Brevkontroll med sentrale helseregistre Datatilsynets oppsummering.

Innhold

1 Hvem ble kontrollert

Våren 2016 gjennomførte Datatilsynet brevlige kontroller med alle de sentrale helseregistrene som da var lovhjemlet i helseregisterloven. Likelydende brev ble sendt til Medisinsk fødselsregister, Hjerte- og karregisteret, MSIS, SYSVAK, Reseptregisteret, Dødsårsaksregisteret, Kreftregisteret, Norsk pasientregister, IPLOS og Forsvarets helseregister. De behandlingsansvarlige for registrene er Folkehelseinstituttet, Kreftregisteret (OUS), Helsedirektoratet og Forsvarsdepartementet.

Av de kontrollerte registrene er alle nasjonale, personidentifiserbare og ikke-samtykkebaserte registre uten reservasjonsrett. Reseptregisteret og IPLOS er pseudonyme registre, hvilket betyr at opplysningene i registeret kan knyttes til enkeltindivider, men at navn og fødselsnummer er erstattet med en kode. Registeret har ikke tilgang til de registreres identitet og det er en ekstern tredjepart som står for pseudonymiseringen.

Behandling av personopplysninger i registrene er regulert i egne forskrifter med hjemmel i helseregisterloven §§ 9 og 11.

2 Tema og gjeldende regelverk

Formålet med kontrollene var å undersøke hvordan registrene praktiserer etterlevelse av kravene i personvernregelverket og hvilke tiltak registerforvalterne benytter seg av for å sikre ivaretakelse av de registrertes personvern. Vi hadde derfor særlig fokus på virksomhetens internkontroll, informasjonssikkerhetstiltak og de registrertes rettigheter.

Kontrollene ble gjennomført og svarene ble vurdert etter kravene i helseregisterloven med tilhørende forskrifter og personopplysningsloven av 2000. Den nye personvernforordningen trådte i kraft 20. juli 2018.

Resultatene fra denne kontrollen er ikke mindre aktuelle som følge av regelverksendringen og vi legger til grunn at de vurderingene vi har gjort også vil være relevante og nyttige når registerforvalterne nå skal etterleve kravene i forordningen. I denne oppsummeringen er det derfor vist til forordningens krav der vi mener det er særlig relevant.

3 Oppsummering av funn

Tabellen nedenfor viser hvilke spørsmål som ble stilt under de tre hovedtemaene for kontrollen hvor det ble avdekket mangler hos ett eller flere registre. Røde felter viser avvik.

Avvik rutiner/system	NPR	IPLOS	FO	KRG	Resept	DÅR	HKR	MFR	SYSVAK	MSIS
Avvikshåndtering										
Opplæring										
Ledelsens gjennomgang										
Informasjon til allmennheten										
Rutiner innsyn/retting/sletting										
Logg faktisk bruk										
Gjennomgang av logg										
Kryptering/infosikkerhet										
Databehandleravtale										
Risikovurdering										
Tilgangskontroll										

Nedenfor går vi nærmere inn på de overordnede funnene fra kontrollene. Vi går ikke inn i detaljer for hvert enkelt register, men tar for oss det vi mener er de viktigste erfaringene fra kontrollene. Fullstendig kontrollrapport for hvert enkelt register finnes i Datatilsynets saksarkiv og er tilgjengelig på våre nettsider.

3.1 Internkontroll

Den som behandler personopplysninger i et helseregister er pålagt å ha tilfredsstillende internkontroll i samsvar med kravene i helseregisterloven § 22 og særbestemmelser inntatt i de respektive registrenes forskrifter.

Vi ba derfor om dokumentasjon som kunne underbygge i hvilken grad registrene hadde tilfredsstillende internkontroll i henhold til helseregisterloven § 22 og personopplysningsloven § 14. Videre ba vi om dokumentasjon på gjennomførte risikovurderinger for å dokumentere etterlevelse av personopplysningsforskriften § 2-4. Vi ba om beskrivelse av virksomhetens system for behandling av avvik jf. personopplysningsforskriften § 2-6, om registrets status i forhold til nye krav om innebygget personvern. Vi undersøkte også hvordan virksomheten arbeidet for å sikre nødvendig kompetanse og opplæring av egne ansatte samt rutiner for ledelsens gjennomgåelse av sikkerheten i registeret.

