CompLex

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Henrik Ulseth og Petter Teie Hellum

Vurdering av Helseetatens etterlevelse av Normens krav til konfidensialitet og tilgangsstyring

Forslag til utbedringer av mangler i etterlevelsen av kravene til autentisering, autorisering, tilgangsstyring og konfidensialitet i Profdoc Vision

2/2020

UiO : Det juridiske fakultet

Henvendelser om denne bok kan gjøres til:
Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
http://www.jus.uio.no/ifp/om/organisasjon/seri/

ISBN 978-82-72261-72-5
ISSN 0806-1912

Grafisk produksjon: 07 Media AS – 07.no

Forord

Denne artikkelen ble opprinnelig skrevet og levert som en masteroppgave i Forvaltningsinformatikk ved Juridisk fakultet på UiO, våren 2020. Vi har ikke gjort nevneverdige endringer i teksten i etterkant, og oppgaven publiseres tilnærmet slik den fremstod ved innlevering.

I avhandlingen så vi nærmere på informasjonssikkerheten hos Kommunal akutt døgnenhet i Oslo kommune. Konkret undersøkte vi tilgangsstyringen i pasientjournalsystemet de benyttet, og vurderte denne opp mot kravene som fremgår av Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren. Vi vurderte hvor egnet tilgangsstyringen deres var til å ivareta krav til konfidensialitet og tilgjengelighet. Ved mangler i etterlevelsen utformet vi konkrete forslag til utbedringer.

Et pasientjournalsystem er juridisk regulert, er bygget opp teknologisk etter tekniske og juridiske spesifikasjoner, og skal bidra til et bedre helsetilbud. Vi vurderte derfor egnetheten fra et forvaltningsinformatisk perspektiv. Dette betyr at vi undersøkte tilgangsstyringen med utgangspunkt i juridiske, samfunnsvitenskapelige og informatiske innfallsvinkler.

Avslutningsvis ønsker vi å takke veilederen vår, Eilif Hjelseth, for gode innspill og støtte underveis i arbeidet.

Oslo, 24. august 2020

Henrik Ulseth og Petter Teie Hellum

Innhold

1 Innledning

1.1 Bakgrunn og aktualitet

Så godt som alle i Norge har på en eller annen måte hatt kontakt med helsevesenet, enten den private eller offentlige delen. De fleste som blir født i Norge kommer til verden ved et sykehus,[1] og hver innbygger hadde i snitt 2,7 konsultasjoner hos fastlege i 2018.[2] Både private og offentlige helseforetak bruker store summer på behandling, rehabilitering, diagnostisering og andre tilstøtende tjenester.[3] Helsevesenet hjelper oss gjennom de vanskeligste stundene i livet, og er der også i de vakreste øyeblikkene. Liv blir til, liv går bort, og helsepersonellet[4] jobber utrettelig for å hjelpe pasienter, brukere og pårørende i alle livets faser.

En forutsetning for å kunne hjelpe pasientene på best mulig måte er helsepersonellets tilgang på god, oppdatert informasjon om pasientens sykdomsbilde og helsesituasjon. For å få riktig behandling er vi vant med å måtte dele personlige og til tider intime detaljer med helsepersonell. Fordi medisinfaget er så komplekst, må informasjon gjerne deles mellom ulike spesialister og helsepersonell, som sammen utreder, stiller diagnoser, behandler og rehabiliterer. Det kan oppstå situasjoner hvor du må få behandling uten at du selv er i stand til å fortelle om en medisinallergi du har. Det kan også tenkes at sykdomsbildet ditt er så sammensatt at legen må studere sykdoms- og familiehistorikken din for å finne ut av hva som bør gjøres. I alle slike tilfeller må informasjon oppbevares, struktureres og deles mellom ulike personer i helsevesenet.

Oppbevaringen av informasjonen er livsviktig, men den kan også være problematisk. Tenk hvis uvedkommende får vite om de høyst personlige detaljene du delte med legen din? Hva kan dette føre til for deg? Eller i et større bilde; hva kan det bety for folkehelsen om vi ikke stoler på dem som skal hjelpe oss? Tap av tillit kan føre til at vi ikke tør å dele informasjonen som helsepersonellet er så avhengig av for å yte god hjelp, eller det kan føre til at noen ikke tør å oppsøke helsehjelp i det hele tatt.

