hendelser for både virksomheten og de registrerte. Risikostyring innebærer også å analysere risikoen og etablere tiltak for å opprettholde et egnet sikkerhetsnivå.46

Virksomhetens leder må derfor sikre at det forebyggende sikkerhetsarbeidet er helhetlig. For at tilstrekkelig sikkerhet skal oppnås, er det ikke nok med for eksempel bare fysiske tiltak eller bare elektroniske tiltak. Tilstrekkelig sikkerhet oppnår man når både organisatoriske, elektroniske, fysiske og menneskelige tiltak er kombinert og virker sammen. En sentral del av det forebyggende sikkerhetsarbeidet er å velge de risikoreduserende sikkerhetstiltakene som er mest hensiktsmessige og effektive når virksomhetens verdier skal beskyttes. Uten et helhetlig syn på sikkerhet vil det være vanskelig for virksomheten å sikre sine verdier i tilstrekkelig grad.47

Ifølge artikkel 32 i personvernforordningen skal den dataansvarlige og databehandleren sikre informasjonssikkerhet som gjelder konfidensialitet, integritet, tilgjengelighet og robusthet i

[45] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 2.3.
[46] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, versjon 6.1 kapittel 3.
[47] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-sikkerhetsstyring/introduksjon.

behandlingssystemene og behandlingstjenestene. Personvernforordningen gir ingen nærmere utdyping av hva som ligger i elementene i informasjonssikkerhet.

Av Nasjonal sikkerhetsmyndighets grunnprinsipper[48] fremgår det at virksomheten bør identifisere regelverk, bransjenormer og avtaler som kan ha innvirkning på sikring av informasjonssystemer. En bransjenorm i denne sammenheng er den nevnte normen for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Punkt 3.2 i denne normen inneholder minimumskravene som skal ivareta informasjonssikkerheten. Dette er minimumskrav som virksomheten skal oppfylle for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet.

Konfidensialitet innebærer at virksomheten skal sikre seg mot at uvedkommende får kjennskap til helse- og personopplysninger. Kravene til konfidensialitet betyr at virksomhetene skal

- hindre uautorisert tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten
- avgrense tilgang for autorisert personell i henhold til tjenstlig behov
- ha oversikt (logger) over alle som har hatt tilgang til helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten

Integritet innebærer at helse- og personopplysninger er sikret mot utilsiktet eller uautorisert endring eller sletting. Kravene til integritet betyr at virksomhetene skal

- logge hvem som har rettet, registrert, endret og slettet
- hindre utilsiktet eller uautorisert endring eller sletting
- sikre at helse- og personopplysninger registreres på rett person
- sikre at helse- og personopplysninger føres i henhold til relevant kodeverk og terminologi
- sikre at helse- og personopplysninger er korrekte og om nødvendig oppdaterte
- hindre at kopier av data blir en kilde til utdatert informasjon

Tilgjengelighet og robusthet innebærer at helse- og personopplysninger og annen informasjon med betydning for informasjonssikkerheten er tilgjengelig til rett tid. Krav til tilgjengelighet betyr at virksomhetene skal

- sikre at helse- og personopplysninger er tilgjengelige i henhold til tjenstlig behov
- sikre forsvarlig og stabil drift av informasjonssystemene
- sikre at det finnes egnede tekniske og organisatoriske tiltak som muliggjør forebygging, deteksjon, skalerbarhet, håndtering og gjenoppretting
- sikre at informasjonssystemene er tilgjengelige i henhold til virksomhetens tilgjengelighetskrav

Virksomhetene skal fastsette et nivå for akseptabel risiko basert på normens minimumskrav til informasjonssikkerhet og eventuelt egne informasjonssikkerhetsmål.

Områder for risikovurdering bør ta utgangspunkt i oversikten over helse- og personopplysningene som behandles, og oversikten over teknologi som brukes.[49]

Under punkt 3.4 i Normen står følgende:

«Risikovurdering er et verktøy for å identifisere uønskede hendelser. Risikovurderingen bør ta utgangspunkt i en kartlegging av informasjonsverdier og hva som vil bli konsekvensen av hendelser som rammer tilgjengeligheten, integriteten og konfidensialiteten til informasjonsverdiene.

[48] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/identifisere-og-kartlegge/kartlegg-styringsstrukturer-leveranser-og-understottende-systemer/, se anbefalte tiltak kapittel 1.1.1.
[49] Se norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, versjon 6.1, kapittel 3.3.

Virksomhetene skal vurdere sannsynligheten for og mulige konsekvenser av at en hendelse inntreffer. Dersom risikoen er uakseptabel, skal virksomheten gjennomføre tiltak for å redusere risikoen.»

«Vurdering og håndtering av risiko skal gjennomføres med utgangspunkt i minimumskravene for konfidensialitet, integritet, tilgjengelighet og robusthet og virksomhetens akseptkriterier.»

«Risikovurderinger bør oppdateres ved endring i trusselbildet. I tillegg skal virksomhetens ledelse jevnlig gjennomføre risikovurderinger som ledd i sitt arbeid med å kontrollere informasjonssikkerheten.»

«Risikovurderinger skal dokumenteres. Der det er nødvendig å gjennomføre tiltak for å oppnå akseptabel risiko, skal tiltakene fremgå av en plan med tydelig frist og hvem som er ansvarlig for gjennomføring. Planen skal forankres hos virksomhetens ledelse.»

4.2.3 Personvernkonsekvensvurdering

Det fremgår av artikkel 35 i personvernforordningen at dersom det er sannsynlig at en type behandling vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den dataansvarlige på forhånd vurdere hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.

I henhold til kapittel 3.5 i normen skal virksomhetene alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger medfører for den registrerte. Virksomhetene skal dokumentere lovligheten av behandlingen, formålet, hvordan personvernet er ivaretatt, og at det er gjort tilstrekkelige tiltak for å håndtere risikoen. Hvis det er sannsynlig at en behandling medfører høy risiko for den registrerte, skal virksomheten gjennomføre en mer grundig personvernkonsekvensvurdering (DPIA). Denne personvernkonsekvensvurderingen skal gjennomføres før behandlingen av personopplysninger påbegynnes, og ifølge kapittel 3.5 i normen skal den minst inneholde følgende:

- en systematisk beskrivelse av behandlingsaktivitetene av helse- og personopplysninger
- beskrivelse av formålet med behandlingen av personopplysninger
- en vurdering av om behandlingene av helse- og personopplysningen er nødvendig og står i et rimelig forhold til formålet
- en vurdering av risikoen for personvernet til den registrerte
- planlagte risikoreduserende tiltak for ivaretakelse av personvernet

4.2.4 Leverandørstyring

NSM har gitt ut sikkerhetsfaglige anbefalinger ved tjenesteutsetting (outsourcing). [50] For at IKT-sikkerheten skal være ivaretatt ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst på behovet for

- oversikt og kontroll på hele livsløpet
- god bestillerkompetanse
- gode risikovurderinger for å kunne ta riktig beslutning
- riktige og gode krav til IKT-tjenesten og til leverandør
- riktig beslutning på riktig nivå

NSM understreker at «grunnprinsippene for IKT-sikkerhet er like relevante for IKT-tjenester som er tjenesteutsatt, som for IKT-tjenester som forvaltes av virksomheten selv. Forskjellen er om man stiller krav til interne eller eksterne tjenesteleverandører».

[50] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/bruk-av-tjenesteutsetting-og-skytjenester/.

Eksempler på faktorer som NSM mener vil kunne påvirke risikobildet, er at virksomhetene får mindre kontroll over stadig mer komplekse verdikjeder, at de taper intern kompetanse, og at de blir avhengige av eksterne tjenesteleverandør for å kunne levere tjenestene sine.

I kapittel 5 i normen oppgis følgende krav til leverandørstyring:

- Ved levering av tjenester, maskinvare, systemer og så videre skal det avtales skriftlig med leverandørene hvilke sikkerhetskrav som skal oppfylles. Virksomheten skal gjennom avtale forsikre seg om at leverandøren har tilfredsstillende styringssystemer med hensyn til sikkerhetsrevisjon og avviksbehandling.
- Ved tjenesteutsetting skal avtalen omfatte dokumentert risikovurdering som viser den tjenesteutsettende virksomhetens nivå for akseptabel risiko, hvilke oppgaver som er omfattet, og ansvarsforholdene for disse, og en beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart.
- Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak (at de oppfyller krav i lov og forskrift).
- Databehandleren skal uten ugrunnet opphold melde til den dataansvarlige at avvik har oppstått.
- Leverandøroppfølging (virksomheten skal sikre klarhet i roller og ansvar og at kompetanseressurser deltar i anskaffelser og leverandørstyring).

4.3 Problemstilling 2: informasjonssikkerhetstiltak

I henhold til helseregisterloven § 21 og artikkel 32 i personvernforordningen skal den dataansvarlige og databehandleren gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Disse tiltakene er blant annet

- pseudonymisering og kryptering av personopplysninger
- evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og behandlingstjenestene
- en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er

Den dataansvarlige og databehandleren skal blant annet sørge for tilgangsstyring, logging og etterfølgende kontroll.

Det fremgår av artikkel 32 nr. 2 i personvernforordningen at ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Av artikkel 32 nr. 4 fremgår det at den dataansvarlige og databehandleren skal treffe tiltak for å sikre at enhver fysisk person som handler på vegne av den dataansvarlige eller databehandleren, og som har tilgang til personopplysninger, behandler nevnte opplysninger bare etter instruks fra den dataansvarlige, med mindre unionsretten eller medlemsstatens nasjonale rett krever at vedkommende gjør dette.

4.3.1 Tekniske og organisatoriske tiltak

Ved valg av egnede tekniske og organisatoriske tiltak skal virksomheten vurdere tiltakene etter virksomhetens størrelse, art og omfang for behandling av helse- og personopplysninger, pasientsikkerhet, risikobildet mv. Tiltakene skal velges basert på risikovurderinger, og tiltakene skal være forholdsmessige.

Virksomheten skal dokumentere alle tiltak. Kapittel 5 i normen beskriver sentrale sikkerhetstiltak for virksomhetene:

- tilgangsstyring
  - rutiner for autorisering, endring og avslutning av tilganger
  - et autorisasjonsregister der autorisasjonen skal registreres
  - autentisering (alle standardpassord på systemer og utstyr skal endres før behandling)
  - kontroll av tilgang (ledelsen skal påse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang, minimum årlig)
- sikker IT-drift
  - konfigurasjonskontroll (oversikt over dataflyt, datakommunikasjon og integrasjoner og kontroll på alt eget utstyr og all programvare)
  - logging (som minimum skal følgende logges: autorisert bruk, all system- og administratorbruk, endringer av konfigurasjon og programvare, sikkerhetsrelevante hendelser, forsøk på uautorisert bruk, bruk av selvautorisering. Det skal etableres rutiner for å analysere loggene, og loggene og autorisasjonsregistret skal sikres mot endring og sletting.)
  - styring og håndtering av tekniske sårbarheter
  - sikkerhetsrevisjon (jevnlig og minimum årlig. Det skal foreligge en godkjent plan.)
- håndtering av informasjonssikkerhetsbrudd
  - avvikshåndtering (rutiner for å oppdage og å håndtere avvik. Avviksbehandlingen skal være dokumentert.)

Faktaboks 3 Nasjonal sikkerhetsmyndighets grunnprinsipper

Nasjonal sikkerhetsmyndighets grunnprinsipper for IKT-sikkerhet er et sett med prinsipper og tiltak for å beskytte informasjonssystemer mot uautorisert tilgang, skade og misbruk. De er et utvalg av de prinsippene og tiltakene som Nasjonal sikkerhetsmyndighet mener er mest relevante for norske virksomheter, men de omfatter ikke alle tenkelige tiltak. Prinsippene er fordelt på fire kategorier med tilhørende tiltak:

1. **Identifisere og kartlegge**
   Målet med prinsippet er at virksomheten identifiserer strukturer og prosesser for sikkerhets- og risikostyring for å styre arbeidet med sikring av IKT-systemene. Virksomheten kartlegger leveranser, informasjonssystemer og understøttende funksjoner og vurderer dette opp mot fastsatte toleransegrenser for risiko for å etablere og justere sikkerhetstiltak.
2. **Beskytte og opprettholde**
   Målet med prinsippet er at sikkerhet er en integrert del av prosessene for anskaffelse og utvikling, og virksomheten minimerer risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter.
3. **Oppdage**
   Målet med prinsippet er at virksomheten oppdager og fjerner kjente sårbarheter og kjent skadelig kode I virksomhetens IKT-systemer.
4. **Håndtere og opprette**
   Målet med prinsippet er at virksomheten har implementert effektive prosesser for hendelseshåndtering slik at hendelser oppdages hurtig, kontrolleres, skaden minimeres og hendelsesårsaken fjernes effektivt. Dette inkluderer gjenopprettelse av integriteten til systemer og nettverk

Kilde: NSM. (2020). *Grunnprinsipper for IKT-sikkerhet versjon 2.0*

NSMs grunnprinsipper for IKT-sikkerhet versjon 2.0 inneholder til sammen 118 sikkerhetstiltak, fordelt på 21 prinsipper i de 4 kategoriene. For å hjelpe virksomhetene med å prioritere tiltakene har NSM fordelt tiltakene på 3 prioriteringsgrupper. De høyest prioriterte sikkerhetstiltakene befinner seg i gruppe 1, som inneholder 15 sikkerhetstiltak. Her er noen av dem:

- Kartlegg programvare i bruk i virksomheten.

- Ta ansvar for virksomhetens sikkerhet også ved tjenesteutsetting.
- Etabler et sentralt styrt regime for sikkerhetsoppdatering.
- Deaktiver unødvendig funksjonalitet.
- Endre alle standardpassord på IKT-produktene før produksjonssetting.
- Minimer rettigheter til sluttbrukere og spesialbrukere.
- Minimer rettigheter på driftskontoer.
- Avgjør hvilke deler av IKT-systemet som skal overvåkes.
- Beslutt hvilke data som er sikkerhetsrelevante og bør samles inn.

Virksomheter må vurdere informasjonssikkerheten selv om de har satt ut IKT-infrastrukturen og IKT-tjenester til eksterne leverandører. NSM har gitt ut sikkerhetsfaglige anbefalinger ved tjenesteutsetting (outsourcing). For at IKT-sikkerheten skal være ivaretatt ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst på behovet for

- oversikt og kontroll på hele livsløpet
- god bestillerkompetanse
- gode risikovurderinger for å kunne ta riktig beslutning
- riktige og gode krav til IKT-tjenesten og til leverandøren
- riktig beslutning på riktig nivå

De tekniske sikkerhetstiltakene er vurdert etter Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* og anbefalingene for grunnleggende IKT-sikkerhet som er utarbeidet av The Center for Internet Security («CIS Controls»), eller anbefalingene fra leverandørene. Samlet gir dette beste praksis for hvilke tiltak som bør iverksettes, og hvordan de bør iverksettes for at virksomheten skal oppnå et egnet sikkerhetsnivå. Dette gjelder for eksempel når virksomheten vurderer hvilke innstillinger som vil gi sikker konfigurasjon av et system, eller hvilke hendelser som bør logges.

4.4 Problemstilling 3: tilgjengeliggjøring

I henhold til helseregisterloven § 19 a skal den dataansvarlige etter søknad tilgjengeliggjøre helseopplysninger i helseregistre, inkludert opplysninger som er sammenstilt etter § 19 c,[51] når

I opplysningene skal brukes til et uttrykkelig angitt formål som er innenfor registrets formål
II mottakeren kan godtgjøre at behandlingen vil ha rettslig grunnlag etter personvernforordningen artikkel 6 og 9
III mottakeren kan godtgjøre at behandlingen av opplysningene vil være innenfor rammene av eventuelle samtykker og ikke i strid med eventuelle reservasjoner
IV mottakeren har gjort rede for hvilke egnede tekniske og organisatoriske tiltak som skal settes i verk for å ivareta informasjonssikkerheten

Det skal ikke tilgjengeliggjøres flere opplysninger enn det som er nødvendig til formålet. Opplysningene skal tilgjengeliggjøres uten navn, fødselsnummer eller andre personidentifiserende kjennetegn med mindre slike opplysninger er nødvendige av særlige grunner.

I henhold til helseregisterloven § 19 f skal den dataansvarlige tilgjengeliggjøre helseopplysninger etter § 19 tredje ledd[52] og § 19 a[53] innen 30 virkedager fra en fullstendig søknad er mottatt. Dersom tilgjengeliggjøringen krever sammenstilling med opplysninger fra flere registre, er fristen 60 virkedager. Tilgjengeliggjøringen kan utsettes dersom særlige forhold gjør det uforholdsmessig

[51] Helseopplysninger i helseregistre kan sammenstilles når målet er å utarbeide statistikk. Det skal ikke sammenstilles flere opplysninger enn det som er nødvendig for formålet.
[52] Statistikk basert på opplysninger i registret og opplysninger som er sammenstilt etter § 19 c, dersom statistikken skal brukes til formål som er innenfor registrenes formål.
[53] Den dataansvarlige skal etter søknad tilgjengeliggjøre helseopplysninger i helseregistre.

vanskelig å overholde fristen. Den dataansvarlige skal i så fall gi et foreløpig svar med informasjon om grunnen til forsinkelsen og tidspunktet for når tilgjengeliggjøring sannsynligvis vil skje.