Svarene vi fikk viste at alle registrene har utarbeidet en rekke omfattende rutiner og retningslinjer som totalt sett innebærer at det finnes et internkontrollsystem. Tatt i betraktning det store omfanget av skriftlig dokumentasjon som ble sendt oss mener vi det kan stilles spørsmål ved om den omfangsrike informasjonen i tilstrekkelig grad er kjent, tilgjengeliggjort og implementert i virksomheten slik at internkontrollen faktisk bidrar til kontinuerlig forbedring av arbeidet med sikkerhet og personvern.

Vi fant at flere av registrene manglet rutiner og system for avviksrapportering og oppfølging av avvik. Vi fant også at det manglet tilstrekkelige rutiner for å sikre ledelsens gjennomgang av sikkerheten i registrene og oppfølging av eventuelle tiltak som ble avdekket ved slik gjennomgang.

Vi fant også mangelfulle rutiner for å sikre nødvendig opplæring av de ansatte når det gjelder særlig krav knyttet til behandling av personopplysninger.

Arbeidet med internkontroll og sikkerhet forutsetter at det ligger en risikovurdering til grunn for valg av sikkerhetsstrategi, nødvendige sikkerhetstiltak og krav til sikkerhetskultur i virksomheten. Det var kun et register som ble pålagt å gjennomføre risikovurdering. Vår vurdering er allikevel at de avvikene som ble avdekket i forhold til kravene til internkontroll viser store ulikheter ved registerforvalternes systematiske arbeid og intern kultur for å prioritere sikkerhets- og personvernrelatert arbeid som en viktig del av kjernevirksomheten til en registerforvalter.

En mulig forklaring kan være at de sentrale registrene har oppstått i fagmiljøer der primærformålene med registrene har hatt betydelig større fokus enn de omfattende pliktene som følger med ansvaret som behandlingsansvarlig eller dataansvarlig for registeret. Desentralisert drift og begrensede ressurser til sikkerhetsarbeid i de medisinske fagmiljøene kan også forklare store ulikheter.

Kontrollen har vist at alle registrene hadde et bevisst forhold til lovpålagte krav om internkontroll, men at det fortsatt eksisterte utfordringer når det kom til systematikk, implementering, etterlevelse og rutinemessig oppfølging, prioritering og kontroll av tiltak som er nødvendige for å sikre en tilfredsstillende internkontroll.

3.2 Informasjonssikkerhet

Innenfor registerfeltet i Norge har vi et stort omfang av obligatoriske registre der norske borgere registreres mer eller mindre uvitende. Helsepersonell har meldeplikt til registrene og formålet med registrene er å sikre bedre helsetjeneste/folkehelse/sykdomsbehandling mv. ved å tilgjengeliggjøre helsedata til forskning, statistikk og analysearbeid.

Når registrene er regulert i lov og forskrift kan man i prinsippet legge til grunn at lovgiver har vurdert at registeret kan forsvares ut fra et personvernperspektiv. I alle lovforarbeider og forslag til lov vi har lest i Datatilsynet blir lovgiver forelagt et lovforslag der det argumenteres for at personvernet til de registrerte er ivaretatt fordi det stilles krav om tilstrekkelig informasjonssikkerhet gjennom tiltak som for eksempel kryptering, tilgangskontroll og logging.

Lovgiver har derfor lagt til grunn at de sentrale registrene har så god informasjonssikkerhet at personvernulempene ved å være registrert er redusert til et akseptabelt nivå i forhold til registrets formål.

Vi ville derfor undersøke om de sentrale registrene kunne dokumenter etterlevelse av lovens krav om tilfredsstillende informasjonssikkerhet og hvilke tiltak de hadde iverksatt for å sikre registrets plikt til å ivareta kravene til konfidensialitet, integritet og tilgjengelighet jf. helseregisterloven § 21.