Helsepersonell har i lang tid jobbet for å bevare den høyst nødvendige tilliten mellom pasient og behandler. Den Hippokratiske ed er et tidlig eksempel på en

1 Johansen, Iversen og Broen (2017).
2 Statistisk sentralbyrå (2019).
3 Monsrud (2020).
4 Helsepersonell: Se helsepersonelloven § 3 første ledd.

legeed som skal binde leger og andre behandlere til en etisk standard.[5] Den inneholder blant annet et løfte om taushet:

> *«Det jeg måtte se eller høre under behandlingen eller også utenfor behandlingen ute blant folk, som ikke bør bringes videre, skal jeg tie om og regne som hellige hemmeligheter.»*[6]

Også i dag er helsepersonell underlagt lovpålagt taushetsplikt.[7] Helsevesenets behov for informasjon har ikke blitt mindre siden år 500 f.v.t. Snarere tvert imot. Både behovet for og tilgangen på informasjon har økt i takt med at leger og andre diagnostiserer og behandler stadig mer komplekse lidelser.

Vi skal undersøke hvordan Kommunal akutt døgnenhet (KAD) i Oslo kommune jobber for å bevare tilliten, samtidig som de balanserer dette mot behovet for rask og nøyaktig tilgang til livsnødvendig informasjon. Vi skal studere hvilke systemløsninger de har på plass i dag, og hvor egnet løsningene er til å beskytte både opplysninger og pasienter, samtidig som de muliggjør effektiv behandling.

Kommunal akutt døgnenhet er en del av Oslo kommunes offentlige helsetilbud.[8] KAD er i dag plassert på tomta til Aker sykehus, og er underlagt Helseetaten.[9] KAD gir pasienter et tilbud om innleggelse for observasjon, pleie og behandling av avklarte diagnoser. Det finnes flere kriterier for hvilke pasienter som kan legges inn på KAD. Blant annet må pasienten være over 18 år, og ha vært tilsett av lege forut for innleggelse. Videre skal pasientens helsetilstand være avklart, og det skal antas å være liten risiko for at helsetilstanden kan forverres.[10] KAD skal i hovedsak dekke etterspørselen etter et tilbud til pasienter som er for syke til å være hjemme, men som ikke nødvendigvis trenger innleggelse på ordinære sykehus. Slik kan sykehusene avlastes og konsentrere seg om de pasientene med mer kompliserte eller sammensatte behov.

I denne avhandlingen skal vi se nærmere på informasjonssikkerheten hos KAD. Vi vil konkret se nærmere på tilgangsstyringen i pasientjournalsystemet de benytter,[11] og vurdere hvor egnet den er til å ivareta krav til konfidensialitet og

5 Holck (2020).
6 Holck (2020).
7 Se blant annet Helsepersonelloven § 21.
8 Oslo kommune (2020).
9 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
10 Oslo kommune (2018).
11 Pasientjournalsystem: Et system der helseopplysninger er lagret systematisk, slik at opplysninger om den enkelte kan finnes igjen. Opplysningene skal danne grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner, jf. pasientjournalloven § 2 første ledd bokstav d.

tilgjengelighet.[12] Et pasientjournalsystem er juridisk regulert, er bygget opp teknologisk etter tekniske og juridiske spesifikasjoner, og skal bidra til et bedre helsetilbud. Vi vil derfor vurdere egnetheten fra et forvaltningsinformatisk perspektiv. Dette betyr at vi vil undersøke tilgangsstyringen med utgangspunkt i juridiske, samfunnsvitenskapelige og informatiske innfallsvinkler.

Behovet for god tilgang til helseopplysninger kontra behovet for beskyttelse av pasientens personvern og integritet er en meget interessant problemstilling, som settes på spissen i helsevesenet. De ansatte i helsevesenet jobber dag og natt for å hjelpe oss, hvilket har blitt særlig aktualisert nå i disse dager.[13] Vi skal i avhandlingen undersøke om systemene de benytter kan utbedres, slik at alle kan få et tryggere og mer tillitsvekkende helsevesen. I tillegg til å undersøke utbedringspotensialene kommer vi med konkrete forslag til hva som bør utbedres, samt hvordan det kan gjøres. Vi vil også legge frem en plan for hvordan Helseetaten kan arbeide videre på dette feltet.

1.2 Tema og forskningsspørsmål

1.2.1 Tema

Vi skal i avhandlingen undersøke Helseetatens evne til å ivareta konfidensialiteten gjennom tilgangsstyring i pasientjournalsystemet Profdoc Vision. For å gjøre dette har vi brukt kravene fastsatt i *Norm for informasjonssikkerhet og personvern i helse- og omsorgstjenesten* (heretter Normen). Vi har utformet to forskningsspørsmål vi ønsker å svare på gjennom avhandlingen:

1. I hvilken grad etterlever Helseetatens elektroniske pasientjournaler Normens krav til konfidensialitet?
2. Hvilke tekniske eller organisatoriske tiltak kan utbedre eventuelle mangler i etterlevelsen av Normens krav til konfidensialitet?