Den dataansvarlige skal føre en oversikt over tilgjengeliggjøring av helseopplysninger fra registret. Oversikten skal vise hvem som har fått opplysningene, og hva som er det rettslige grunnlaget for mottakerens bruk av opplysningene. Oversikten skal oppbevares i minst ti år etter tilgjengeliggjøringen.[54]

[54] Helseregisterloven § 19 h.

5 Metoder

Revisjonen er gjennomført ved hjelp av systematisk innhenting av informasjon om saksforholdet. Informasjonen er bearbeidet og analysert etter revisjonskriteriene og danner grunnlaget for våre funn, konklusjoner og anbefalinger.

For å belyse problemstillingene har vi intervjuet ansvarlige personer i Helse- og omsorgsdepartementet, Folkehelseinstituttet, Helsedirektoratet, Statens legemiddelverk og Norsk helsenett. Videre har vi analysert dokumentasjon og uttrekk av data om tilgangsrettigheter, passordoppsett og andre sikkerhetsinnstillinger.

Vi har valgt ut noen sikkerhetstiltak som har betydning for informasjonssikkerheten, og vi har kontrollert om virksomhetene har gjennomført tiltakene.

5.1 Risikostyring og leverandøroppfølging

5.1.1 Dokumentanalyser

For å undersøke om virksomhetene har gjennomført risikostyring og leverandøroppfølging slik at de kan iverksette tiltak for å oppnå et akseptabelt sikkerhetsnivå, har vi innhentet og analysert følgende dokumentasjon:

- alle risikovurderinger for de fire utvalgte registrene
- alle personvernkonsekvensvurderinger
- rutiner for å sikre at kravene overholdes, inkludert rutiner for
  - oppfyllelse av krav om at personidentifiserende opplysninger bare behandles når det er nødvendig for å fremme formålet med behandlingen av opplysningene, og i tråd med gjeldende bestemmelser om taushetsplikt
  - dokumentasjon og kvalitetskontroll av helseopplysningene
- rutiner for avvikshåndtering og opplysninger om hvem som er ansvarlig
- oversikt over og dokumentasjon av virksomhetenes innmeldte avvik, behandling og oppfølging
- databehandleravtaler med tilhørende driftsavtaler og kravdokumentasjon
- agenda og referat fra driftsmøter og strategiske møter med Norsk helsenett og Advania

5.1.2 Intervjuer

For å undersøke virksomhetenes risikostyring og leverandøroppfølging har vi gjennomført intervjuer med fagpersoner og ledelsen i de aktuelle avdelingene for helseregistre i Statens legemiddelverk, Folkehelseinstituttet, Helsedirektoratet og Norsk helsenett:

- intervju med Statens legemiddelverk 5. januar 2023
- intervju med Folkehelseinstituttet, avdeling for smittevernregistre, 11. januar 2023
- intervju med Norsk helsenett om MSIS og DÅR 12. januar 2023
- intervju med Helsedirektoratet, avdeling for helseregistre, 17. januar 2023
- intervju med Norsk helsenett om KPR 18. januar 2023
- intervju med Folkehelseinstituttet, avdeling for helseregistre, 26. januar 2023
- oppfølgingsintervju med Statens legemiddelverk 17. mars
- oppfølgingsintervju med Folkehelseinstituttet, avdeling for smittevernregistre og avdeling for helseregistre, 22. mars
- oppfølgingsintervju med Helsedirektoratet, avdeling for helseregistre, 13. april

Videre har vi gjennomført intervjuer med de ansvarlige for etatsstyringen av de tre virksomhetene og eierstyringen av Norsk helsenett i Helse- og omsorgsdepartementet.[55] Referatene fra intervjuene er verifisert.

Intervjuene er fulgt opp med skriftlige spørsmål som virksomhetene har besvart. Her følger en oversikt:

- Statens legemiddelverk svarte 24. mars og 11. april.
- Folkehelseinstituttet svarte 31. mars, 13. april, 14. april, 17. april, 28. april og 3. mai.
- Helsedirektoratet svarte 28. april, 3. mai og 10. mai.

5.2 Informasjonssikkerhetstiltak

5.2.1 Kontroll av sikkerhetstiltak

Vi har kontrollert om de aktuelle sikkerhetstiltakene for helseregistrene og den tilhørende IKT-infrastrukturen er gjennomført og dokumentert i samsvar med kravene i regelverket og anbefalingene i de anerkjente standardene.

I Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet*[56] er 15 tiltak gitt høyeste prioritering, da de etter Nasjonal sikkerhetsmyndighets syn er de sikkerhetstiltakene som haster mest. Det at flere av disse tiltakene ikke blir iverksatt, er som oftest årsaken til vellykkede dataangrep.

Vi har valgt noen av de sikkerhetstiltakene som er sentrale i henhold til normen, og som ifølge Nasjonal sikkerhetsmyndighet bør prioriteres høyest:

- tilgangsstyring
- sikkerhetskonfigurasjon og gjennomføring av sikkerhetsoppdateringer
- logging

Dette har ikke vært en fullstendig sikkerhetsrevisjon. Utover de utvalgte sikkerhetstiltakene, kan det være etablert sikkerhetstiltak som har betydning for IKT-sikkerheten, men som ikke er vurdert i revisjonen.

Vi har analysert uttrekk av data om brukere og rettigheter, sikkerhetsoppdateringer, oppsett og innstillinger, installert programvare og logging. Datauttrekkene er basert på våre egenutviklede skript og på autorisasjonslister over brukere fra virksomhetene og leverandørene deres.

Uttrekk av data er innhentet i flere omganger, og det har vært behov for en del avklaringer underveis for å sikre fullstendige leveranser av data. Det har vært noe utfordrende å få riktige uttrekk av data fra Helsedirektoratet. Alle funn er verifisert med skriftlige spørsmålslister, avklaringsmøter og oppsummeringsmøter.

Utkast til rapport ble sendt til Helse- og omsorgsdepartementet 13. juni 2023 for uttalelse. I den forbindelse sendte Helsedirektoratet en epost, der det fremkommer at Norsk helsenett uttalte at det kan hende Riksrevisjonen ikke har mottatt fullstendig dokumentasjon, og at sammenstillinger og konklusjoner om avvik derfor ikke trenger å være korrekt.

Helsedirektoratet og Norsk helsenett ble i epost 26. juni 2023 bedt om å gjøre nødvendige undersøkelser, og sende oss eventuell utfyllende dokumentasjon. Vi har ikke mottatt ytterligere

[55] 15. mars 2023.
[56] Se faktaboks 3.

dokumentasjon som bidrar til å oppklare de områder de mener det er usikkerhet på. Deres kommentarer framgår under funn i kapittel 6.2.1.

5.2.2 Intervjuer

For å undersøke virksomhetenes informasjonssikkerhetstiltak for helseregistrene har vi gjennomført intervjuer med fagpersoner og ledelsen i aktuelle avdelinger for helseregistre i Statens legemiddelverk, Folkehelseinstituttet, Helsedirektoratet og Norsk Helsenett:

- intervju med Statens legemiddelverk 5. januar 2023
- intervju med Folkehelseinstituttet, avdeling for smittevernregistre, 11. januar 2023
- intervju med Norsk helsenett om MSIS og DÅR 12. januar 2023
- intervju med Helsedirektoratet, avdeling for helseregistre, 17. januar 2023
- intervju med Norsk helsenett om KPR 18. januar 2023
- intervju med Folkehelseinstituttet, avdeling for helseregistre, 26. januar 2023
- oppfølgingsintervju med Statens legemiddelverk 17. mars
- oppfølgingsintervju med Folkehelseinstituttet, avdeling for smittevernregistre og avdeling for helseregistre, 22. mars
- oppfølgingsintervju med Helsedirektoratet, avdeling for helseregistre, 13. april

Videre har vi gjennomført intervjuer med de ansvarlige for etatsstyringen av de tre virksomhetene og eierstyringen av Norsk helsenett i Helse- og omsorgsdepartementet.[57] Referatene fra intervjuene er verifisert.

Intervjuene er fulgt opp med skriftlige spørsmål som virksomhetene har besvart. Her følger en oversikt:

- Statens legemiddelverk svarte 24. mars og 11. april.
- Folkehelseinstituttet svarte 31. mars, 13. april, 14. april, 17. april, 28. april og 3. mai.
- Helsedirektoratet svarte 28. april, 3. mai og 10. mai.

5.3 Tilgjengeliggjøring

5.3.1 Utvalg

Ved problemstilling 3, som handler om tilgjengeliggjøring, har vi tatt utgangspunkt i søknader fra forskningsprosjekter om utlevering av data, og vi har sett på de søknadene som er blitt sent til forhåndsgodkjenning hos regionale komiteer for medisinsk og helsefaglig forskningsetikk (REK). Problemstillingen omfatter alle utleveringer av indirekte eller direkte personidentifiserende opplysninger til forskningsformål i perioden 2020–2022. For de tre registrene utgjør dette 290 utleveringer til sammen.

For å kontrollere om virksomhetene behandler søknadene om utlevering av helseregisterdata i samsvar med de lovregulerte forutsetningene, har vi gjennomført en detaljkontroll av 15 utvalgte utleveringer til forskningsprosjekter i tidsrommet 2020–2022. De 15 utleveringene er tilfeldig valgt ut fra den totale mengden utleveringer på 290. Ettersom det har vært ønskelig å vurdere alle de tre registrene og det er noe variasjon i antallet utleveringer fra dem, fordeler de 15 utleveringene seg som følger:

- fire utleveringer fra kommunalt pasient- og brukerregister (KPR)
- fem utleveringer fra meldingssystemet for smittsomme sykdommer (MSIS)

[57] 15. mars 2023

- seks utleveringer fra dødsårsaksregisteret (DÅR)

Da vi utførte revisjonen, hadde ikke bivirkningsregisteret hos Statens legemiddelverk mottatt noen søknader om utlevering av data til forskning.

5.3.2 Intervju

For å undersøke virksomhetenes system og rutiner for tilgjengeliggjøring av data har vi gjennomført intervjuer med fagpersoner og ledelsen i de aktuelle avdelingene for helseregistre i Statens legemiddelverk, Folkehelseinstituttet og Helsedirektoratet:

- intervju med Statens legemiddelverk 5. januar 2023
- intervju med Folkehelseinstituttet, avdeling for smittevernregistre, 11. januar 2023
- intervju med Helsedirektoratet, avdeling for helseregistre, 17. januar 2023
- intervju med Folkehelseinstituttet, avdeling helseregistre, 26. januar 2023

5.3.3 Detaljkontroll

Virksomhetene som forvalter lovpålagte helseregistre, skal etter søknad tilgjengeliggjøre helseopplysninger fra helseregistrene under visse lovregulerte forutsetninger.

Viktige kontrollpunkter fra vår side har vært krav til søknadsdokumentasjon, rettslig grunnlag for utlevering og i hvilken grad virksomhetene stiller krav til forskeren eller institusjonen angående informasjonssikkerhet og personvern. Videre har vi kontrollert hvordan virksomhetene sikrer at data blir behandlet slik som forskeren eller institusjonen har beskrevet i søknaden.

Vi har bedt Folkehelseinstituttet og Helsedirektoratet om å oversende Excel-filene de benytter for å føre oversikt over tilgjengeliggjøring av helseopplysninger fra MSIS, DÅR og KPR. I bestillingene ba vi om at filene kun skulle inneholde utleveringer til forskningsprosjekter, og at utleveringene skulle ha skjedd i perioden 2020–2022.

Når vi har beregnet antall dager det har tatt å tilgjengeliggjøre data, har vi sett på den tiden som har gått fra datoen for fullstendig søknad til datoen for utlevering. Det er kun antall virkedager som er inkludert i beregningene. Vi har brukt kolonnen for antall kilder for å skille mellom om virksomhetene har hatt 30 dagers eller 60 dagers frist på seg til å tilgjengeliggjøre dataene. Når det gjelder meldingssystem for smittsomme sykdommer er det kun tatt utgangspunkt i første søknad per prosjekt. Dette fordi gjentakende utleveringer og oppdateringer for samme prosjekt gir begrenset mulighet for å beregne overholdelse av frist, da utleveringene skjer etter avtale eller i dialog med prosjektet.

6 Funn

6.1 Risikostyring og leverandøroppfølging

I henhold til helseregisterloven § 22 og artikkel 24 i personvernforordningen skal den dataansvarlige gjennomføre tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen, personopplysningsloven og helseregisterloven. Nevnte tiltak skal gjennomgås jevnlig og oppdateres ved behov.

Av forskriftene til helseregisterloven fremgår det at databehandlere som behandler helseopplysninger på vegne av dataansvarlige, skal behandle opplysninger i samsvar med rutiner den dataansvarlige har innført. Forskriftene viser videre til at internkontrollen blant annet skal inneholde rutiner som virksomheten skal følge dersom avvik oppstår, og opplysninger om hvem som er ansvarlig. Videre skal virksomheten dokumentere rutiner som skal følges for at avvikene ikke skal gjenta seg.

Basert på kriteriene har vi kontrollert om virksomhetene har gjennomført risikostyring og leverandøroppfølging slik at de kan iverksette tiltak som er egnet for å oppnå et akseptabelt sikkerhetsnivå.

Hovedfunn

Virksomhetene jobber ikke systematisk med risiko og tiltak, og de har ikke oversikt over sikkerhetsarbeidet som gjøres hos leverandørene.

- **Arbeidet med å identifisere og håndtere risiko, personvernkonsekvenser og avvik er mangelfullt.**
- **Sikkerhetsarbeidet hos leverandøren som drifter infrastrukturen for helseregistrene, følges ikke opp.**

6.1.1 Arbeidet med å identifisere og håndtere risiko, personvernkonsekvenser og avvik er mangelfullt

Personvernforordningen, helseregisterloven, Nasjonal sikkerhetsmyndighets *Grunnprinsipper for IKT-sikkerhet* (jf. faktaboks 3 i kapittel 4.1.3) og norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (normen) setter krav til og gir føringer for virksomhetenes arbeid med informasjonssikkerhet.

Normen er en bransjenorm som er utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren. Det fremgår av kapittel 2.4 i normen at alle virksomheter skal ha et styringssystem for informasjonssikkerhet og personvern (internkontroll). Med styringssystem menes en formalisering av hvordan virksomhetene planlegger, gjennomfører, evaluerer/kontrollerer og korrigerer etterlevelsen av relevant regelverk og relevante krav og avtaler.

Informasjonssikkerhet og personvern bør inngå i det totale styringssystemet i virksomheten. Styringssystemet skal tilpasses virksomhetens størrelse, risiko, egenart og aktiviteter og informasjonsbehandlingens art, omfang og formål og sammenhengen den utføres i.[58]

[58] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 2.4.

Styringssystemet skal dokumenteres. Dokumenter som er angitt i styringssystemet, skal holdes løpende oppdatert og arkiveres på det tidspunktet da dokumentet erstattes med en ny gjeldende versjon. Dette kan for eksempel være rutiner for sikkerhetsrevisjoner, risikovurderinger, driftsrutiner, avvik og hvordan de håndteres, ledelsens gjennomgang, databehandleravtaler mv.[59]

Revisjonen viser at det er flere mangler ved virksomhetenes arbeid med informasjonssikkerhet:

- Risikovurderingene er mangelfulle.
- Det mangler vurderinger av personvernkonsekvenser.
- Virksomhetene har ikke den totale oversikten over alle registrerte avvik som er knyttet til registrene.

Risikovurderingene er mangelfulle

I Nasjonal sikkerhetsmyndighets grunnprinsipper[60] fremgår det at virksomhetene bør identifisere regelverk, bransjenormer og avtaler som kan ha innvirkning på sikring av informasjonssystemer. I kapittel 3.2 og 3.4 i normen er det stilt minimumskrav til risikovurderinger av informasjonssikkerhet. Vurdering og håndtering av risiko skal gjennomføres med utgangspunkt i minimumskravene for konfidensialitet, integritet, tilgjengelighet og robusthet og virksomhetenes akseptkriterier.[61] Overholdelse av kravene i normen kan brukes til å påvise at virksomhetene etterlever de forpliktelsene de har etter regelverket.[62]

Ifølge NSMs grunnprinsipper bør risikovurderingene oppdateres med utgangspunkt i endringer i både regelverk og bransjenormer. Av normen fremgår det at risikovurderingene bør oppdateres når trusselbildet endrer seg.[63] I tillegg skal ledelsen i den enkelte virksomheten jevnlig gjennomføre risikovurderinger for å kontrollere informasjonssikkerheten.

Vi har analysert dokumenterte risikovurderinger fra Helsedirektoratet, Folkehelseinstituttet og Statens legemiddelverk og sammenlignet dem med regelverket og normen. Risikovurderingene viser ikke til hvilket krav i normen de er knyttet til. Flere av minimumskravene i normen som gjelder konfidensialitet, integritet og tilgjengelighet, er ikke dokumentert. Manglende henvisning til minimumskravene for informasjonssikkerhet gjør det vanskelig å se helheten i risikovurderingene, og om virksomhetene etterlever kravene i regelverk og bransjenormer.

Det fremgår ikke av de dokumenterte risikovurderingene at virksomhetene har brukt en bransjenorm for informasjonssikkerhet. Statens legemiddelverk opplyser at de ønsker å følge normen, og Helsedirektoratet opplyser at de følger normen så langt det passer.[64] Folkehelseinstituttet opplyser at de forholder seg direkte til lov og forskrift.[65]

Dokumentanalysen vår viser at flere av risikovurderingene ikke er blitt oppdatert siden personvernforordningen ble innført i 2018. Risikovurderingen for dødsårsaksregisteret er ikke blitt oppdatert siden 2015. Manglende oppdateringer av risikovurderinger gjør det vanskelig å se utviklingen og sammenhengen mellom risiko og tiltak over tid.