Tilfredsstillende informasjonssikkerhet er en nødvendig forutsetning og et grunnkrav som må være oppfylt for at behandling av personopplysninger er tillatt. Ivaretakelse av strenge krav til konfidensialitet er en side av saken, men det er også viktig å sikre at opplysningene i registeret er tilgjengelige for det formålet de er samlet inn for og at de er og fortsetter å være, korrekte og ikke endres eller manipuleres av uvedkommende.

I to tilfeller fant vi at registrene ikke oppfylte kravene i helseregisterloven § 21 på kontrolltidspunktet. Moderniseringsprosjekter er gjennomført og avvikene er nå lukket også for disse registrene.

Hva som skal til for å oppfylle lovpålagte krav om tilfredsstillende informasjonssikkerhet avhenger av en konkret risikovurdering der man analyserer verdien av de dataene man forvalter, alle eventuelle risiko og sårbarheter, samt konsekvensene av eventuelle avvik.

Når det gjelder risikovurderinger ved behandling av personopplysninger kan det være nyttig å presisere at det må tas hensyn til hvilke konsekvenser eventuelle sikkerhetsbrudd kan ha for de registrertes rettigheter og friheter. Hensynet til den registrerte skiller en risikovurdering etter personopplysningsloven fra en mer tradisjonell risikovurdering som gjerne setter virksomheten, dens omdømme og økonomi i sentrum.

I den nye personvernforordningen er dette presisert og tydeliggjort i artikkel 24 og 32 som omtaler den behandlingsansvarliges plikt til å sørge for sikkerhet ved behandling av personopplysninger. Personvernforordningen er dermed tydeligere i sin ordlyd når det gjelder hvilke hensyn som skal ivaretas gjennom sikkerhetsarbeidet, enn hva som var tilfellet etter personopplysningsloven av 2000.

Vår vurdering er at krav til kryptering og logging av tilgang til registeret kun er to eksempler på tiltak som er nødvendige for å minimere tilgangen til direkte identifiserbare helseopplysninger og for å oppdage utilsiktet eller uautorisert tilgang til registeret etter at avvik faktisk har skjedd. Krav om logging og innsyn i logg er et forebyggende tiltak som ikke i seg selv reduserer personvernulempen ved å være registrert i et register. Tilstrekkelig informasjonssikkerhet handler om å ha tekniske løsninger som uavhengig av retningslinjer og rutiner gjør det vanskelig eller helt umulig å benytte opplysningene i registeret på en annen måte enn det de er ment for og som sikrer at det ikke er mulig å få tilgang uten å være autorisert for slik tilgang.

Kravet til innbygget personvern er inntatt i personvernforordningen artikkel 25, men var ikke et lovkrav da kontrollen ble gjort. Det var allikevel interessant å undersøke i hvilken grad eksisterende registre hadde løsninger som i noen grad tilfredsstilte kravene til innbygget personvern.

Vi ba om rutiner for tilgangsstyring, loggføring av bruk av registeret, rutiner og system for kontroll og systematisk gjennomgang av logg. Vi ba også om informasjon om hvordan registrerte etterlever kravet til kryptering i helseregisterloven § 21 annet ledd og om registrene benytter seg av skylagring, databehandlere og eventuell kontroll av databehandlere.

3.2.1 Tilgangsstyring

Tilgangsstyring i registrene er avhengig av hvor gammelt eller moderne registeret er. Moderniseringsprosjekter var igangsatt der det var nødvendig, men det kan synes som om det har tatt lang tid å få alle registerplattformer opp på et tidsriktig nivå når det kommer til sikkerhetsløsninger og moderne funksjonalitet. Noen registre har et tilgangsregime tilpasset bruken av registeret som i noen tilfeller krever direkte oppslag som ledd i tilbud om helsehjelp. Når den teknologiske plattformen ikke opprinnelig ble bygget opp rundt prinsippet om begrenset tilgangskontroll og innebygget personvern, innebærer bruken av registret at det etter vår vurdering er for mange ansatte i registrene som har tilgang til for mange registeropplysninger.