12 Se kapittel 2.2. Konfidensialitet og tilgjengelighet.

13 Avhandlingen ble skrevet våren 2020, midt under COVID-19-pandemien som traff Norge og verden.

1.2.2 Forskningsspørsmål

Undersøkelsene i denne studien består av to forskningsspørsmål, som bygger på hverandre. Se *figur 1, nedenfor.*

Forskningsspørsmål 1:

I hvilken grad etterlever Helseetatens elektroniske pasientjournaler Normens krav til konfidensialitet?

Normen har 294 krav til informasjonssikkerhet. Som forskningsspørsmålet ovenfor tilsier, ønsker vi å undersøke Profdoc Visions etterlevelse av kravene. Av kravene har vi valgt ut 44. Utvalget er gjort basert på hvilke krav vi anser som mest relevante for å kontrollere tilgangsstyringens evne for å ivareta konfidensialitet.[14] Som første del av forskningsspørsmålet tilsier ønsker vi å undersøke graden av etterlevelse. Med dette mener vi hvor mange krav de oppfyller og i hvilken grad det enkelte krav er oppfylt.

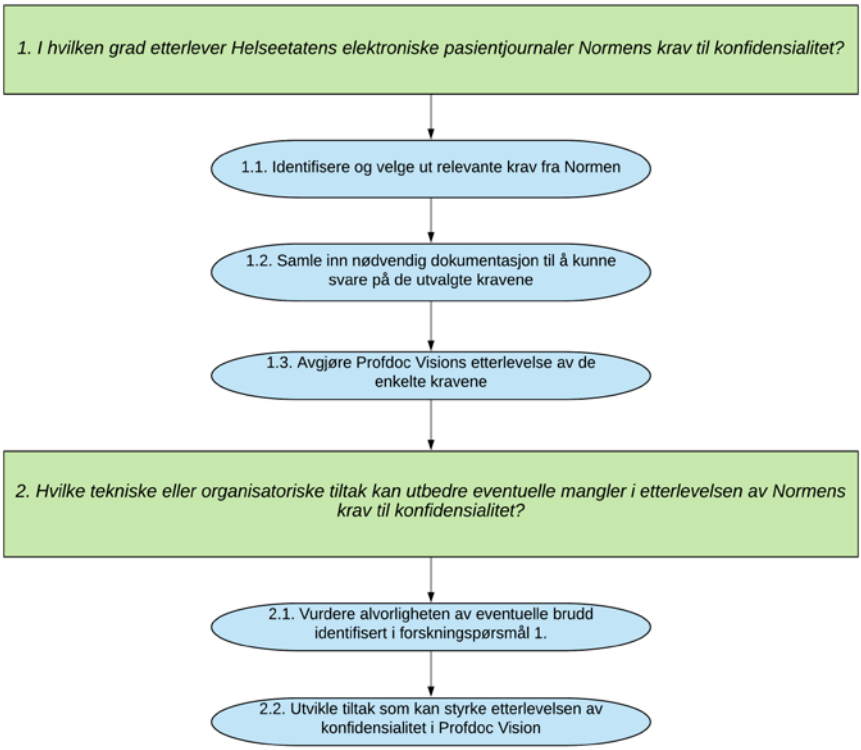
Forskningsspørsmål 2:

Hvilke tekniske eller organisatoriske tiltak kan utbedre eventuelle mangler i etterlevelsen av Normens krav til konfidensialitet?

Dersom forskningsspørsmål 1 avdekker hull og mangler i Helseetatens tilgangsstyring, vil vi gjennom å svare på forskningsspørsmål 2 finne tekniske eller organisatoriske tiltak som kan utbedre manglene i etterlevelsen av Normen. Med tekniske tiltak sikter vi til tiltak som gjøres for å endre systemet, som for eksempel å modifisere programvare eller å endre kravene til passord. Organisatoriske tiltak er derimot endringer som kan gjøres i virksomheten som omkranser den tekniske delen av systemet. Vi snakker her om rutiner for å logge ut av systemet etter bruk, opplæring av de ansatte, gjennomføring av risikoanalyser, og lignende.

«*Figur 1: Undersøkelsessteg*» nedenfor viser sammenhengen mellom de to forskningsspørsmålene, som står skrevet inne i de grønne boksene. De har i tillegg tilhørende undersøkelsessteg som er nødvendige for å komme frem til et svar på forskningsspørsmålene. Undersøkelsesstegene står skrevet inne i de blå ovalene. Som figuren viser, fører forskningsspørsmålene frem til de ulike undersøkelsesstegene. Dette er illustrert med piler.