Dokumentanalysen av risikovurderingene viser videre at det er store variasjoner mellom de tre virksomhetene når det gjelder hvor detaljert de beskriver de enkelte risikomomentene, og hvor detaljert omfanget av risikovurderingene og risikohåndteringen er. Enkelte av risikovurderingene er på et overordnet nivå og lite beskrevet, mens andre risikovurderinger er mer detaljerte og gjelder spesifikke deler av et helseregister. Det kan også være vanskelig å se om risikovurderingene gjelder

[59] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 2.4.
[60] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/identifisere-og-kartlegge/kartlegg-styringsstrukturer-leveranser-og-understottende-systemer/, se anbefalte tiltak kapittel 1.1.1.
[61] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 3,4, 4. avsnitt.
[62] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 1.4.
[63] Se norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren,, versjon 6.1, kapittel 3.4, 5. avsnitt.
[64] Svar på skriftlige spørsmål fra Statens legemiddelverk 24. mars 2023 og Helsedirektoratet 27. april 2023.
[65] Svar på skriftlige spørsmål fra Folkehelseinstituttet 17. april 2023.

virksomhetene selv eller den delen av registret som er tjenesteutsatt, det vil si der virksomhetene bruker eksterne leverandører. Risikovurderinger som er gjort av Helsedirektoratet er mer detaljerte og gir mer informasjon om hvilke tiltak som skal iverksettes, enn risikovurderingene som er gjort av Statens legemiddelverk og Folkehelseinstituttet.

Tjenesteutsettingen er ikke risikovurdert

Ved tjenesteutsetting av IKT-funksjoner eller andre funksjoner som er av betydning for informasjonssikkerheten eller personvernet, skal virksomheten gjennom relevante avtaler forsikre seg om at leverandøren har et tilfredsstillende styringssystem. Ifølge normen skal avtalen omfatte en dokumentert risikovurdering som viser den tjenesteutsettende virksomhetens nivå for akseptabel risiko, hvilke oppgaver som er omfattet, og ansvarsforholdene for disse. I tillegg skal avtalen inneholde en beskrivelse av leverandørens løsning og grensesnitt mot virksomheten i form av konfigurasjonskart.[66] Virksomheten må revidere risikoen ved tjenesteutsettinger jevnlig og i alle faser av tjenesteutsettingen ettersom risikobildet vil endre seg over tid.[67]

Ingen av virksomhetene har gjort overordnede risikovurderinger av tjenesteutsettingen som sådan, heller ikke av tjenesteleverandøren eller av sin egen oppfølging av tjenesteleverandøren. Som leverandør har Norsk helsenett utarbeidet en risiko- og sårbarhetsanalyse (ROS) av Helsedirektoratets og Folkehelseinstituttets tekniske plattform.

Folkehelseinstituttet uttaler i et intervju at de forutsetter at Norsk helsenett gjennomfører egen ROS. Folkehelseinstituttet mottar ikke slike ROS-er automatisk, men de kan be om å få innsyn og har fått noe på forespørsel.

Advania har utarbeidet en overordnet rapport over risiko som er forelagt Statens legemiddelverk, men det er ikke gjennomført en risikovurdering, slik det er beskrevet i avtalen mellom dem.

Manglende vurderinger av personvernkonsekvenser

Det fremgår av artikkel 35 i personvernforordningen at dersom det er sannsynlig at en type behandling vil medføre en høy risiko for personers rettigheter og friheter, skal den dataansvarlige på forhånd vurdere hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En slik vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer.

I henhold til kapittel 3.5 i normen skal dataansvarlige virksomheter alltid vurdere hvilke konsekvenser behandling av helse- og personopplysninger vil medføre for den registrerte. Det skal gjennomføres en personvernkonsekvensvurdering (DPIA) før behandlingen av personopplysninger påbegynnes.

Vår gjennomgang av virksomhetenes protokoll over behandlingsaktiviteter[68] og gjennomførte DPIA-er viser at det ikke er gjennomført DPIA for alle registrene.

- For dødsårsaksregisteret er det i protokollen over behandlingsaktiviteter[69] konkludert med at det må gjennomføres DPIA. Det er likevel ikke gjennomført ROS eller DPIA for dette registret etter at GDPR trådte i kraft i 2018. Folkehelseinstituttet opplyser at det ved innføringen av GDPR ble vurdert at behovet for DPIA var redusert ettersom driften av registrene var lovpålagt og lovlig før ny lov trådte i kraft.[70]
- For kommunalt pasient- og brukerregister (KPR) vurderte Helsedirektoratet først at det ikke var nødvendig med en egen DPIA fordi Stortinget hadde regulert registret gjennom forskrift. I etterkant er det blitt vurdert at det likevel er behov for det. Det jobbes nå med DPIA for KPR.

[66] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.7.3.
[67] https://nsm.no/regelverk-og-hjelp/rapporter/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/om-temarapporten/.
[68] Jf. artikkel 30 i personvernforordningen.
[69] Protokoll – helseregistre – Folkehelseinstituttet 31. august 2022.
[70] Innspill/merknader fra Folkehelseinstituttet på utkast til rapport fra Riksrevisjonen, 5. juli 2023

- For bivirkningsregisteret og meldingssystemet for smittsomme sykdommer (MSIS) er det gjennomført DIPA i 2022. For MSIS ble DIPA-en igangsatt i 2018, og den er blitt oppdatert løpende med endringer som oppsto i forbindelse med koronapandemien. DPIA for MSIS ble godkjent i 2022.

Folkehelseinstituttet og Statens legemiddelverk har ikke den totale oversikten over registrerte avvik knyttet til registrene

I henhold til forskrifter[71] til helseregisterloven skal den dataansvarlige ha kunnskap om gjeldende regler om behandling av helseopplysninger og tilstrekkelig og oppdatert dokumentasjon for gjennomføring av rutiner, i tillegg til å ha denne dokumentasjonen tilgjengelig for de som den måtte angå. Virksomhetene skal ha rutiner for hvordan avvik skal håndteres, og hvordan avvikene skal hindres i å gjenta seg.[72]

I henhold til kapittel 5.8.1 i normen skal virksomhetene behandle avvik for å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentakelse. Avviksbehandlingen skal dokumenteres. Avviksmeldinger som inneholder personopplysninger eller informasjon med betydning for informasjonssikkerheten, skal sikres. Virksomheten skal videre samle inn fakta om hendelsesforløpet for å iverksette korrigerende tiltak. Effekten av korrigerende tiltak skal vurderes, og eventuelle andre tiltak skal settes i verk ved behov.

Ved alvorlige eller gjentatte avvik skal det gjennomføres en ny risikovurdering.

Virksomhetene har retningslinjer og system for rapportering og håndtering av avvik internt, det varierer hvor mye systemene brukes

Alle tre virksomheter har rutinebeskrivelser og egne systemer for registrering og behandling av avviks- og forbedringsmeldinger. Rutinene beskriver at alle ansatte har ansvar for å melde avvik, slik at virksomhetene kan registrere og behandle avvikene for å hindre at samme feil gjentar seg.

Vår gjennomgang av mottatt dokumentasjon viser at avvikssystemene i registrene brukes ulikt. Statens legemiddelverk oppgir i et intervju[73] at avvikssystemet brukes ved vesentlige avvik. Folkehelseinstituttet oppgir i et intervju[74] at enkelte av helseregistrene har hatt for høy terskel for å melde avvik. Folkehelseinstituttet oppgir videre at det er planlagt e-læringskurs for å gi opplæring og øke forståelsen for hvorfor avviks- og forbedringsmeldinger skal meldes, og behandles. Det er ikke meldt noen avvik i forbedringssystemet for dødsårsaksregisteret i perioden 2020–2022. Tabellen viser antallet avvik som er meldt i det interne avvikssystemet i perioden 2020–2022 for de utvalgte registrene.

Helseregister	Antall avvik meldt i perioden 2020-2022
Dødsårsaksregisteret	0
Meldingssystem for smittsomme sykdommer	25
Kommunalt pasient- og brukerregister	10
Bivirkningsregisteret	4

[71] Dødsårsaksregisterforskriften, MSIS-forskriften.
[72] Dødsårsaksregisterforskriften, MSIS-forskriften.
[73] Verifisert referat fra møte med bivirkningsregisteret i Statens legemiddelverk 5. januar 2023.
[74] Verifisert referat fra møte med dødsårsaksregistret i Folkehelseinstituttet 26. januar 2023.

Vi har kontrollert virksomhetenes oversikt over innmeldte avvik for de utvalgte helseregistrene i perioden 2020–2022. I tillegg har vi kontrollert hvordan virksomhetene har analysert disse avvikene, og hvilke tiltak de eventuelt har truffet.[75]

For MSIS er det meldt 25 avvik i perioden 2020–2022. Avvikene går for eksempel ut på at helseopplysninger har kommet på avveie i forbindelse med mottak av meldinger, eller at Norsk helsenett har gitt saksbehandlere tilgang til sikker sone uten at det er bestilt eller avklart med Folkehelseinstituttet. Vi har mottatt dokumentasjon som viser at avvikene er vurdert og fulgt opp med tiltak. Enkelte av avvikene er fortsatt under behandling.

Det er meldt til sammen ti avvik som kan knyttes til KPR i Helsedirektoratets avvikssystem i perioden 2020–2022. Avvikene gjelder for eksempel at personopplysninger feilaktig er blitt eksponert, at data er blitt utlevert på tross av reservasjon mot dette, eller at det er utlevert for stort utvalg av data. Mottatt dokumentasjon viser at avvikene er analysert og fulgt opp med tiltak.

Statens legemiddelverk oppgir i et intervju[76] at avvikssystemet brukes ved vesentlige avvik. Dokumentasjon vi har mottatt, viser at det er meldt fire avvik ved bivirkningsregisteret i det interne avvikssystemet i perioden 2020–2022. Avvikene går ut på at det er tekniske svakheter som fører til at meldinger ikke mottas, at den sikre sonen er åpen mot Internett, eller at personopplysninger feilaktig er blitt eksponert. Avvikene er analysert og fulgt opp med tiltak. Et av tiltakene er fortsatt under arbeid.

Mindre feil og avvik (hendelser) rapporteres i leverandørenes avvikssystem

Av Folkehelseinstituttets årsrapport for 2022 fremgår det at mindre feil og avvik som regel rapporteres til Norsk helsenett og ikke fanges opp i den interne avviksrapporteringen. Norsk helsenett innførte et nytt saksbehandlingssystem i 2021, og i 2022 kom det på plass en mulighet for å merke feil og henvendelser som «sikkerhetshendelser». 30 slike hendelser ble rapportert til Norsk helsenett fra Folkehelseinstituttet i 2022.

Statens legemiddelverk oppgir i et intervju[77] at avvik som gjelder leverandøren, meldes i leverandørens avvikssystem. Statens legemiddelverk viser til at alle hendelser som gjelder bivirkningsregisteret, vil involvere en ekstern leverandør siden de hverken drifter IT-infrastruktur eller applikasjoner selv. Statens legemiddelverk følger derfor opp de ulike hendelsene sammen med de respektive leverandørene i leverandørenes servicedesksystemer.

6.1.2 Sikkerhetsarbeidet hos leverandøren som drifter infrastruktur for helseregistrene, følges ikke opp

Nasjonal sikkerhetsmyndighet har gitt ut sikkerhetsfaglige anbefalinger ved tjenesteutsetting (outsourcing). For at IKT-sikkerheten skal ivaretas ved tjenesteutsetting, anbefaler NSM at virksomheten er bevisst på behovet for

- oversikt og kontroll på hele livsløpet
- god bestillerkompetanse
- gode risikovurderinger for å kunne ta riktige beslutninger
- riktige og gode krav til IKT-tjenesten og til leverandøren
- riktig beslutning på riktig nivå

[75] Kommunalt pasient- og brukerregister, bivirkningsregisteret, meldingssystem for smittsomme sykdommer og dødsårsaksregisteret.
[76] Verifisert referat fra møte med bivirkningsregisteret i Statens legemiddelverk 5. januar 2023.
[77] Verifisert referat fra møte med bivirkningsregisteret i Statens legemiddelverk 5. januar 2023.

Nasjonal sikkerhetsmyndighet understreker «at grunnprinsippene for IKT-sikkerhet er like relevante for IKT-tjenester som er tjenesteutsatt, som for IKT-tjenester som forvaltes av virksomheten selv. Forskjellen er om man stiller krav til interne eller eksterne tjenesteleverandører».[78]

Eksempler på faktorer som Nasjonal sikkerhetsmyndighet mener vil kunne påvirke risikobildet, er at virksomhetene får mindre kontroll over stadig mer komplekse verdikjeder, at de taper intern kompetanse, og at de blir avhengig av eksterne tjenesteleverandør for å kunne levere tjenestene sine.

Revisjonen viser at virksomhetene ikke følger opp sikkerheten hos leverandørene:

- Kravene i avtalene er ikke tydelig avklart mellom virksomhetene og leverandørene.
- Virksomhetene har mangelfull oppfølging av om leverandørene etterlever de kravene som er avtalt.

Kravene i avtalene er ikke tydelig avklart mellom virksomhetene og leverandørene

Ifølge normen skal det ved levering av for eksempel tjenester, maskinvare eller systemer avtales skriftlig med leverandørene hvilke sikkerhetskrav som skal oppfylles. Gjennom en avtale skal virksomheten forsikre seg om at leverandøren har et tilfredsstillende styringssystem for sikkerhetsrevisjon og avviksbehandling. Virksomheten skal sikre klarhet i roller og ansvar og at kompetanseressurser deltar i anskaffelser og leverandørstyring. Den dataansvarlige kan bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak, slik at de oppfyller kravene i lov og forskrift.[79]

I 2017 ble alle virksomhetene i helseforvaltningen pålagt å bruke Norsk helsenett som felles tjenestesenter for arkiv, anskaffelser og IKT-tjenester.[80] Helsedirektoratet og Folkehelseinstituttet benytter Norsk helsenett som leverandør av datainfrastruktur. Statens legemiddelverk har en databehandleravtale med Advania om drift av IT-systemene, som forvaltes av Norsk helsenett. I 2017 inngikk Statens legemiddelverk en avtale med Norsk helsenett med intensjon om at Norsk helsenett skulle overta driften fra Advania. Foreløpig har Norsk helsenett valgt å forlenge avtalen med Advania som driftsleverandør for Statens legemiddelverk.

Helse- og omsorgsdepartementet oppgir i et intervju at den overordnede målsettingen med å opprette et felles tjenestesenter var effektivisering og tilrettelegging for større og sterkere kompetansemiljøer. I forbindelse med opprettelsen av senteret ble det overført ressurser fra virksomhetene til Norsk helsenett. Departementet var tydelig på at virksomhetene selv måtte vurdere kompetansebehovet i sin egen virksomhet i forbindelse med at ressursene ble overført. Helse- og omsorgsdepartementet oppgir videre at det tok tid før virksomhetene forsto rekkevidden av sitt eget ansvar overfor leverandøren.[81]

Avtalene mellom virksomhetene og Norsk helsenett inneholder overordnede føringer om at databehandlerens oppgaver skal være i henhold til normen. Dokumentanalysen viser at føringene er omfattende og generelle, og formuleringer rundt tekniske sikkerhetsmessige krav er ikke direkte avstemt mot normens krav.[82] Videre er det eksempler på at virksomhetenes interne policyer og instrukser som har betydning for informasjonssikkerheten, inneholder føringer og prinsipper som ikke nødvendigvis inngår i avtalene som forplikter leverandørene.

Videre viser dokumentanalysen av databehandleravtalene og vedleggene til dem at det er ulikt hvor tydelige krav virksomhetene stiller til sikkerhet. Det er ingen standardisering av krav som benyttes i

[78] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/bruk-av-tjenesteutsetting-og-skytjenester/.
[79] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.
[80] Tildelingsbrevene til Helsedirektoratet, Folkehelseinstituttet og Statens legemiddelverk for 2017.
[81] Verifisert referat fra intervju med Helse- og omsorgsdepartementet 15. mars 2023.
[82] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 5.7.3.

databehandleravtalene om helseregistre i sektoren. Dokumentanalysen viser at Helsedirektoratets og Folkehelseinstituttets avtaler med Norsk helsenett er svært ulike.

Statens legemiddelverk og Helsedirektoratet har utdypet krav i vedlegg til databehandleravtalene med Advania og Norsk helsenett. Folkehelseinstituttet opplyste i et intervju at de ikke har stilt spesifikke krav i avtalen, da forutsetningen var at de som driftet systemene internt før ressursene ble overført, fortsatt skulle drifte dem på samme måte etter at de ble overført til Norsk helsenett.[83]

Ved de tekniske tiltakene som er undersøkt i denne revisjonen[84], er det avdekket at leverandørene ikke alltid følger beste praksis og kravene i normen, og de følger heller ikke alle kravene som er stilt i avtalene. Flere av disse svakhetene var ikke virksomhetene kjent med. Som tilbakemelding på funnene oppgir Statens legemiddelverk at de stiller seg undrende til å måtte «*fortelle IT- tilbyder i detalj hvordan de skal utføre grunnleggende beste praksis*»[85] når tilbyderen er ISO-sertifisert.