3.2.2 Logg

Kravet til logging er mye brukt som et viktig argument for å forsikre beslutningstakere og allmennheten om at personvernhensyn er ivaretatt. Registrene opererer med ulike former for logging. Det synes å ha vært en alminnelig oppfatning om at det kun er tilgang til direkte

identifiserbare opplysninger som krever logging av bruk av data, og at dette begrunnes i hensynet til de registrertes rett til innsyn i bruk av slike opplysninger. I et av de pseudonyme registrene fantes det ikke system for logg fordi registeret (per definisjon) ikke inneholder personidentifiserbare opplysninger.

Vi har derfor sett det nødvendig å påpeke at det er ulike hensyn som ligger til grunn for plikten til å gi den registrerte innsyn i hvem som har fått tilgang til eller fått utlevert direkte identifiserbare opplysninger fra registeret jf. helseregisterloven § 24 annet ledd og kravet til logg som en del av et tilfredsstillende system for informasjonssikkerhet etter helseregisterloven § 21.

Dersom det skjer et avvik skal logging av trafikken i registeret bidra til å fremskaffe viktig informasjon om hva for eksempel en uautorisert inntrenger har foretatt seg i registeret. Dersom slik logg ikke finnes, er det umulig for den dataansvarlige å finne ut om opplysninger er slettet, manipulert eller om det på annen måte er utført ureglementerte handlinger. Det er da vanskelig å i det hele tatt oppdage og deretter vurdere omfanget og konsekvensene av et sikkerhetsbrudd.

Vi fant mangler hos nesten alle registre når det gjaldt etterlevelse av kravet til logg. Noen avvik skyldes mangelfullt system og andre avvik skyldes mangelfulle rutiner.

Like alvorlig mener vi det har vært å se at det i stor grad mangler både system og rutiner for etterfølgende kontroll og gjennomgang av logg. En av loggens formål er å avdekke avvik i ettertid og at systemet dermed kan forebygge såkalt snoking og eventuelle forsøk på ulovlig inntrengning. Dersom det ikke eksisterer tekniske løsninger for rutinemessig og systematisk gjennomgang av loggen er risikoen for at avvik oppdages svært liten. Logg som forebyggende sikkerhetstiltak mister da sin effekt.

I etterkant av at kontrollene ble gjennomført har de fleste registrene gjennomgått og oppdatert sine rutiner for gjennomgang og kontroll av logg. Gjennomgangen er i de fleste registrene basert på en mer eller mindre manuell gjennomgang av loggen. Vi mener det er et stort potensiale for å få på plass automatiske systemer for gjennomgang og kontroll av logg, slik at dette verktøyet i større grad kan bidra til å avdekke forsøk på inntrengning og ureglementert bruk når det skjer og ikke lang tid etter at hendelsen har funnet sted.

3.2.3 Kryptering

Når det gjelder kravet til kryptering av sentrale helseregistre er det, etter at dette kravet kom inn i loven samtidig med at NPR ble føyd til rekken av lovregulerte registre, ulike løsninger som er valgt for å tilfredsstille kravet. De nyeste registrene har løsninger for separat lagring av helseopplysninger og identitet, mens eldre registre preges av behov for omfattende endringer og modernisering for å få på plass det man i dag forventer når et er snakk om kryptering. Alle registrene hadde skallkryptering som et minimum.

Vi mener det er stort potensial for forbedringer også på dette området, men vi har ikke funnet at noen av registrene opererer i strid med kravet til kryptering, slik det ble fortolket i etterkant av at bestemmelsen ble inntatt i lovverket.

3.2.4 Bruk av skytjenester

Ingen av registrene har tatt i bruk skylagringstjenester. Bruk av databehandlere er heller ikke utbredt, og vi har ikke funnet vesentlige avvik i de tilfellene der det finnes slike avtaler, men et register ble pålagt å oppdatere eksisterende databehandleravtale.