14 Les mer om dette i kapittel «5.1. Utvalgskriterier for kravene fra Normen».



Figur 1: Undersøkelsessteg.

Vi ønsker gjennom figur 1 ovenfor å tydeliggjøre de nødvendige stegene for å svare på forskningsspørsmålene, samt relasjonen mellom disse. Vi mener dette i hovedsak er en stegvis prosess. Det vil likevel være nødvendig å gå tilbake til tidligere steg for å gjøre endringer etter hvert som vi utvikler bredere kunnskap og forståelse av systemet.

For å svare på forskningsspørsmål 1 anser vi det nødvendig å gjennomføre tre undersøkelsessteg. Det første steget er å identifisere og velge ut de kravene fra Normen vi anser som relevante for avhandlingen. Det andre undersøkelsessteget er å samle inn tilstrekkelig dokumentasjon fra Helseetaten til å kunne beslutte om de valgte kravene er oppfylt i Profdoc Vision. Det tredje undersøkelsessteget er å bruke dokumentasjonen til å beslutte om Profdoc Vision etterlever de utvalgte kravene fra Normen.

Avhengig av antallet og størrelsen på manglene vi avdekker gjennom forskningsspørsmål 1, kan vi bli nødt til å velge ut de vi anser som viktigst å utbedre. Vi er dermed nødt til å vurdere alvorligheten av de eventuelle manglene vi identifiserer i forskningsspørsmål 1, og deretter utbedre de vi anser som de mest problematiske. Også ved utvikling av tiltakene vil målet være å styrke konfidensialiteten i systemet. Likevel må vi alltid balansere konfidensialiteten mot andre verdier som også er viktig for Helseetaten.

1.3 Metode

Metode er strategien forskeren bruker for å samle inn data om virkeligheten. Ifølge Dag Ingvar Jacobsen dreier metode seg om hvordan forskeren kan samle inn empiri om virkeligheten på en troverdig måte.[15] Hensikten med forskning er å frembringe gyldig og troverdig kunnskap. Metoden forskeren har brukt er dermed avgjørende for kvaliteten på forskningen.

Forskningsspørsmålene i kapittel «1.2.2. Forskningsspørsmål» er av en tverrfaglig karakter, og vi har benyttet oss av både samfunnsfaglige og juridiske metoder for informasjonsinnsamling. I hovedsak har vi samlet inn kvalitative data. Dette er data som inneholder meninger, og de blir oftest formidlet via språk og handlinger.[16]

Videre i dette delkapittelet vil vi se nærmere på hvilke vurderinger og utfordringer vi har støtt på gjennom prosessen med utarbeidelsen av avhandlingen.

1.3.1 Dokumentanalyse og litteraturstudie

Dokumentundersøkelser handler om å benytte seg av informasjon som er skrevet eller samlet inn av andre.[17] Vi har brukt dokumentanalyse og litteraturstudie aktivt for å samle inn nødvendig informasjon til å kunne svare på forskningsspørsmål 1. I innsamlingsfasen lette vi etter relevante dokumenter, og vi var særlig ute etter dokumenter som stilte krav til informasjonssikkerhet i helsevesenet generelt og i pasientjournaler spesifikt. For å skaffe tilstrekkelig datagrunnlag, har vi i denne fasen kartlagt lover, instrukser og veiledere. Vi har også benyttet faglitteratur og offentlige rapporter. Etter kartleggingen av rettsområdet systematiserte vi informasjonen, og gjorde et utvalg utfra hva vi anså som mest relevant for vår avhandling.

15 Jacobsen (2015) s. 15
16 Jacobsen (2015) s. 125
17 Jacobsen (2015) s. 188

En utfordring med undersøkelsene vi har gjort er at dokumentasjonen som omhandler informasjonssikkerhet i helsevesenet ofte er generell og uklar. Informasjonssikkerhet handler blant annet om å kartlegge risikoer og svakheter i et konkret system, og deretter tilpasse systemet eller organisasjonen rundt systemet for å minimere sannsynligheten for, eller konsekvensen av, de kartlagte risikoene. Litteratur som omhandler informasjonssikkerhet er derfor ofte utformet i generelle ordelag, for å kunne tilpasses ulike systemer og utfordringer. Bearbeidelsen av litteraturen innebærer derfor en del tolkningsarbeid.