Mangelfull oppfølging av om leverandør etterlever de kravene som er avtalt

Virksomhetene har selv ansvaret for informasjonssikkerheten selv om systemene driftes av andre.[86] Derfor må virksomhetene gjøre vurderinger av informasjonssikkerheten selv om IKT-infrastruktur og IKT-tjenester er satt ut til eksterne leverandører.[87]

Ifølge normen skal virksomhetens ledelse følge opp at sikkerheten ivaretas ved jevnlige sikkerhetsrevisjoner som skal foretas minst årlig. Dette inkluderer å gå gjennom dokumentasjon på at databehandlere og leverandører ivaretar informasjonssikkerheten.[88]

Sikkerhetsrevisjon

Hensikten er å kontrollere at det er gjennomført nødvendige sikkerhetstiltak i tråd med gjennomførte risikovurderinger, vurdere om sikkerhetstiltakene er tilstrekkelige, kontrollere at lover og regler om informasjonssikkerhet følges, og sikre at etablerte prosedyrer for sikkerhet benyttes og fungerer etter hensikten.

I avtalene virksomhetene har med leverandørene, er det åpnet for innsyn i de prosessene og rutinene som gjelder kunden, samt revisjoner av leverandøren, uten at dette er fullt ut utnyttet av virksomhetene.

Vår dokumentanalyse og intervju med virksomhetene viser at ingen av dem systematisk følger opp at leverandøren etterlever de sikkerhetskravene som er stilt i avtalene. Ingen av de tre virksomhetene har gjennomført sikkerhetsrevisjoner av leverandøren, noe som er anbefalt i normen, og som avtalene åpner for. Virksomhetene har i liten grad etterspurt dokumentasjon fra leverandøren, og de har i liten grad mottatt slik dokumentasjon når de har etterspurt den. Norsk helsenett opplyser for øvrig på sine nettsider at de som en del av sitt arbeid med sikkerhet og personvern gjennomfører «*årlig revisjon og internkontroll av våre produkter og tjenester, samt årlig revisjon av utvalgte områder der det er særlig behov for å måle etterlevelse av kravene i styringssystemet*».[89]

[83] Verifisert referat fra intervju med Folkehelseinstituttet 26. januar 2023.
[84] Se kapittel 6.1.3, 6.1.4 og 6.1.5.
[85] Svar fra Statens legemiddelverk 24. mars 23. D – spørsmål – databaser.
[86] Helseregisterloven § 21 og artikkel 32 i personvernforordningen.
[87] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet-2-0/introduksjon-1/bruk-av-tjenesteutsetting-og-skytjenester/.
[88] Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren, kapittel 5.4.6.
[89] https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/sikkerhetsarbeid-internt-i-norsk-helsenett/revisjon.

Alle virksomhetene har gjennomført penetrasjonstest av sikker sone[90] ved hjelp av eksterne leverandører.

Alle de tre virksomhetene har jevnlige driftsmøter med leverandørene hvor det utarbeides agenda og skrives referat. Eksempler på agendaer og referat fra denne typen møter viser at temaene i hovedsak er utfordringer og forbedringer rundt den daglige driften av systemene. Fra driftsmøtene foreligger det lite dokumentasjon som viser at virksomhetene følger med på om leverandørene av datainfrastrukturen – Norsk helsenett og Advania – forvalter systemene og sikkerheten i henhold til de kravene som er stilt i avtalene. Det er heller ikke dokumentert at risikovurderinger og endringer i risikobildet er tema i disse møtene.

Virksomhetene har taktiske møter med leverandøren på sikkerhetsområdet, som ikke er rettet mot helseregistrene spesifikt, men mot Norsk helsenett SF (NHN) som leverandør av tjenester generelt. Helsedirektoratet har ettersendt referat fra slike møter, som viser at risiko og sikkerhet hos leverandøren har vært fulgt opp på overordnet nivå.

Statens legemiddelverk uttaler at de ikke kan se at Advania og Norsk helsenett har etterlevd pliktene i driftsavtalen. Dette gjelder flere punkter om informasjonssikkerhet og personvern, og Statens legemiddelverk har heller ikke påsett at pliktene er blitt etterlevd.[91] Fra 1. januar 2017 og frem til i dag er det altså ikke blitt fulgt opp om Advania har etterlevd driftsavtalen.

6.2 Informasjonssikkerhetstiltak

I henhold til helseregisterloven § 21 og artikkel 32 i personvernforordningen skal den dataansvarlige og databehandleren gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Ved vurderingen av hva som er et egnet sikkerhetsnivå, skal de særlig ta hensyn til risikoene forbundet med behandlingen, dette gjelder særlig risikoene for utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.[92]

For å kontrollere om virksomhetene har gjennomført informasjonssikkerhetstiltak, har vi analysert de følgende tiltakene:

- tilgangsstyring, jf. kapittel 6.2.1
- sikkerhetskonfigurasjon og gjennomføring av sikkerhetsoppdateringer, jf. kapittel 6.2.2
- logging, jf. kapittel 6.2.3

[90] Defandable for Statens legemiddelverk 21. oktober 2022, Helsecert for Folkehelseinstituttet 27. mars 2020 og Mnemonic for Helsedirektoratet 13. desember 2021.
[91] Statens legemiddelverks svar på spørsmålsliste A Leverandørstyring.
[92] Artikkel 32 i personvernforordningen.

Hovedfunn

Viktige informasjonssikkerhetstiltak hos leverandørene er ikke er implementert, eller fungerer ikke etter hensikten. Virksomhetenes manglende oppfølging av tilganger, sikkerhetsinnstillinger og logging kan medføre at det finnes sårbarheter i systemene som virksomhetene ikke er kjent med.

- Tilgangsstyringen er mangelfull, og leverandørene har omfattende tilganger.
- Vedlikeholdet av sikkerhetskonfigurasjon og gjennomføringen av sikkerhetsoppdateringer er varierende.
- Loggingen på servere og databaser er mangelfull.

6.2.1 Tilgangsstyringen er mangelfull, og leverandørene har omfattende tilganger

God kontroll på tilganger er viktig for å sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Tilgangsstyring omfatter rutiner for autorisering, endring og avslutning av tilganger, dokumentasjon av autorisasjonen i et autorisasjonsregister og kontroll av tilgangene.[93]

Helseregisterloven § 21 sier at den dataansvarlige og databehandleren blant annet skal sørge for tilgangsstyring, logging og etterfølgende kontroll. Normen anbefaler virksomhetene å sikre at uvedkommende ikke får kjennskap til helse- og personopplysninger eller informasjon med betydning for informasjonssikkerheten, og uvedkommende skal heller ikke ha mulighet til å endre slike opplysninger.[94]

Bruk av administratorkontoer bør begrenses til minimum, det bør benyttes ulike kontoer til forskjellige driftsoppgaver, og kontoer som ikke er blitt benyttet på lenge, bør følges opp.[95]

Revisjonen viser at virksomhetene ikke har god nok kontroll på tilganger:

- Prinsipper for tilgangsstyring er definert, men gjennomføres ikke som beskrevet.
- Autorisasjonsregistre mangler eller er mangelfulle.
- Leverandørene har omfattende administratorrettigheter i systemene.

En angriper har ofte til hensikt å få tilgang til en konto for å få ytterligere tilgangsrettigheter eller ta over andre kontoer med utvidede rettigheter for å ta seg lenger inn i et IKT-system og få tilgang til flere ressurser.[96]

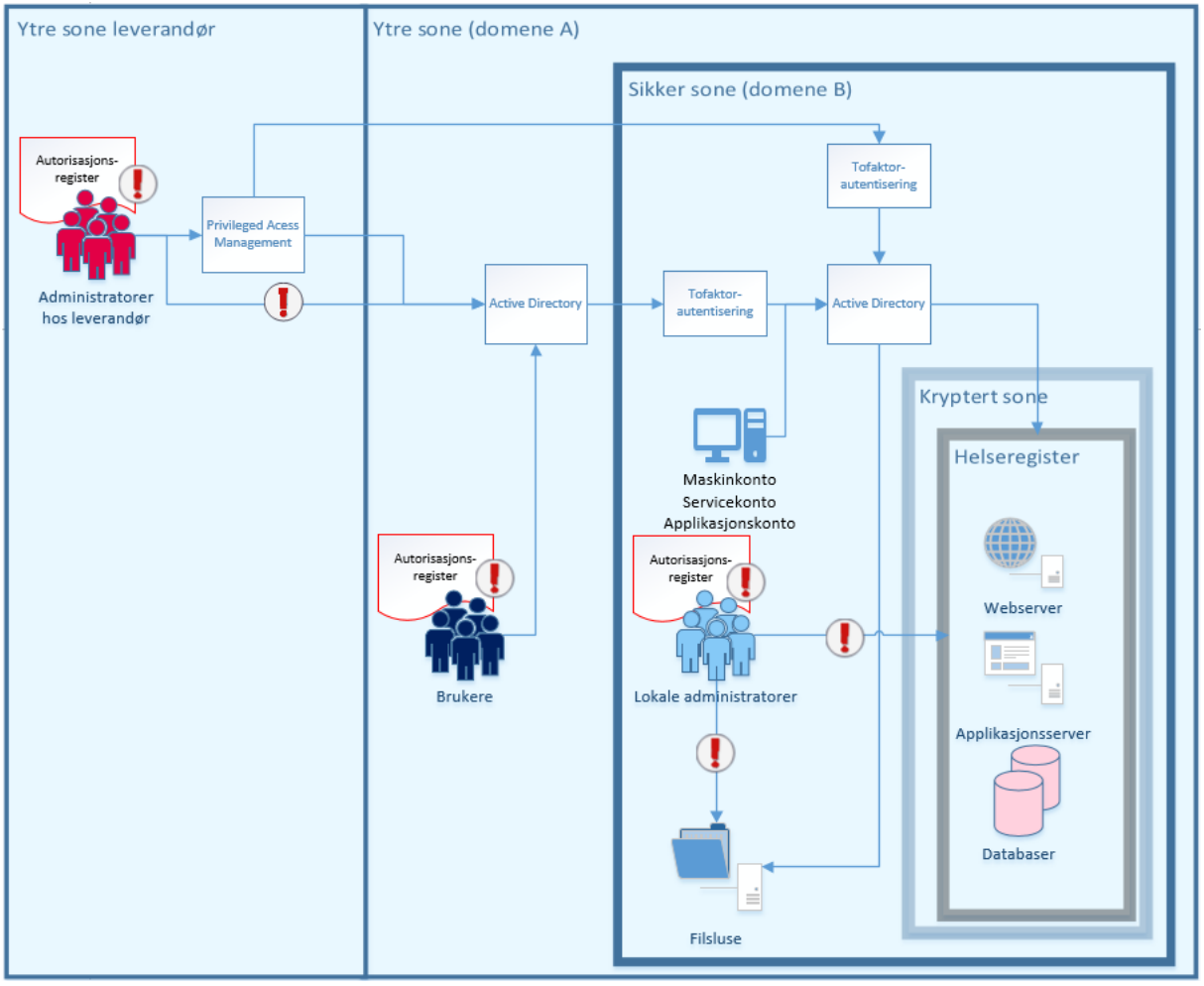
Ifølge Nasjonal sikkerhetsmyndighet bør virksomhetene dele opp rettighetene til de ulike delene av et informasjonssystem for å redusere eventuell skade fra et eksternt angrep, en utro eller en uvøren ansatt. Kontoer som er blitt gjort inaktive uten at rettighetene er fjernet, utgjør også en risiko ved at de kan bli misbrukt av en angriper eller utro tjener.

Figur 7 viser hvordan de ulike brukergruppene har tilgang til helseregistrene og den underliggende infrastrukturen. Utropstegnene viser hvor det er svakheter i tilgangsstyringen. Alle brukere som skal

[93] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.2.
[94] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 3.2.
[95] NSMs grunnprinsipper for IKT-sikkerhet kapittel 2.6.
[96] NSMs grunnprinsipper for IKT-sikkerhet kapittel 2.6.

logge seg på sikker sone i virksomhetene, må enten gjennom ytre sone hos virksomheten eller gjennom leverandørens egen sone. Ytre sone er altså en del av sikkerhetsarkitekturen.

Figur 7 Forenklet skisse over tilgang til helseregistrene og underliggende infrastruktur



Kilde: Riksrevisjonen, basert på informasjon fra Folkehelseinstituttet, Helsedirektoratet og Statens legemiddelverk

Prinsipper og prosesser for tilgangsstyring er definert

Normen anbefaler at virksomheten har rutiner for autorisering, endring og avslutning av tilganger. Det bør etableres tilgangsstyring for alle informasjonssystemer, og tilgangsstyringen bør også gjelde for administrator- og systembrukere. Bare autorisert personell med tjenstlige behov bør få tilgang til helse- og personopplysninger.[97] Ifølge Nasjonal sikkerhetsmyndighet bør rutinene følge minste privilegiums prinsipp, og upersonlige kontoer bør unngås.[98]

Minste privilegiums prinsipp

Hensikten med å styre tilgangen til servere, applikasjoner eller data er å hindre at personer uten tjenstlig behov får tilgang. Det skal ikke gis mer omfattende tilgang enn det som strengt tatt er nødvendig for å ivareta en funksjon eller gi tilgang til funksjonalitet eller informasjon.

[97] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.2.
[98] NSMs grunnprinsipper for IKT-sikkerhet, kapittel 2.6.

Virksomheten er ansvarlig for å tildele, administrere og kontrollere autorisasjoner til helseregistre, og virksomheten skal registrere opplysningene i et autorisasjonsregister.[99] Videre anbefaler normen at virksomhetens ledelse påser at tilgangsstyringen og de tildelte autorisasjonene kontrolleres jevnlig.[100]

I registre som er opprettet med hjemmel i helseregisterloven §§ 10 og 11, skal direkte personidentifiserende kjennetegn lagres kryptert.[101]

Dokumentanalysen viser at alle virksomhetene har beskrevet overordnede prinsipper og krav til tilgangsstyring. Prinsippene og kravene fremgår av ulike styrende dokumenter om policy, retningslinjer og lignende eller av avtaler med leverandøren og dokumenter som viser virksomhetens krav til sikkerhetstiltak. Til sammen dekker disse prinsippene og kravene anbefalingene om autorisering, tjenstlig behov, endring, avslutning og regelmessig kontroll av tilgang for både virksomhetenes egne ansatte og ansatte hos leverandøren. Analyser av faktisk tildelte rettigheter i nettverket, i applikasjoner, i databaser og på servere viser imidlertid at tilgangsstyringen ikke alltid fungerer i praksis, jf. delkapitlene om autorisasjonsregister og administratorrettigheter nedenfor.

Dokumentanalyse og intervjuer med virksomhetene viser at alle tre de virksomhetene i stor grad har opprettet aktiviteter som sikrer at virksomhetens egne ansatte får tildelt rettigheter ut fra hvilke oppgaver de utfører, og at brukerkontoer blir fjernet eller deaktivert når den ansatte slutter eller har langvarig fravær. Alle tre virksomheter utfører jevnlige kontroller av tilganger til systemene.

Virksomhetene kontrollerer at brukerne har fått riktige rettigheter, og følger opp at personidentifiserende opplysninger bare blir dekryptert dersom det er nødvendig. De personidentifiserende opplysningene i registrene er kryptert på databasenivå og kan kun dekrypteres gjennom bruk av applikasjonene. Ingen av de tre registrene viser personopplysninger med mindre saksbehandleren aktivt velger å dekryptere opplysningene. Systemet logger denne aktiviteten, og saksbehandleren må registrere årsaken til dekryptering i loggen. Alle de tre virksomhetene følger opp loggene regelmessig.

Alle tre virksomheter går jevnlig gjennom tilgangsrettighetene i applikasjonene som benyttes til saksbehandling i registrene. Vår analyse av uttrekk av tildelte rettigheter i registrene og dokumentasjon av gjennomførte kontroller viser at kontrollene bidrar til å sikre at rettighetene er godkjent og gitt i henhold til tjenstlig behov.

Virksomhetenes tilgangsstyring omfatter imidlertid ikke driftsleverandørens tilganger til infrastrukturen. Det er leverandørene selv som administrerer den tilgangen deres egne ansatte har til kundenes systemer. Norsk helsenett har utarbeidet en rutine for tilgangsstyring som gjelder tilgang til Folkehelseinstituttets og Helsedirektoratets systemer. Legemiddelverket opplyser at det ikke er utarbeidet retningslinjer eller prosedyrer for tildeling av rettigheter til grupper som gir administratorprivilegier, ut over at prinsippene for tilgangsstyring er formidlet til leverandørene av IT-tjenestene. Basert på resultatene fra våre analyser av hvilke rettigheter som er tildelt leverandørens ansatte, kommenterer Statens legemiddelverk at det burde vært bedre skriftlige prosedyrer for dette og mer systematisk kontroll av hvilke tilganger som er tildelt.[102]

For å kontrollere om virksomhetenes rutiner for tilgangsstyring fungerer, slik at risikoen for at noen kan oppnå uautorisert tilgang er håndtert, har vi analysert rettighetene til de utvalgte registrene. Vi har analysert rettigheter i applikasjoner og utvalgte deler av den underliggende infrastrukturen som nettverk (Active Directory – AD)[103], databaser og servere.

[99] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.2.1.
[100] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.2.3.
[101] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.3.5.
[102] Svar fra Statens legemiddelverk 24.03.23 B – Active Directory – spørsmål.
[103] Se faktaboks 4.