3.3 De registrertes rettigheter

Vår hypotese før denne kontrollen ble gjennomført var at vi mente at de registrerte i registrene, altså allmennheten, i for liten grad hadde kjennskap til registrene og hvilke opplysninger som finnes der. Vi antok derfor at det vil være et viktig tiltak for å redusere personvernulempen for de registrerte å sikre kjennskap til registrene slik at de registrerte i større grad enn i dag kan benytte seg av sine rettigheter til innsyn, krav som sletting/retting, reservasjon mv.

Vi var derfor særlig opptatt av å finne ut hvordan og i hvilken grad registrene sikret etterlevelse av plikten til å informere allmennheten jf. helseregisterloven § 23. Vi ba også om oversikt over antall innsynsbegjæringer og andre krav fra registrerte de siste to år før kontrollen, samt registerets rutiner for håndtering av slike krav.

Som ventet fant vi mangelfulle rutiner og strategier for informasjon til allmennheten hos alle registrene. Noen registre hadde relativt god informasjon tilgjengelig for allmennheten, men det manglet dokumentasjon som viste en bevisst strategi for ivaretakelse av denne plikten. I registerforskriftene er det en egne bestemmelser[1] som pålegger registrene å utarbeide informasjonsstrategi tilpasset deres brukergrupper for å fremme bruken av registeret. I HKR-forskriften § 3-6 er det presisert at informasjonsstrategien også skal rettes mot publikum. Forskriftene til Reseptregisteret, IPLOS og Forsvarets helseregister har ikke egne bestemmelser om informasjonsstrategi.

De fleste registrene har lagt ressurser i å utarbeide informasjonsmateriell til helsepersonell, forskere og andre som ønsker data fra registrene, mens informasjon til allmennheten ikke har vært prioritert på samme måte. Vårt inntrykk etter kontrollene, var at de fleste registrene ikke var klar over plikten de har til å informere i samsvar med helseregisterloven § 23.

I tabellen nedenfor kan man se oversikt over de enkelte registrene, antall registrerte totalt, nye registrerte per år og antall krav om innsyn fra de registrerte. Nederste linje viser totalt antall utleveringer av data etter søknad til registrene per år.

	NPR	Forsvaret	KRG*	Resept	DÅR	HKR	MFR**	SYSVAK	MSIS	IPLOS
Registrerte	5.073’	2.762’	4.365’	3.577’	2.596’	702’	5.649’	4.029’	278’	826’
Nye 2015	370’	67’	131’	121’	41’/40’	162’	115’	921’	15’/13’	57’
Innsynskrav 2014/15	22/24	0	11	5/1	30/31	2/2	13/19	109’	2/0	0/4
Krav om retting osv.	0	0	0	0	0	0	0	-	0	0/1
Utleveringer	863	12	170	114	142	30	104	189	13	34

*KRG inkludert screeningprogrammene

**Mødre, fedre og barn

[1] Kreftregisterforskriften § 3-6, NPR-forskriften § 3-11, HKR-forskriften § 3-6, MFR-forskriften § 3-6, DÅR-forskriften § 3-6, MSIS-forskriften § 4-6, SYSVAK-forskriften § 3-6.

Tabellen viser at alle registrene unntatt SYSVAK i svært liten grad mottar krav om innsyn fra de registrerte. Det har i all hovedsak ikke kommet krav om retting og sletting de siste to år før kontrollen. Når det gjelder SYSVAK må det understrekes at krav om innsyn her inkluderer innsyn i egne vaksiner på Vaksinetjenesten på helsenorge.no. Dette registerets formål er med andre ord annerledes enn de øvrige registrene fordi det har en nettbasert tjeneste som er rettet direkte mot publikum. Registeret blir også brukt i helsetjenesten når det er behov for vaksinasjonsstatus hos en pasient.

Basert på disse tallene mener vi at det er en lang vei å gå når det gjelder informasjonsarbeid overfor befolkningen og den generelle bevisstheten om hva som skjer med våre helsedata. Vi mener et avgjørende tiltak for å sikre bedre personvern i Norge er å sørge for at befolkningen blir kjent med omfanget av registreringer og omfanget av meldepliktige registre som mottar opplysninger fra våre journaler uten hensyn til taushetsplikt.