Autorisasjonsregistre mangler eller er mangelfulle

Dokumentanalysen vår viser at alle tre virksomheter har interne krav om at rettigheter skal autoriseres ved godkjenning fra leder eller dataansvarlig, og at godkjenningen skal dokumenteres. Normen anbefaler at autorisasjonsregistret som et minimum inneholder hvem som er tildelt autorisasjon, hvilken rolle som er tildelt, formålet med autorisasjonen og tidspunktet når autorisasjonene er gitt og eventuelt trukket tilbake.[104]

Statens legemiddelverk opplyser at det ikke er opprettet et autorisasjonsregister for tilgang til bivirkningsregisteret.[105] Det er heller ikke opprettet et autorisasjonsregister over leverandørens rettigheter i systemene til Statens legemiddelverk. Brukerkontoene kan bare bestilles og godkjennes av ansatte i IT-enheten i Statens legemiddelverk.

Helsedirektoratet har gitt Norsk helsenett i oppdrag å vedlikeholde autorisasjonsregistret for kommunalt pasientregister. Autorisasjonsregistret mangler informasjon om sluttdato, slik at mange brukere står som aktive i autorisasjonsregistret, men er deaktivert i AD. Norsk helsenett opplyser at sluttdatoen vil fremgå av saksbehandlingssystemet for tilgangsstyringen, og derfor oppdateres ikke sluttdatoen i autorisasjonsregistret. Våre stikkprøver av tildelte rettigheter i systemet viser at det er avvik mellom autorisasjonsregistret og faktiske tilganger. Norsk helsenett har også utarbeidet autorisasjonsregister som skal vise hvilke av de ansatte i Norsk helsenett som er autorisert til hvilke rettigheter i sikker sone. Mottatt autorisasjonsregister synes ikke å være oppdatert, da det bare er dokumentert autorisasjoner for én PAM-gruppe (PAM = Privileged Access Management), og listen over hvem som er autorisert, ikke fullt ut samsvarer med de rettighetene som er gitt i denne PAM-gruppen. Datoen for når rettighetene opphører, er ikke registrert i autorisasjonsregistret. Vi har ikke mottatt noe autorisasjonsregister for ytre sone. PAM er nærmere beskrevet i avsnittet «Leverandørene har omfattende administratorrettigheter i systemene» nedenfor. I forbindelse med Helse- og omsorgsdepartementets uttalelse til utkast til rapport opplyser Norsk helsenett[106] at det kan se ut som at ikke alle relevante autorisasjonsregister for Helsedirektoratet sine helseregistre er oversendt Riksrevisjonen, og at sammenstillingen og avvik mellom autorisasjonsregister og faktiske tilganger derfor ikke trenger å være korrekt. Norsk helsenett har ikke oversendt de nevnte autorisasjonsregistre som kunne ha vist at det ikke er avvik. Riksrevisjonen har derfor ikke grunnlag for å endre ordlyden i rapporten.

Folkehelseinstituttet vedlikeholder oversiktene over autorisasjoner som gir tilgang til meldingssystemet for smittsomme sykdommer og dødsårsaksregisteret. Autorisasjonsregistret for MSIS oppfyller normens minimumskrav til dokumentasjon. Autorisasjonsregisteret for DÅR inneholder bare navn, rolle og domene og oppfyller ikke normens minimumskrav. Norsk helsenett skal føre et autorisasjonsregister over egne PAM-brukere, men opplyser at registeret ved en feil ikke er blitt oppdatert. Driftsansvarlig og nærmeste leder bekrefter og godkjenner tilgang for PAM-grupper.

Leverandørene har omfattende administratorrettigheter i systemene

Hvis alle brukere har rettigheter til «alt», vil kompromittering av én bruker kunne kompromittere hele IKT-systemet. Rettighetene til de ulike delene av et informasjonssystem bør derfor deles opp, slik at man reduserer skaden fra et eksternt angrep eller fra en utro eller uvøren ansatt.[107] Nasjonal sikkerhetsmyndighet anbefaler at retningslinjene for tilgangskontroll dekker flest mulig av ressursene i virksomheten: brukere, klienter, felles-mapper, server-applikasjoner, servere, nettverksenheter, sikkerhetsenheter og databaser. Videre bør tilgangskontrollen følge minste privilegiums prinsipp: Ikke gi sluttbrukere, servicekontoer, utviklere eller driftsbrukere flere privilegier enn nødvendig. Videre fremhever Nasjonal sikkerhetsmyndighet at det er spesielt viktig å revidere kontoer, tilganger og

[104] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.2.1.
[105] Svar fra Statens legemiddelverk 24. mars C – applikasjon – spørsmål.
[106] Norsk helsenetts tilbakemeldinger på Riksrevisjonens Utkast til rapport 4. juli 2023
[107] NSMs grunnprinsipper for IKT-sikkerhet kapittel 2.6.

rettigheter for drift og spesialbrukere jevnlig.[108] Microsoft anbefaler at de innebygde administratorgruppene i AD ikke inneholder andre brukere enn den innebygde administratorbrukeren, og at denne er forbeholdt bruk i beredskapssituasjoner.[109]

Uttrekk av brukere og rettigheter fra virksomhetenes systemer viser at tilganger og rettigheter som brukes til drift av infrastrukturen, er omfattende og involverer mange brukere hos leverandørene.

Mange brukere har administratorrettigheter som gir utvidet tilgang til å administrere domenet (AD), servere og databaser. Der brukere og kontoer ikke er angitt særskilt i funnene videre i rapporten, inkluderer funnene både personlige og upersonlige administratorkontoer og maskin-, service- og applikasjonskontoer i oppsummeringen av administratorbrukere.

Leverandørene har et høyt antall brukere med administratorrettigheter i AD, noe som gir tilgang til alle maskiner i nettverket

I alle de tre virksomhetene administreres AD av leverandøren (Norsk helsenett og Advania). Norsk helsenett har innført «Privileged Access Management» (PAM) for pålogging til kundenes systemer når de ansatte i Norsk helsenett skal gjennomføre driftsoppgaver. Den ansatte benytter sin AD-konto i Norsk helsenetts domene til å logge på PAM. I PAM er det opprettet ulike grupper som gir tilgang til bestemte kontoer med tildelte rettigheter i kundens AD-domene. Hvilke Norsk helsenett-kontoer (ansatte) som har tilgang til hvilke av kundens kontoer, kan leses ut av gruppemedlemsskap i PAM-systemet. Advania benytter foreløpig ikke PAM, men har egne kontoer i kundens AD-domene og logger på direkte for å gjennomføre driftsoppgaver.

Faktaboks 4 Generelt om Active Directory og PAM

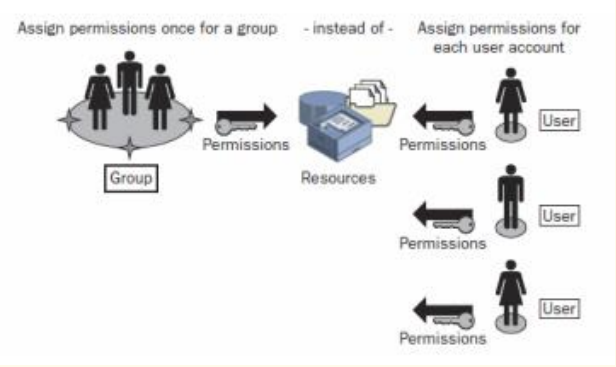
Active Directory (AD) er en sentralisert database som brukes av Microsoft Windows-operativsystemer til å lagre og administrere informasjon om nettverksressurser som datamaskiner, brukerkontoer og tilgangsgrupper på tvers av nettverket.

Et nettverk kan deles inn i domener, og hvert domene er et administrativt avgrenset område i nettverket som administreres gjennom en domenekontroller (serveren hvor AD er installert). Eksempler på domener fremgår av figur 8, der ytre sone er ett domene og sikker sone et annet.

En person trenger en brukerkonto i domenet for å få tilgang til maskiner og systemer, alt etter hvilke rettigheter som er tildelt brukerkontoen. Brukernavn og passord blir sendt via nettverket til domenekontrolleren, som kontrollerer brukernavnet og passordet mot den sentrale brukerkatalogen (autentisering).

Hvis flere brukere skal ha de samme rettighetene, kan brukerkontoene samles i en gruppe.

AD har noen innebygde grupper med standard administratorrettigheter som gir medlemmene omfattende rettigheter i hele domenet.



Det kan også angis en gruppepolicy (Group Policy Objects – GPO) på domenekontrolleren som definerer flere parametere for operativsystemet, brukerne, applikasjonene og så videre. Parameterne styrer hvordan systemet oppfører seg, og gir mulighet for å angi forskjellige sikkerhetsinnstillinger, blant annet for brukerkontoer og nettverk.

[108] NSMs grunnprinsipper for IKT-sikkerhet kapittel 2.6.1.
[109] Appendix B - Privileged Accounts and Groups in Active Directory | Microsoft Learn.

Privileged Access Management (PAM) er en identitetssikkerhetsløsning som bidrar til å beskytte en organisasjon mot cybertrusler ved å overvåke, oppdage og forhindre uautorisert privilegert tilgang til viktige ressurser. En PAM-løsning kan støtte ulike sikkerhetsmekanismer som automatisert passordadministrasjon og -rotasjon, flerfaktorautentisering og overvåking av aktiviteter.

Kilde: www.windowsnett.no, Microsoft[110] og Riksrevisjonen 2023

Analyse av uttrekk fra AD i Statens legemiddelverk viser at det finnes over 150 ulike AD-kontoer i standard administratorgrupper i brukerdomenet (ytre sone). Av disse er det flere systembrukere og upersonlige kontoer, og en del er deaktivert. I produksjonsdomenet (sikker sone) er det 17 brukere i standard administratorgrupper. På våre spørsmål om bruken av disse gruppene svarer Statens legemiddelverk at Advania har kommet med forslag til forbedringer, blant annet å innføre PAM-løsningen og rydde opp i AD.[111]

Analyse av uttrekk fra AD og PAM for Folkehelseinstituttet viser at Norsk helsenett har opprettet to PAM-brukere med standard administratorrettigheter. Norsk helsenett opplyser at det nylig er innført en funksjon i PAM som krever at det må være involvert to ansatte i bruken av PAM-kontoene med de videste rettighetene. For øvrig er det mange Norsk helsenett-brukere som har tilgang til Folkehelseinstituttets systemer. For eksempel er det opprettet 41 ulike PAM-grupper med til sammen 170 ulike Norsk helsenett-brukere som er tilknyttet disse systemene i sikker sone. I Norsk helsenetts innspill[112] til Helse- og omsorgsdepartementet i forbindelse med utkast til rapport framgår det at Norsk helsenett mener antallet brukere er feil fremstilling og tatt ut av sammenheng. De fremhever at Norsk helsenett drifter en stor IKT-portefølje for Folkehelseinstituttet. Dette inkluderer brukerstøttefunksjoner, skrivere, arbeidsflater og andre kontorstøttetjenester. Norsk helsenett sine ansatte gis tilgang til PAM-grupper ut fra sine spesialistområder.

Norsk helsenett har ikke ryddet opp i AD-kontoer som ikke er i bruk etter at PAM ble innført. I uttrekkene finnes det også PAM-grupper som ikke er tilknyttet en AD-bruker i Folkehelseinstituttets domene, og som dermed ikke har noen funksjon.

Analyse av uttrekk fra AD og PAM-grupper for Helsedirektoratet viser at antallet Norsk helsenett-brukere med tilgang til direktoratets systemer er betydelig mindre i sikker sone enn i ytre sone. Det er opprettet 35 PAM-grupper med til sammen 63 Norsk helsenett-kontoer i sikker sone, mens det i ytre sone er opprettet 71 PAM-grupper med til sammen 193 Norsk helsenett-brukere.

Norsk helsenett har ryddet i PAM-grupper i sikker sone uten å deaktivere AD-kontoer som ikke lenger er i bruk, eller fjerne rettighetene. Det finnes også PAM-grupper som ikke har noen funksjon, ved at de ikke er tilknyttet en tilsvarende AD-bruker. Norsk helsenett opplyser at tilganger til de ulike seksjonene i Norsk helsenett skal revideres minst en gang i året, med særlig vekt på privilegerte tilganger.

[110] Hva er Privileged Access Management (PAM) | Microsoft Sikkerhet.
[111] Svar fra Statens legemiddelverk 24. mars 2023 C – applikasjon – spørsmål.
[112] Norsk helsenetts tilbakemeldinger på Riksrevisjonens Utkast til rapport 4. juli 2023

Leverandørene har et høyt antall brukere med administratorrettigheter på servere som understøtter helseregistrene

Lokal administrator på en server

En bruker som er tildelt rettighet til den lokale gruppen «Administratorer» på en server, er lokal administrator på denne serveren. Dette gir brukeren full kontroll over serveren. Blant annet får brukeren mulighet til å endre sikkerhetsoppsett og passordoppsett og legge til og fjerne brukere.

En konto med lokale administratorrettigheter kan være en upersonlig konto som brukes av en tjeneste eller applikasjon til automatiserte og planlagte oppgaver på servere. Dette kan for eksempel gjelde sikkerhetskopiering og innlasting av data.

Analyse av uttrekk fra Folkehelseinstituttets servere viser at antall unike administratorkontoer, inklusive servicekontoer, varierer fra 43 til 78. Den samme brukerkontoen kan ha fått tildelt rettigheter til samme server gjennom flere ulike gruppemedlemskap.

Folkehelseinstituttet kommenterer at dette er mange administratorer.[113] De ønsker ikke å gjenbruke servicekontoer med administratorrettigheter i flere systemer på én gang dersom det ikke er særskilt gode grunner for dette. Videre jobber Norsk helsenett i driftsteam og ønsker at hele driftsteamet skal ha tilgang. Folkehelseinstituttet opplyser at de vil be Norsk helsenett gjennomgå tilganger og vurdere om tilgangene er gitt ut fra tjenstlig behov.

Analyse av uttrekk fra Statens legemiddelverks domenekontroller i ytre sone viser at det er ca. 150 unike administratorkontoer som har fått tildelt lokal administratortilgang gjennom standard administratorgrupper i AD, jf. delkapittelet ovenfor om leverandørens utvidede rettigheter gjennom Active Directory. På domenekontroller og utvalgte servere i sikker sone er antallet unike administratorer ca. 30. Advania opplyser at «visse kontoer» har behov for administratortilgang, men at en opprydding er å anbefale.

Analyse av uttrekk av lokale administratorer på en server i ytre sone hos Helsedirektoratet viser at ca. 50 unike administratorkontoer har tilgang gjennom standard administratorgrupper i AD, jf. delkapittelet ovenfor om leverandørens utvidede rettigheter gjennom Active Directory. Helsedirektoratet opplyser at servere i sikker sone der registeret ligger, bare skal være tilgjengelige for et fåtall personer med lokale administratorrettigheter basert på tjenstlig behov. Behovet vurderes og godkjennes av nærmeste leder i hvert enkelt tilfelle, etter standard rutine for tilgangsstyring. Analyse av uttrekk fra utvalgte servere i sikker sone viser at antallet unike aktive administratorer varierer fra ca. 10 til 25.

Leverandørene har et høyt antall brukere med administratorrettigheter til databasene

Databaseinstans

En databaseinstans er et databasesystem som kan administrere flere ulike databaser og bestå av én eller flere databaser. En rettighet til databaseinstansen vil gi brukeren mulighet til å administrere alle databasene i den aktuelle instansen. Dette innebærer for eksempel å kunne endre brukeres rettigheter i de ulike databasene, å kunne endre data i databasene og å kunne endre ulike innstillinger som passordkrav og logging.

Analyse av uttrekk fra Folkehelseinstituttets databaseinstans viser at ca. 40 unike brukere har administratorrettigheter, og dette er i hovedsak brukere hos Norsk helsenett. Folkehelseinstituttet kommenterer at de er overrasket over det høye antallet og ser at det må ryddes i gitte tilganger. De tre databasene som utgjør helseregistret, ligger i samme databaseinstans som ca. 100 andre databaser

[113] Svar fra Folkehelseinstituttet 17. april 2023. E – servere lokal admin – spørsmål.

med andre funksjoner. Disse ca. 40 unike brukerne med administratorkonto til databaseinstansen har dermed også utvidet tilgang til de nevnte 100 databasene.

Uttrekk av lokale administratorer for databasene til Folkehelseinstituttet viser at de har færre brukere og mindre omfattende rettigheter, men det forekommer enkelte tilfeller hvor brukere har sluttet uten at rettighetene deres er fjernet. Videre finnes det roller med rettigheter som ikke er blitt fjernet selv om de er opprettet for midlertidig bruk.

Statens legemiddelverk har tre ulike databasesystemer (databasetyper). Uttrekk fra et av databasesystemene viser at det er ca. 70 unike brukere med administratorrettigheter på databaseinstansen. Alle brukerne er knyttet til Advania eller applikasjonsleverandøren.

I de to andre databasesystemene hos Statens legemiddelverk har databaseinstansene kun upersonlige administratorkontoer. Statens legemiddelverk er kritisk til at det benyttes administratorkontoer som ikke er personlige. Legemiddelverket mener at Advania må kunne oppfylle informasjonssikkerhetskravene i sitt eget styringssystem og beste praksis når de håndterer

administratorkontoer på Legemiddelverkets vegne ettersom Advania er en IT-tilbyder som er sertifisert

i henhold til ISO 27001/2.[114]

Helsedirektoratet har to databaseinstanser med ca. 75 databaser til sammen, inkludert de tre databasene som gjelder KPR. Brukere som har en administratorkonto til databaseinstansen, har utvidet tilgang til alle de 75 databasene. Uttrekk fra databaseinstansene viser at det totalt er ca. 30 unike brukere som har fulle administratorrettigheter til de to databaseinstansene. Noen av brukerne er deaktivert, men ikke fjernet fra tilgangsgruppen.

I Helsedirektoratet er også en annen rolle med utvidede rettigheter i bruk i databasene. Denne gir tilgang til å hente ut og legge inn data direkte i databasen. Analyse av uttrekk fra databasen viser at rollen er tildelt ca. 160 brukerkontoer i de to databaseinstansene. Helsedirektoratet opplyser at alle brukerne har tjenstlig behov og bare får tilgang til den databasen de skal ha rettigheter til.

Svakheter i administrasjon av tilganger til mapper på filsluser

En filsluse er en teknisk løsning for å utveksle filer og datasett mellom ulike nettverkssoner på en sikker måte, for eksempel fra helsenettet til en ekstern forskningsbruker. På filslusene opprettes det mapper som kun er tilgjengelige for én person, slik at man reduserer antallet brukere som har tilgang til de ulike datasettene.

Norsk helsenett har satt opp filsluser for Folkehelseinstituttet og Helsedirektoratet for blant annet utlevering av data fra dødsårsaksregisteret, meldingssystemet for smittsomme sykdommer og kommunalt pasientregister. Statens legemiddelverk benytter ikke denne løsningen til overføring av filer og datasett.

Uttrekk av tilgangsrettigheter til filslusene hos Folkehelseinstituttet viser at ca. 40 brukere har tilgang til de personlige mappene på filslusene gjennom gruppemedlemskap i AD eller PAM. Videre viser uttrekket at mange brukere er slettet fra AD uten at brukeren har mistet tilgangsrettigheten til filslusen.

Uttrekk av tilgangsrettigheter på filslusene hos Helsedirektoratet viser at ca. 60 brukere har tilgang til de personlige mappene.

[114] Svar på skriftlige spørsmål fra Statens legemiddelverk 24. mars 2023.

Oppsummert viser revisjonen at virksomhetene har god kontroll med egne brukere, men ikke med leverandørenes. Virksomhetenes internkontroll omfatter ikke de brukerne leverandørene har i virksomhetenes systemer. Det er utarbeidet rutiner og prosesser for tilgangsstyring hos virksomhetene og leverandørene, men antallet brukere med administratorrettigheter hos leverandørene er høyt, både gjennom AD og lokale administratorer på servere og i databaser. Et høyt antall brukere med tilgang til data øker risikoen for tap av dataintegritet og data på avveie. Administratorkontoer har utvidede rettigheter og bør derfor begrenses til et minimum. Misbruk av en konto med slike rettigheter kan gjøre omfattende skade på virksomhetenes systemer.

6.2.2 Vedlikeholdet av sikkerhetskonfigurasjon og gjennomføringen av sikkerhetsoppdateringer er varierende

Ifølge Nasjonal sikkerhetsmyndighet har systemer som ikke er eksplisitt konfigurert, mest sannsynlig sårbarheter i sine sikkerhetsinnstillinger som en angriper kan utnytte. Herding er en prosess for å fjerne svakheter i et system, for eksempel ved at man endrer standardinnstillinger for passord, oppdaterer systemet, fjerner programmer som ikke er i bruk, og konfigurerer sikkerhetsinnstillingene.

Herding er en viktig del av IKT-sikkerheten, og manglende herding av systemkomponenter er ofte en årsak til at angripere får fotfeste i IKT-infrastrukturen.

Normen anbefaler at alle standardpassord (fabrikkinnstillinger) på systemer og utstyr endres før behandlingen av helse- og personopplysninger på begynnes.[115]

Revisjonen viser at det er flere svakheter ved virksomhetenes herding av systemene:

- Passordinnstillingene er svakere enn anbefalt og følges ikke opp.
- Tofaktorautentisering er innført, men det gjennomføres ikke etterkontroller.
- Sikkerhetsinnstillinger på servere er ikke i henhold til beste praksis.

Revisjonen viser også at operativsystemet på servere og databaser vedlikeholdes, at sikkerhetsoppdateringer gjennomføres jevnlig, og at det i hovedsak bare er installert nødvendig og oppdatert programvare på serverne.

Passordinnstillinger er svakere enn anbefalt og følges ikke opp

De tekniske innstillingene som regulerer brukerens valg av passord kan konfigureres på flere måter. Passord kan angis og kontrolleres sentralt i AD og gjelde for mange systemer. Passord kan også angis lokalt for direkte pålogging til et system eller en database.

I AD kan innstillingene brukes på flere måter. AD har en generell passordpolicy som gjelder for alle brukere i domenet. Det kan også opprettes passordpolicyer som gjelder for spesielle grupper eller brukere og overstyrer den generelle passordpolicyen. I tillegg er det mulig å overstyre begge deler ved å benytte parametere for den enkelte bruker når det gjelder enkelte regler, for eksempel for bytte av passord. Det finnes flere anbefalinger for oppsett av passord, i denne revisjonen benytter vi *Center of Internet Security Password Policy Guide* som grunnlag for beste praksis.[116]

Alle tre virksomheter har beskrevet interne krav til passord og bruk av tofaktorautentisering i interne policydokumenter, retningslinjer eller kravdokumenter. De interne kravene er generelle og omfatter

[115] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel5.2.2.
[116] https://learn.cisecurity.org/cis-password-policy-guide-passphrases-monitoring-and-more?_gl=1*1npl3zq*_ga*NTA3NzIyNzk5LjE2ODMwMzMzMzE.*_ga_N70Z2MKMD7*MTY4MzAzMzMzMC4xLjEuMTY4MzAzNDY4MC42MC4wLjA.

ikke egne passordkrav eller unntak for enkeltbrukere eller grupper. Vi har analysert passordoppsettet i AD og passordoppsettet for utvalgte databaser.

Analyse av uttrekk fra passordinnstillinger i AD hos Statens legemiddelverk viser at generell passordpolicy ikke er satt opp i henhold til beste praksis eller interne passordkrav. Legemiddelverket opplyser at det har vært feil i interne krav, at det siden 2022 har vært vesentlige endringer i passordregimet, og at det jobbes med å få på plass nye passordregler.

Analyse av uttrekk fra passordinnstillinger i AD hos Folkehelseinstituttet viser at den generelle passordpolicyen ikke er satt opp i henhold til Folkehelseinstituttets krav til lengde. I tillegg er det opprettet to passordpolicyer som ikke er gjort gjeldende for noen brukere, og to passordpolicyer som er knyttet til AD-grupper som ikke synes å være vedlikeholdt; de inneholder for eksempel deaktiverte brukere. Hos Folkehelseinstituttet er det også tatt i bruk parametere som overstyrer utløp av passord, for det meste for systembrukere, testbrukere eller såkalte postboksbrukere.

Når det gjelder Folkehelseinstituttets passordinnstillinger, kommenterer Norsk helsenett at de fraråder bruk av passordpolicyer for enkeltgrupper.[117] Folkehelseinstituttet opplyser at Norsk helsenett ikke har informert dem om bruken av passordpolicyer for enkelte grupper og bruken av parametere. Folkehelseinstituttet opplyser videre at de har forutsatt at passordreglene som er bestemt i samarbeid med Norsk helsenett, er blitt innført i alle tjenester som leveres via Norsk helsenett. Dette ble ifølge instituttet sist tatt opp i taktisk møte med Norsk helsenett i september 2022, men instituttet har ikke verifisert om passordreglene er blitt innført.

Analyse av uttrekk fra passordinnstillinger i AD hos Helsedirektoratet viser at den generelle passordpolicyen i sikker sone for enkelte innstillinger ikke er satt opp i henhold til interne passordkrav eller beste praksis. Det er angitt parametere for overstyring av passordpolicy for noen brukere i både ytre og sikker sone. På spørsmål om hvordan Helsedirektoratet følger opp passordinnstillinger i AD, svarer direktoratet at sikker sone ble konfigurert da domenet ble satt opp. Endringer i konfigurasjonen må bestilles Norsk helsenett. Vi tolker svaret dithen at det ikke har vært gjennomført etterkontroll av passordinnstillinger etter at domenet ble satt opp.

Analyse av uttrekk av passordoppsett for utvalgte databaser i både Folkehelseinstituttet og Statens legemiddelverk viser at det er svakheter ved kravene om bytte av passord, passordkompleksitet og passordlengde for lokale administratorer.

Analyse av uttrekk fra utvalgte databaser hos Folkehelseinstituttet viser at de fleste lokale administratorene ikke har byttet passord siden 2017. For én lokal administratorkonto med omfattende rettigheter er ikke passordet blitt endret siden 2015. Folkehelseinstituttet kommenterer at det er uheldig at det ikke er innført faste rutiner for bytte av passord for disse kontoene.

Advania kommenterer at kunden/applikasjonsleverandøren må stille krav til passordene til databaser, og at Statens legemiddelverk / applikasjonsleverandøren ikke har stilt slike krav. Statens legemiddelverk oppgir at de er kritiske til at Advania ikke følger beste praksis for serveroppsett for kunden, og anser det som nødvendig å innføre leverandørstyring ned på detaljnivå for sikkerhetskrav til IT-tilbyder.

I Helsedirektoratets databaser er antallet lokale administratorbrukere begrenset, da innebygd lokal administratorkonto er deaktivert. Derfor er det ikke aktuelt med lokale passordkrav.

[117] Svar på skriftlige spørsmål fra Folkehelseinstituttet 17. april 2023.

Tofaktorautentisering er implementert, men det gjennomføres ikke etterkontroller

Det bør benyttes flerfaktorautentisering til å autentisere brukere. Der flerfaktorautentisering ikke støttes, bør brukerkontoer som har tilgang til viktige data eller systemer, og brukere som har driftsoppgaver, bli pålagt å bruke sterke passord i systemet.[118]

Alle tre virksomheter har tatt i bruk tofaktorautentisering ved at den aktuelle brukerkontoen blir meldt inn som medlem av en AD-gruppe. Vi har ikke undersøkt på hvilken måte Norsk helsenett og Advania bruker tofaktor til sine systemer.

AD-gruppene synes ikke å være vedlikeholdt. Hverken virksomhetene eller leverandørene har kontrollert om alle brukere som skal ha aktivert tofaktor, faktisk har fått det aktivert.

Vår analyse av AD-grupper som gir tilgang til bruk av tofaktor, viser at noen brukere hos Statens legemiddelverk hadde ikke fått aktivert tofaktorautentisering. Legemiddelverket opplyser at tofaktor aktiveres automatisk når det opprettes nye brukere. Videre opplyser legemiddelverket at unntakene som analysen har avdekket, sannsynligvis har oppstått fordi aktuelle brukere er blitt opprettet manuelt. Det kontrolleres ikke regelmessig om alle brukere har aktivert tofaktor.

Folkehelseinstituttet opplyser at det ikke er noen unntak for bruk av tofaktorløsningen for pålogging til sikker sone. Brukere i AD i ytre sone opprettes uten medlemskap i en tofaktorgruppe. Når en bruker fratrer stillingen, skal alle AD-gruppemedlemsskap avsluttes og brukeren deaktiveres. Norsk helsenett opplyser at det ikke gjennomføres noen etterkontroll av om rutinene for fratredelser fungerer.

Analyse av uttrekk fra AD i ytre sone hos Folkehelseinstituttet viser at det er mange deaktiverte brukere som fortsatt er medlem av AD-gruppen som gir tilgang til tofaktorløsningen. Fem av dem er merket som sluttet. I AD for sikker sone finnes det mange aktive brukere som ikke er medlem av en tofaktorgruppe og dermed ikke vil kunne logge seg på sikker sone dersom løsningen for tofaktor fungerer som beskrevet. Folkehelseinstituttet opplyser at de forutsetter at tilgang til tofaktor avsluttes når Folkehelseinstituttet sender fratredelsesmelding til Norsk helsenett.

Helsedirektoratet opplyser at det kun er pålogging i sikker sone som har tofaktorkrav, og at innmelding i AD-grupper for tofaktor inngår i rutinen når det bestilles tilgang til sikker sone. Det er kundesenteret hos Norsk helsenett som utfører bestillingen.

Sikkerhetsinnstillinger på servere er ikke i henhold til beste praksis

Sikkerhetskonfigurasjoner sørger for krav til for eksempel hvordan passordene settes opp, hva en bruker kan gjøre lokalt på maskinen, og hvilke programmer og funksjoner som kan kjøres av brukeren, i tillegg til å sikre maskinen mot trusler på nettverket. De fleste IKT-produkter leveres i standard konfigurasjon som er utviklet av produsenten eller forhandleren. Standard konfigurasjon er vanligvis utviklet for å forenkle installasjon eller bruk, ikke for å tilby god sikkerhet. Nasjonal sikkerhetsmyndighet anbefaler å ivareta sikker konfigurasjon blant annet gjennom å etablere og vedlikeholde en egen standard for sikkerhetskonfigurasjoner, og denne standarden bør gjelde for hver type enhet i virksomheten, for eksempel servere.

Center of Internet Security (CIS) har utarbeidet Microsoft Windows Server Benchmark[119] som beskriver beste praksis for konfigurasjon av GPO-er på servere, se faktaboks 4. Det er ulike anbefalinger for domenekontrollere og medlemsservere i domenet.

Analyser av uttrekk fra servere hos alle tre virksomheter viser at GPO-innstillinger ikke er satt opp etter beste praksis.

[118] NSMs grunnprinsipper for IKT-sikkerhet, kapittel 2.6.7.
[119] CIS Microsoft Windows Server 2019 Benchmark v1.3.0 – 18. mars 2022.

Norsk helsenett har etablert sin egen standard for sikkerhetsinnstillinger som er basert på Microsoft Security Baseline og ikke CIS. De to standardene har tilnærmet samme anbefalinger for god praksis for å sikre systemer og påvirker ikke våre vurderinger.

Vår analyse av GPO hos Statens legemiddelverk viser at mange innstillinger ikke er angitt i henhold til beste praksis for alle utvalgte servere. Årsaken er ifølge Advania at kunden ikke har bestilt dette.[120]

Uttrekk fra Folkehelseinstituttets servere viser at flere GPO-innstillinger ikke er angitt i henhold til beste praksis for ca. halvparten av serverne. For domenekontrollerne følger innstillingene i stor grad beste praksis. Norsk helsenett har etablert en standard for sikkerhetsinnstillinger. Norsk helsenett opplyser at det ikke er noen grunn til at noen av disse serverne skal avvike fra sikkerhetsstandarden som er satt på overordnet nivå, og det er laget egne rutiner for å håndtere systemer dersom de kun har noen få avvik i sikkerhetsinnstillingene. Videre opplyser Norsk helsenett at den eneste grunnen til at det forekommer avvik i dag, er at standarden for sikkerhetsinnstillinger ikke er blitt fulgt opp eller prioritert av det ansvarlige driftsteamet eller kunden. Dette medfører at en rekke av serverne er blitt behandlet som avvik i Norsk helsenetts driftsstruktur. For eksempel gjelder dette sikkerhetsavvik knyttet til lokal brannmur, noe som var kjent for Norsk helsenett, men som Folkehelseinstituttet opplyser å ikke ha fått informasjon om.[121] I forbindelse med Helse- og omsorgsdepartementets uttalelse til utkast til rapport opplyser Norsk helsenett[122] at de ikke kjenner seg igjen i beskrivelsen. Norsk helsenett opplyser at oppfølging av sårbarheter og sikkerhetsavvik i miljøene til Folkehelseinstituttet har vært tema siden virksomhetsoverdragelsen og at dette kan dokumenteres gjennom møtereferater.

Uttrekk av GPO fra både domenekontrollere og servere hos Helsedirektoratet viser at enkelte innstillinger ikke er gjort i henhold til beste praksis. Norsk helsenett kommenterer[123] at de har rutiner for administrasjon av sikkerhetsinnstillinger, men avvikene fra beste praksis er ikke kommentert i tilbakemeldingen fra Helsedirektoratet.

Vedlikehold og sikkerhetsoppdateringer gjennomføres jevnlig

Normen anbefaler at det bare brukes IKT-produkter som fortsatt vedlikeholdes og mottar sikkerhetsoppdateringer fra produktleverandøren. Virksomhetene bør sørge for at sikkerhetsoppdateringene installeres så fort som mulig.[124] Analysene våre omfatter vedlikehold og sikkerhetsoppdateringer av servere og databaser.

Analyser av uttrekk fra serverne som understøtter helseregistrene, viser at alle serverne kjører på et operativsystem som fortsatt vedlikeholdes, men at enkelte servere har en versjon av operativsystemet hvor generelt vedlikehold fra Microsoft avsluttes i oktober 2023. Etter dette vil det kun komme helt nødvendige sikkerhetsoppdateringer fra leverandøren. Alle tre virksomheter har servere med denne versjonen. Av totalt 20 servere hadde 7 denne versjonen. Alle de tre virksomhetene er i dialog med leverandørene og har begynt å oppdatere operativsystemet på serverne.

Leverandørenes rutiner tilsier at sikkerhetsoppdateringene som hovedregel utføres ved hjelp av automatiserte prosesser. Uttrekk av installerte sikkerhetsoppdateringer for operativsystemet i perioden juli 2021 til desember 2022 viser om oppdateringer utføres jevnlig.