Vi mener det er gode grunner til å stille spørsmål til om befolkningens lave interesse for hva som står om dem i helseregistre skyldes en uforbeholden tillit til helsetjenesten og offentlige myndigheter generelt, eller om det kan skyldes manglende kunnskap om det totale omfanget av sekundær bruk av helseopplysninger.

I den nye personvernforordningen er kravet til rettferdig behandling av personopplysninger nedfelt og tydeliggjort som et viktig prinsipp for å sikre lovlighet ved behandling. Kjernen i prinsippet er at behandling av personopplysninger skal være gjennomsiktig, forutsigbar og rettferdig i den forstand at de registrerte skal kunne ivareta sin rettigheter så langt det er mulig avhengig av inngrepets natur og formålet med behandlingen. Når så få mennesker ber om innsyn i sine opplysninger, samtidig som registrene i utstrakt grad benyttes til andre formål og utleverer data i stort monn til forskning og styringsformål, mener vi at det er grunn til å spørre om de registrerte har vært informert på en måte som har gjort dem i stand til å ivareta sin interesser i forhold til de sentrale helseregistrene.

Vi ser det som svært positivt at det pågår et viktig arbeid i regi av Direktoratet for eHelse (helsenorge.no), der målet er å samle viktig informasjon om helseregistre og bruk av helsedata i en informasjonstjeneste rettet mot befolkningen. Vi tror derfor at situasjonen slik den var i 2016 litt etter litt blir bedre og at økt informasjon til befolkningen kan bidra til at den enkelte i større grad blir informerte nok til å være i stand til å benytte seg av sine personvernrettigheter.

4 Oppsummering

De sentrale helseregistrene kunne i 2016 dokumentere at det var gjort et omfattende arbeid for å etablere en tilfredsstillende internkontroll. Vi mener utfordringen i det videre arbeidet ligger i en profesjonalisering og forankring av sikkerhetsarbeidet og oppfølging av internkontrollen og i å utvikle og implementere internkontrollen slik at den blir tilgjengelig for de ansatte og en naturlig del av den daglige virksomheten i registeret.

Når det gjelder informasjonssikkerhet er vår vurdering at det generelt er en del å gå på når det gjelder moderne informasjonsteknologi og løsninger for optimalt sikkerhetsarbeid.

De fleste registrene har løsninger som er i tråd med gjeldende regelverk på kontrolltidspunktet, men tatt i betraktning de verdiene som forvaltes i registrene kan man fra et informasjonssikkerhetsperspektiv legge til grunn at det er et stor potensiale for modernisering og bedre tekniske sikkerhetsløsninger.

Når det gjelder registrenes plikt til å ivareta de registrertes personvern er vår klare oppfatning at informasjon er det viktigste hjelpemidlet de har for å gjøre de registrerte i stand til å benytte seg av

sine rettigheter når registeret i utgangspunktet ikke krever samtykke fra de registrerte. Manglende strategier for informasjon til allmennheten er det vi mener er det viktigste funnet ved disse kontrollene og det området vi mener det viktigst å ta tak i og gjøre bedre i fremtiden.

Vi understreker at alle registrene allerede har tatt tak i våre varslede funn og situasjonen er bedre enn den var. Kontinuerlig bevissthet rundt plikten til å ivareta de registrertes rettigheter er i tillegg til tilfredsstillende sikkerhetstiltak, det viktigste registrene må fokusere på når det gjelder å forbedre de registrertes stilling. Særlig i et samfunn der svært store mengder sensitive personopplysninger behandles for andre formål enn det den registrerte er kjent med. Vi mener dette er avgjørende for å opprettholde nødvendig tillit fra befolkningen.

Den demokratiske prosessen som ligger til grunn for et lovvedtak om etablering av et helseregister er ikke en prosess som involverer allmennheten på en måte som tilsier at Ola og Kari dermed er kjent med hva lovforslaget innebærer. Det er dermed opp til de behandlingsansvarlige å sikre at personverninteresser faktisk ivaretas gjennom daglig drift og forvaltning av registrene.