Vår analyse av uttrekket viser at det varierer hvilke servere virksomhetene oppdaterer, og hvor ofte de gjør det. Analysen viser også at det er perioder hvor oppdateringer ikke er gjennomført. Norsk helsenett opplyser at manglende oppdateringer kan skyldes at de i en periode har gjort vedlikehold på systemene, og at oppdateringene da er blitt utført i en senere periode. Videre har Norsk helsenett

[120] Svar på skriftlige spørsmål fra Statens legemiddelverk 24. mars 2023.
[121] Svar på skriftlige spørsmål fra Folkehelseinstituttet 3. mai 2023
[122] Norsk helsenetts tilbakemeldinger på Riksrevisjonens Utkast til rapport 4. juli 2023
[123] Svar på skriftlige spørsmål for KPR fra Norsk helsenett 3. mai 2023.
[124] NSMs grunnprinsipper for IKT-sikkerhet, kapittel 2.3.1.

opplyst at ulike typer servere kan ha forskjellig oppdateringsfrekvens (for eksempel kvartalsvis), og at dette er vurdert som godt nok, men at viktige oppdateringer vil bli installert så raskt som mulig dersom Norsk helsenetts sikkerhetssenter gir beskjed om det.

Vår analyse viser at en server hos Statens legemiddelverk ikke ble oppdatert i en periode på seks måneder. Advania opplyser at årsaken til det var en feil på systemet som brukes til sikkerhetsoppdateringer.

Når det gjelder databasesystemene på serverne, viser våre analyser av uttrekk at alle databasesystemer er vedlikeholdte versjoner, men vi ser også følgende:

- For et av databasesystemene i Folkehelseinstituttet er generelt vedlikehold avsluttet fra leverandørens side, og systemet støttes bare med helt nødvendige sikkerhetsoppdateringer. Dette databasesystemet er installert på en av serverne hvor generelt vedlikehold avsluttes i oktober 2023 (se tidligere omtale). Folkehelseinstituttet opplyser at databasesystemet skal oppdateres samtidig med operativsystemene til serverne.
- For et databasesystem i Statens legemiddelverk ville utvidet vedlikehold med helt nødvendige sikkerhetsoppdateringer opphørt ved utgangen av 2023. Statens legemiddelverk opplyser at de har oppdatert databasesystemet til en nyere og vedlikeholdt versjon mens revisjonen har pågått.[125]

I hovedsak er bare nødvendig og oppdatert programvare installert på servere

Normen anbefaler at virksomheten har et bevisst forhold til installert programvare, og sikrer at programvaren kun utfører de funksjonene som er formålsbestemt.[126]

Analyser av uttrekk på utvalgte servere viser at det er installert noe programvare som ikke synes å være nødvendig, eller at det er installert gamle versjoner av programvaren. Virksomhetene har forklart hvorfor det er behov for det meste av programvaren som er installert, og i hovedsak er det bare nødvendig og oppdatert programvare på serverne. Statens legemiddelverk og Folkehelseinstituttet har imidlertid opplyst[127] at serverne har enkelte programmer som kan fjernes. Virksomhetene opplyser videre at de skal se nærmere på enkelte installerte programvarer som er knyttet til behov hos tredjeparter (utviklingsleverandører).

Oppsummert viser revisjonen at leverandøren foretar sikkerhetsoppdateringer, men at sikkerhetsinnstillingene ikke alltid er satt opp i henhold til beste praksis. Noen av svakhetene har vært kjent for leverandøren, men ikke tatt opp med virksomhetene. Manglende kontroll over sikkerhetsinnstillingene kan føre til sårbarheter i systemene som virksomheten ikke er kjent med.

6.2.3 Loggingen på servere og databaser er mangelfull

Mangelfull logging i IKT-systemer og mangelfull sammenstilling og analyse av sikkerhetsrelevante data medfører at en angriper kan skjule sin tilstedeværelse og sine handlinger og aktiviteter i virksomhetens informasjonssystemer. En systematisk tilnærming til hva som logges, og oppfølging av logger kan bidra til at virksomhetene oppdager sikkerhetshendelser tidlig og kan vurdere skadeomfanget og hendelsens karakter og forstå hendelsesforløpet.

[125] Oppdatert 10. februar 2023.
[126] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.4.
[127] Svar på skriftlige spørsmål fra Statens legemiddelverk 24. mars 2023 og Folkehelseinstituttet 17. april 2023.

Nasjonal sikkerhetsmyndighet anbefaler at virksomhetene aktivt beslutter hvilke deler av IKT-systemet som skal overvåkes og logges (operativsystem, databaser, applikasjoner og klienter).[128]

Normen angir et sett med minimumskrav til hva som skal logges for helseregistre. Som et minimum skal virksomhetene logge autorisert bruk, all system- og administratorbruk, endringer av konfigurasjon og programvare, sikkerhetsrelevante hendelser, forsøk på uautorisert bruk og bruk av selvautorisering.[129]

Revisjonen viser at det er mangler ved loggingen:

- Logging på servere har enkelte mangler i henhold til beste praksis.
- Administrasjon av databaseinstanser og endringer i databaser logges ikke.

Logging på servere har enkelte mangler i henhold til beste praksis

I denne revisjonen benytter vi anbefalinger fra Center of Internet Security som grunnlag for beste praksis. Anbefalingene fra CIS omfatter 59 ulike innstillinger for logging av hendelser og viser hvordan man bør angi innstillinger for logging på domenekontrollere og medlemsservere.

Analyser av uttrekk fra serverne til alle tre virksomheter viser at virksomhetene logger viktige parametere som pålogging av brukere og endringer i GPO-innstillinger på servere, men at andre innstillinger ikke alltid logges i henhold til anbefalingene fra CIS.[130]

Ved domenekontrollere er det bedre etterlevelse av beste praksis og kun få avvik hos Folkehelseinstituttet og Helsedirektoratet, mens domenekontrollerne til Statens legemiddelverk viser flere unntak fra beste praksis.

For mange av de utvalgte medlemsserverne i domenene (webservere, filservere, applikasjonsserverer og databaseservere) i alle tre virksomheter logges det mindre enn anbefalt. Eksempler på innstillinger som gjennomgående mangler logging, er parametere for hendelser knyttet til opprettelse/endring/sletting av filområder. Logging av prosesser på serverne hos Helsedirektoratet skiller seg ut med færre unntak fra beste praksis enn de øvrige.

Advania opplyser at det utføres «standard logging» dersom kunden ikke bestiller eller spesifiserer noe. Norsk helsenett opplyser at en rekke av Folkehelseinstituttets servere hvor det ikke logges i henhold til anbefalingene i CISblir behandlet som avvik i Norsk helsenetts driftsstruktur, jf. avsnitt over om sikkerhetsinnstillinger på servere.

Administrasjon av databaseinstanser og endringer i databaser logges ikke

Virksomhetene benytter tre ulike databasesystemer til sine helseregistre. Analyser av uttrekk fra logginnstillinger i databasene viser i hovedsak at data som overføres inn eller ut av databasen, logges. Kun ett av de tre databasesystemene til Statens legemiddelverk har logging i henhold til beste praksis. I et av de to andre er logging av administrasjon av databaseinstans aktivert, men det er ingen logging av endring av data i disse to. Advania opplyser at logging ikke er aktivert for disse to databasesystemene hos Statens legemiddelverk fordi det ikke er bestilt av kunden.[131]

Hos Folkehelseinstituttet og Helsedirektoratet logges hverken administrasjon eller endring av brukere i databaseinstansen eller endring av data i databasene.

[128] NSMs grunnprinsipper for IKT-sikkerhet, kapittel 3.2.3.
[129] Norm for informasjonssikkerhet og personvern i helse og omsorgstjenesten, kapittel 5.4.4.
[130] CIS Microsoft Windows Server 2019 Benchmark v1.3.0 – 18. mars 2022.
[131] Svar fra Statens legemiddelverk 24. mars 2023. D – databaser – spørsmål.

Folkehelseinstituttet opplyser at de ikke var kjent med at logging ikke var aktivert for databasene deres.[132]

Helsedirektoratet har ikke innført logging i databaser og databaseinstanser, men viser til at de har innført prosesslogging for all endring av data i databasen som skjer i automatiserte prosesser, og at Norsk helsenetts aktiviteter via pålogging i PAM blir tatt opp på video. Oppslag og endringer som gjøres av en Norsk helsenett-bruker som har logget seg inn i databasen, vil ikke fanges opp av prosessloggingen, og vil være vanskelig å identifisere gjennom sesjonsopptak såfremt ikke alle sesjonsopptak gjennomgås jevnlig.

Oppsummert viser revisjonen at det er mangelfull logging på servere og i databaser. Det er særlig mangler knyttet til logging av aktiviteter direkte i databaser. Krav til hva som skal logges, og kommunikasjonen med leverandørene om hva som faktisk logges, har ikke vært tydelig.

For både servere og databaser er det en stor mengde brukere med administratorrettigheter som kan gjøre endringer på sikkerhetsoppsettet eller direkte i databasen, jf. kapittel 6.2.1 Manglende logging medfører blant annet at det vil være vanskelig å oppdage og undersøke uønskede hendelser.

6.3 Tilgjengeliggjøring

Den dataansvarlige skal etter søknad tilgjengeliggjøre helseopplysninger i helseregistre når dataene skal brukes til et uttrykkelig angitt formål som er innenfor registrets formål.[133] Mottakeren skal godtgjøre at behandlingen vil ha rettslig grunnlag etter artikkel 6 og 9 i personvernforordningen. Videre skal behandlingen av opplysningene være innenfor rammene av eventuelle samtykker og ikke i strid med eventuelle reservasjoner. Mottakeren skal også gjøre rede for hvilke egnede tekniske og organisatoriske tiltak som skal settes i verk for å ivareta informasjonssikkerheten.

Helseregisterloven slår fast at den dataansvarlige skal tilgjengeliggjøre data fra helseregistrene innen 30 virkedager fra tidspunktet da en fullstendig søknad er mottatt. Dersom tilgjengeliggjøringen krever sammenstilling av opplysninger fra flere registre, er fristen 60 virkedager.[134]

Da vi utførte revisjonen, hadde ikke bivirkningsregisteret ved Statens legemiddelverk mottatt noen søknader om utlevering av data til forskning. Vi har kontrollert saksbehandlingstiden for alle utleveringer av direkte eller indirekte personidentifiserende opplysninger til forskere fra KPR, MSIS og DÅR i årene 2020–2022. Når vi har beregnet antall dager det har tatt å tilgjengeliggjøre data, har vi summert den tiden som har gått fra datoen for fullstendig søknad til datoen for utlevering. Det er kun antall virkedager som er inkludert i beregningene. Når det gjelder meldingssystem for smittsomme sykdommer er det kun tatt utgangspunkt i første søknad per prosjekt. Dette fordi gjentakende utleveringer og oppdateringer for samme prosjekt gir begrenset mulighet for å beregne overholdelse av frist, da utleveringene skjer etter avtale eller i dialog med prosjektet. Videre har vi valgt ut 15 tilfeldige utleveringer for å kontrollere at virksomhetene følger regelverket ved behandling av søknadene.

[132] Svar fra Folkehelseinstituttet 17. april 2023. D – databaser – spørsmål.
[133] Helseregisterloven av 20. juni 2014 § 19 a.
[134] Helseregisterloven av 20. juni 2014 § 19 f.

Hovedfunn

Helsedirektoratet og Folkehelseinstituttet kontrollerer at dokumentasjonen er i henhold kravene i regelverket, men tilgjengeliggjør ikke helseopplysninger innen lovpålagte frister. Brudd på fristen for utlevering vil kunne ha som konsekvens at et forskningsprosjekt blir forsinket, og at nytten av forskningen først blir tilgjengelig på et senere tidspunkt.

- Helsedirektoratet og Folkehelseinstituttet påser at forskerne dokumenterer det som er kravene i regelverket, før helseopplysningene tilgjengeliggjøres.
- Helsedirektoratet og Folkehelseinstituttet utleverer ikke helsedata innen lovpålagte frister.
- Virksomhetene har ikke grunnlag for å vurdere eller undersøke om mottakeren av helseopplysninger har tilfredsstillende informasjonssikkerhet.

6.3.1 Helsedirektoratet og Folkehelseinstituttet påser at forskerne dokumenterer det som er kravene i regelverket, før helseopplysningene tilgjengeliggjøres

Analysen av de utvalgte 15 søknadene viser at alle har dokumentasjon og vurderinger som bekrefter at søknadene inneholder de formelle kravene for å få utlevert data fra helseregistrene. Både Helsedirektoratet og Folkehelseinstituttet dokumenterer saksbehandlingen. Hver søknad får eget saksnummer, og all kommunikasjon og dokumentasjon lagres i arkivsystemet.

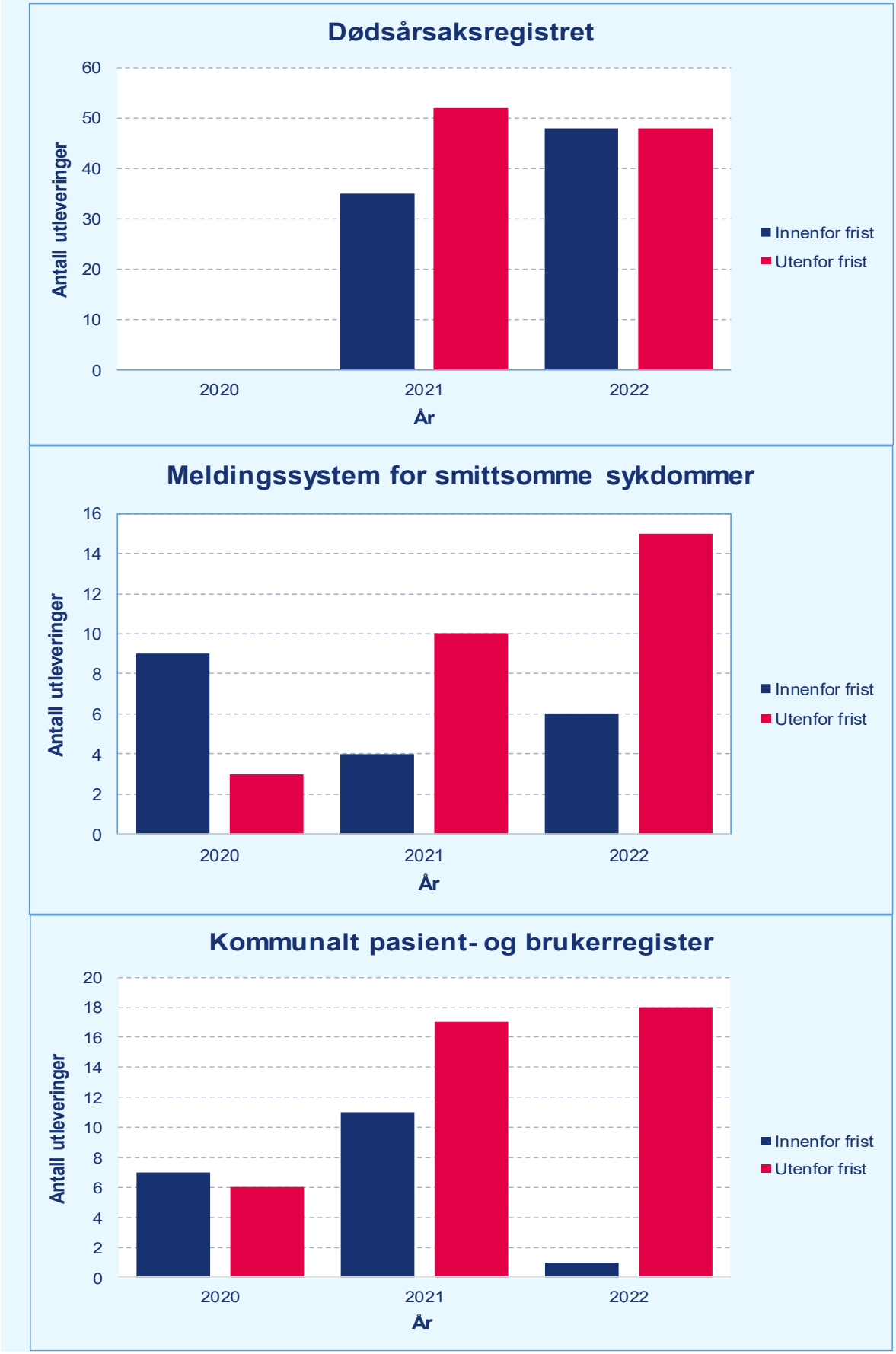
Alle de kontrollerte søknadene om utlevering av data inneholder en beskrivelse av formålet med prosjektet og en forhåndsgodkjenning fra regional komité for medisinsk- og helsefaglig forskningsetikk. Forskerne har argumentert for hvilket rettslig grunnlag de mener å ha for å få tilgjengeliggjort helseopplysninger fra helseregistrene. Den gjennomgående argumentasjonen er enten at de har innhentet samtykke fra de personene helseopplysningene gjelder, jf. artikkel 6 nr. 1 bokstav a i personvernforordningen, eller at behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den dataansvarlige er pålagt, jf. artikkel 6 nr. 1 bokstav e i personvernforordningen. Argumentasjonene underbygges av artikkel 9 nr. 2 bokstav i og nr. 2 bokstav j.

6.3.2 Helsedirektoratet og Folkehelseinstituttet tilgjengeliggjør ikke helseopplysninger innen lovpålagte frister

Vår gjennomgang av alle utleveringer av indirekte og direkte personidentifiserende helseopplysninger til forskning viser at Folkehelseinstituttet og Helsedirektoratet ikke overholder de lovpålagte fristene på dager og 60 dager. Figurene under viser antall utleveringer innenfor frist og utenfor frist i perioden 2020–2022, fordelt på de tre helseregistrene som denne problemstillingen omfatter.[135] For dødsårsaksregisteret fremkommer ikke utleveringer for 2020, dette fordi mottatt datagrunnlag ikke inneholder informasjon om dato for komplett søknad.

[135] Bivirkningsregisteret hos Statens legemiddelverk hadde ingen utleveringer til forskningsprosjekter i kontrollperioden.

Figur 8 Utleveringer fra dødsårsaksregisteret, meldingssystemet for smittsomme sykdommer og kommunalt pasient- og brukerregister



Kilde: Riksrevisjonen, basert på informasjon fra virksomhetene

Figuren viser at alle de tre registrene har utfordringer med å etterleve de lovpålagte fristene for å levere ut forespurt helsedata til forskning. DÅR har fra 2021–2022 en positiv utvikling i andelen utlevering innenfor fristen. For MSIS og KPR er trenden at andelen utleveringer innenfor fristen er synkende.

Vår gjennomgang av alle utleveringer fra registrene i perioden 2020–2022 viser at det er mange eksempler på at det kan ta over 300 virkedager fra søknaden er vurdert fullstendig, til data utleveres fra registrene.

Fra kontrollen av de 15 utvalgte sakene (jf. kapittel 6.2.1) ser vi at forklaringer på at utleveringstiden overskrider fristene, for eksempel kan være generell saksbehandlingstid, eller at registrene venter på en koblingsnøkkel fra en ekstern part som skal benyttes i forbindelse med uttrekket av data fra registret.

Tilgjengeliggjøringen kan utsettes dersom særlige forhold gjør det uforholdsmessig vanskelig å overholde fristen. Den dataansvarlige skal i så fall gi et foreløpig svar med informasjon om grunnen til forsinkelsen og tidspunktet for når tilgjengeliggjøring sannsynligvis vil skje.[136] Gjennomgangen av de 15 utvalgte sakene viser at virksomhetene ikke har noen ensartede rutiner for å varsle søkeren i de tilfellene hvor fristen for utlevering overskrides. I flere av sakene har ikke virksomhetene varslet når fristen ikke overhodes. Når de varsler om forsinkelser, oppgir de sjelden årsak.

Fremstillingen i figuren ovenfor tar utgangspunkt i antall virkedager fra tidspunktet da fullstendig søknad foreligger, til tidspunktet for utlevering av data. Vår analyse viser at det i mange tilfeller tar noe tid fra forskerne sender inn søknaden, til søknaden vurderes som fullstendig. Dette tidsrommet bidrar til å øke den totale tiden forskerne må vente på forskningsdataene fra søknadstidspunktet. Antall dager det i snitt tar fra tidspunktet da helseregistrene mottar søknaden, til tidspunktet da søknaden anses som fullstendig, er følgende for årene 2020–2022:

- dødsårsaksregisteret: 46 dager
- meldingssystemet for smittsomme sykdommer: 68 dager
- kommunalt pasient- og brukerregister: 20 dager

Det er et politisk mål om å bruke helsedata mer til analyser og forskning.[137] Ny forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata trådte i kraft 11. januar 2023. Direktoratet for e-helse ved helsedataservice har fra 15. mars 2023 fått ansvaret for å behandle og avgjøre eventuelle tilgjengeliggjøringer av helsedata fra helseregistre.[138]

Folkehelseinstituttet har gitt tilbakemelding på funnene. De mener at ventetiden for å motta koblingsnøkkel ikke bør inngå når det skal måles om en sak er utlevert innenfor frist. For koblingssaker summerer Folkehelseinstituttet antall virkedager fra komplett søknad til vedtak med antall virkedager fra mottatt nøkkel til utlevering.

6.3.3 Virksomhetene har ikke grunnlag for å vurdere eller undersøke om mottakeren av helseopplysninger har tilfredsstillende informasjonssikkerhet

I søknaden eller den vedlagte vurderingen av personvernkonsekvenser (DPIA) beskrives det hvordan prosjektene har planlagt å ta vare på dataene når de mottas. For prosjektene som er tilknyttet universitets- og høgskolesektoren, opplyses det at de skal benytte tjenester for sensitive data (TSD). Andre søkere, for eksempel forskere tilknyttet helseforetak eller andre forskningsinstitusjoner, har egne systemer for lagring av sensitive data.

[136] Helseregisterloven av 20. juni 2014 §19 f.
[137] Verifisert referat fra intervju med Helse- og omsorgsdepartementet 15. mars 2023.
[138] Forskrift om nasjonal løsning for tilgjengeliggjøring av helsedata § 3,15. mars 2023.

Systembeskrivelsene som blir lagt ved søknaden eller er beskrevet i DPIA, er overordnet. Det står blant annet at dataene vil oppbevares i sikker sone. Beskrivelsene har ikke en detaljeringsgrad som gjør det mulig for de som skal levere ut dataene, å kunne vurdere om rutinene og systemene for lagring har tilfredsstillende informasjonssikkerhet. Gjeldende regelverk gir virksomhetene hverken plikt eller adgang til å følge opp at behandlingen av helsedataene faktisk skjer som beskrevet i søknaden.

Helsedirektoratet har i sin risikovurdering påpekt at de har begrenset kontroll med hvor god sikkerhet mottakeren har. Det fremgår videre at det er umulig for virksomheten å vite sikkerhetstilstanden til mottakeren ut over egenerklæringen i form av DPIA.[139]

I forbindelse med gjennomgangen av dokumentasjonen i de 15 utvalgte sakene har vi sett at det kan forekomme tilfeller hvor et forskningsprosjekt ber om data fra mange registre. Forskningsprosjektet kobler sammen de utleverte dataene, inkludert person- og helsedata, med det resultat at det blir etablert et midlertidig register med store mengder data. Lederen av prosjektet blir dataansvarlig for en samling av helseopplysninger som vil kunne overstige omfanget av data i de enkelte registrene.

I forbindelse med tilretteleggingen av datasett vurderer helseregistrene dataminimering for å sikre at det ikke blir utlevert en større mengde helseopplysninger enn det som er nødvendig for formålet. Selv om hver enkelt registereier er bevisst på dataminimering, kan en sammenstilling fra flere registre medføre risiko for at de sammenstilte dataene blir mer sensitive enn ønskelig. Dette synliggjøres i vedtaksbrevene fra helseregistrene gjennom at mottakeren av utleveringen blir bedt om ikke å foreta enkelte typer koblinger.

Alle tre registrene sender ut et vedtaksbrev når søknaden er ferdig behandlet. Vedtaksbrevene inneholder ingen krav til søkeren om å sette i verk tekniske og organisatoriske tiltak for å ivareta informasjonssikkerheten. Brevene påpeker at mottaker har et ansvar for å sikre at behandlingen av personopplysninger følger kravene i personopplysningsloven og personvernforordningen, alternativt at prosjektlederen har ansvar for at opplysningene oppbevares trygt og på en slik måte at uvedkommende ikke får tilgang til dem.

Helse- og omsorgsdepartementet viser i et intervju til at virksomhetene ikke har adgang til å vurdere eller følge opp informasjonssikkerheten hos mottakeren av registerdata. Mottakeren av opplysningene vil ha eget ansvar for informasjonssikkerheten etter at disse er tilgjengeliggjort, jf. artikkel 32 i personvernforordningen. Departementet påpeker at Helsetilsynet er pålagt oppgaven å føre tilsyn med regelverket i sektoren, og at Datatilsynet har generell tilsynskompetanse for all behandling av person- og helseopplysninger.[140]

[139] Helsedirektoratets risikovurdering «Risikovurdering av søknadsbehandling og utlevering av data» av 19. oktober 2022, risiko R8 «Det utleveres data til en mottaker som ikke har tilfredsstillende sikkerhet til å ivareta konfidensialiteten i dataene».
[140] Verifisert referat fra intervju med Helse- og omsorgsdepartementet 15. mars 2023.

7 Konklusjon

Formålet med helseregistrene er å samle helseopplysninger, slik at disse kan brukes til blant annet kvalitetsforbedring, forebyggende arbeid, beredskap, analyser eller forskning. Helseregistrene gir informasjon om blant annet smittsomme sykdommer, bivirkninger, dødsårsaker og helse- og omsorgstjenester.

Både lov om helseregistre og behandling av helseopplysninger (helseregisterloven) og lov om behandling av personopplysninger (personopplysningsloven) stiller krav til virksomhetenes håndtering av person- og helseopplysninger i helseregistrene. Personopplysningene skal behandles i samsvar med prinsippene i personvernforordningen (GDPR).

Målet med revisjonen har vært å kontrollere om person- og helseopplysninger i lovbestemte personidentifiserende helseregistre som er underlagt Helse- og omsorgsdepartementet, behandles i henhold til kravene om informasjonssikkerhet, personvern og tilgjengeliggjøring i helseregisterloven og personopplysningsloven.

Basert på kriteriene har vi kontrollert om virksomhetene som er dataansvarlig for helseregistrene, har

- etablert risikostyring og leverandøroppfølging
- gjennomført informasjonssikkerhetstiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen
- tilgjengeliggjort helseopplysninger fra helseregistre i henhold til regelverket

Konklusjon

Person- og helseopplysninger i helseregistre behandles ikke i tilstrekkelig grad i henhold til kravene i helseregisterloven og personopplysningsloven.

Konklusjonen bygger på følgende hovedfunn:

- Virksomhetene har ikke oversikt over sikkerhetsarbeidet som gjøres hos leverandørene, og jobber ikke systematisk med risiko og tiltak.
- Viktige informasjonssikkerhetstiltak hos leverandørene er ikke er implementert eller fungerer ikke etter hensikten.
- Helsedirektoratet og Folkehelseinstituttet overholder ikke lovpålagte frister for tilgjengeliggjøring av helseopplysninger.

7.1 Virksomhetene har ikke oversikt over sikkerhetsarbeidet som gjøres hos leverandørene, og jobber ikke systematisk med risiko og tiltak

Den dataansvarlige for helseregistrene skal gjennomføre tekniske og organisatoriske tiltak, både for å sikre og påvise at behandlingen utføres i samsvar med regelverket, og for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Virksomhetene har mangelfull risikostyring og manglende oppfølging av krav i avtaler med leverandøren, og de etterlever dermed ikke helseregisterloven § 22 og artikkel 24 i personvernforordningen. Når virksomhetene ikke har oversikt over det totale risikobildet eller informasjon om hvordan leverandørene gjennomfører tiltak, kan det være vanskelig å iverksette tiltak som samlet sett er egnet til å ivareta sikkerheten.

Revisjonen viser at virksomhetenes risikovurderinger og vurderinger av personvernkonsekvenser er mangelfulle. Folkehelseinstituttet og Statens legemiddelverk har ikke full oversikt over registrerte avvik knyttet til registrene. Virksomhetene har ikke system og rutiner for kvalitetssikring og etterkontroll av sikkerhetsarbeidet som gjennomføres hos leverandørene.

7.2 Viktige informasjonssikkerhetstiltak hos leverandørene er ikke implementert, eller fungerer ikke etter hensikten

Den dataansvarlige og databehandleren skal gjennomføre tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Viktige informasjonssikkerhetstiltak hos leverandørene er ikke er implementert, eller fungerer ikke etter hensikten. Virksomhetene har ikke påsett at viktige sikkerhetstiltak er implementert hos leverandørene, og de etterlever dermed ikke helseregisterloven § 21 og artikkel 32 i personvernforordningen. Virksomhetene kunne ha identifisert svakhetene i sikkerhetstiltak som tilgangsstyring, sikkerhetskonfigurasjoner og logging dersom de hadde hatt en helhetlig risikostyring og tettere oppfølging av leverandørene.

Revisjonen viser at antallet brukere med administratorrettigheter hos leverandørene er høyt. Videre er det mangelfull logging på servere og i databaser, særlig logging av aktiviteter som foregår direkte i databasene. Revisjonen viser også at passordinnstillinger er svakere enn anbefalt, og at sikkerhetsinnstillingene ikke alltid er satt opp i henhold til beste praksis.

Manglende oppfølging av sikkerhetsinnstillingene kan medføre sårbarheter i systemene som virksomheten ikke er kjent med. Et høyt antall brukere med administratorrettigheter øker risikoen for misbruk eller feil som kan gjøre omfattende skade på virksomhetenes systemer. Manglende logging medfører at det kan være vanskelig å oppdage og undersøke uønskede hendelser.

7.3 Helsedirektoratet og Folkehelseinstituttet overholder ikke lovpålagte frister for tilgjengeliggjøring av helseopplysninger

Virksomhetene skal etter søknad tilgjengeliggjøre helseopplysninger i helseregistre når dataene skal brukes til et uttrykkelig angitt formål som er innenfor registrets formål. Mottakeren skal godtgjøre at behandlingen vil ha rettslig grunnlag, og gjøre rede for hvilke egnede tekniske og organisatoriske tiltak som skal settes i verk for å ivareta informasjonssikkerheten. Virksomhetene skal tilgjengeliggjøre data fra helseregistrene innen 30 virkedager etter at en fullstendig søknad er mottatt. Dersom

tilgjengeliggjøringen krever sammenstilling med opplysninger fra flere registre, er fristen 60 virkedager. Tilgjengeliggjøringen kan utsettes dersom særlige forhold gjør det uforholdsmessig vanskelig å overholde fristen. Den dataansvarlige skal i så fall gi et foreløpig svar med informasjon om grunnen til forsinkelsen og tidspunktet for når tilgjengeliggjøring sannsynligvis vil skje.

Folkehelseinstituttet og Helsedirektoratet påser at forskerne dokumenterer det som er kravene i regelverket, men tilgjengeliggjør ikke helseopplysninger innen lovpålagte frister. Etter vår vurdering blir ikke helseopplysninger tilgjengeliggjort i tilstrekkelig grad i henhold til kravene i regelverket om tilgjengeliggjøring.

Revisjonen viser at søknadene vi har kontrollert, inneholder dokumentasjon og vurderinger som bekrefter at den formelle saksbehandlingen er i henhold til gjeldende regelverk. Saksbehandlingen synliggjør også at virksomhetene er opptatt av å ikke levere ut mer data enn nødvendig, blant annet for å redusere risikoen for personidentifisering.

Revisjonen viser videre at det er mange tilfeller hvor fristen for tilgjengeliggjøring ikke blir overholdt for de tre helseregistrene dødsårsaksregistret, meldingssystemet for smittsomme sykdommer og kommunalt pasient- og brukerregister. Folkehelseinstituttet og Helsedirektoratet har ingen enhetlig rutine for å varsle søkerne i de tilfellene hvor de ikke overholder fristen. Det er mange eksempler på at det kan ta over 300 virkedager fra søknaden er fullstendig, til data utleveres fra registrene. I tillegg kan det ta lang tid fra søknaden mottas, til den er vurdert fullstendig, noe som bidrar til å forlenge den totale tiden forskerne må vente på forskningsdataene.

Både godkjenningen fra regional komité for medisinsk- og helsefaglig forskningsetikk og finansieringen av det enkelte forskningsprosjekt kan inneholde tidsfrister for når prosjektet må være ferdig, det er derfor viktig at forskningen ikke forsinkes som følge av saksbehandlingen hos virksomhetene. Brudd på fristen for utlevering vil kunne ha som konsekvens at forskningsprosjektet blir forsinket, og at nytten av forskningen først blir tilgjengelig på et senere tidspunkt.

Vedlegg

Vedlegg 1:

Antall utleveringer av data til forskning

Vedlegg 1:
antall utleveringer av direkte eller indirekte personidentifiserende data til forskning, fordelt på 30 og 60 dager for årene 2020–2022

Tabellen viser datagrunnlaget for figur 9.

Antall utleveringer for DÅR, MSIS og KPR 2020–2022

Register	Årstall			
DÅR	**2020**	**2021**	**2022**	**Antall dager i snitt fra søknad til fullstendig søknad alle tre år**
Innenfor frist 30 dager (antall)	0	7	10	
Utenfor frist 30 dager	0	3	2	
Innenfor frist 60 dager	0	28	38	
Utenfor frist 60 dager	0	49	46	
Fra søknad til fullstendig søknad (snitt dager)	0	56	36	46
MSIS	**2020**	**2021**	**2022**	**Antall dager i snitt fra søknad til fullstendig søknad alle tre år**
Innenfor frist 30 dager (antall)	0	0	2	
Utenfor frist 30 dager	0	1	0	
Innenfor frist 60 dager	9	4	4	
Utenfor frist 60 dager	3	9	15	
Fra søknad til fullstendig søknad (snitt dager)	69	52	83	68
KPR	**2020**	**2021**	**2022**	**Antall dager i snitt fra søknad til fullstendig søknad alle tre år**
Innenfor frist 30 dager (antall)	0	0	1	
Utenfor frist 30 dager	0	3	2	
Innenfor frist 60 dager	7	11	0	
Utenfor frist 60 dager	6	14	16	
Fra søknad til fullstendig søknad (snitt dager)	15	25	19	20

Kilde: Utleveringsoversikter vi har mottatt fra Folkehelseinstituttet og Helsedirektoratet