I avhandlingen har vi undersøkt en rekke skriftlige kilder som omhandler informasjonssikkerhet i helsevesenet. Vi har brukt Normen og lovtekst mye, men også faglitteratur på helserettsområdet. Normen inneholder en rekke krav til informasjonssikkerhet og personvern i helsevesenet, men de fleste av kravene er konkretiseringer og fortolkninger av eksisterende lovverk. Det betyr at Normen ikke kan regnes som primærkilde, og at kravene er fortolkninger gjort av andre.

Ordlyden i det første forskningsspørsmålet lener seg fullstendig på Normen. Vi har gjennomgående vært bevisste på at Normen er en fortolkning av lovverk, og at lovverket må anses som primærkilden. Av den grunn har vi kontinuerlig undersøkt hjemmelsgrunnlaget for de enkelte kravene, og gjort egne fortolkninger og vurderinger av lovkravet. Vi har deretter holdt vurderingene opp mot Normens krav, og sett til at det er overenstemmelse mellom hva vi mener loven sier, og hva Normen sier.

I tillegg til å kontrollere Normens krav opp mot lovhjemmelen, har vi gjennomgående benyttet annen litteratur som omhandler konfidensialitet, tilgjengelighet og informasjonssikkerhet i helsevesenet. Vi har blant annet benyttet ulike kommentarutgaver av relevant lovverk, faglitteratur på helserettsområdet, offentlige informasjonssikkerhetsveiledere mv.

1.3.2 Kvalitative intervjuer

Vi har gjennomført to kvalitative intervjuer. Disse var viktige for å få tilstrekkelig informasjon til å svare på forskningsspørsmål 1. Som tidligere nevnt var forskningsspørsmål 2 avhengig av et svar på spørsmål 1, og vi kunne derfor heller ikke svart på dette uten informasjonen fra intervjuene. Det første intervjuet var et innledende og generelt intervju om informasjonssikkerheten i Profdoc Vision. Det andre intervjuet fokuserte på tilgangsstyring og konfidensialitet i Profdoc Vision.

Det første intervjuet var et åpent semistrukturert intervju. Den åpne formen var nyttig tidlig i prosjektet. Vi hadde få holdepunkter og lite kjennskap til informa-

sjonssikkerheten hos Helseetaten, og var avhengige av å skaffe kunnskap på et felt vi på forhånd hadde begrenset detaljkunnskap om. De åpne spørsmålene muliggjorde utfyllende svar fra intervjuobjektet som tilførte samtalen mer enn vi i utgangspunktet spurte om. Den åpne intervjuformen, i tillegg til at intervjuet fant sted tidlig i prosjektprosessen, ga oss fleksibiliteten til å stille oppfølgingsspørsmål på svar vi fant spesielt interessante og dermed ønsket å få utdypet. Dette intervjuet har vært avgjørende for utformingen av forskningsspørsmålene. Det var også fordelaktig at intervjuet ble gjennomført ansikt til ansikt. Dette bidro til at samtalen fløt bedre, og at kroppsspråket kom tydeligere frem enn hva som ville vært tilfellet ved bruk av video-intervju. Muligheten til å bruke kroppsspråk kan føre til større tillit mellom intervjuer og intervjuobjekt, og kan øke graden av åpenhet mellom partene.[18]

Helseetaten ønsket før gjennomføringen av det andre intervjuet å få oversendt spørsmålene, slik at de kunne kontrolleres. Begrunnelsen for dette var at de ikke ønsket å oppgi informasjon som kunne skade informasjonssikkerheten deres. Spørsmålene vi skulle stille ble derfor på forhånd oversendt til intervjuobjektet og hennes overordnede, og det var i mindre grad mulig å stille oppfølgingsspørsmål som dukket opp underveis. Intervjuet bar preg av å være strukturert etter en på forhånd fastsatt spørsmålsrekkefølge. Spørsmålene var i større grad lukket og målrettet formulert, fordi vi på forhånd visste hva vi ønsket informasjon om. Det var i midlertidig noe rom for å stille enkelte oppfølgingsspørsmål der vi anså det nødvendig. Vi vurderer derfor ikke den sterke struktureringsgraden som veldig problematisk. Intervjuet ble gjennomført som en samtale over nett, på grunn av retningslinjer tilknyttet Covid-19-utbruddet i Norge. I løpet av intervjuet fikk intervjuobjektet trøbbel med kameraet på PC-en sin. Hun kunne se oss, men vi kunne bare se henne i noen få minutter i begynnelsen av intervjuet.

I etterkant av intervjuene har vi hatt dialog med intervjuobjektene der det var nødvendig med en utdypning av de opprinnelige svarene.

Til tross for at vi anser kvalitative intervjuer som det mest hensiktsmessige metodevalget for avhandlingen, finnes det svakheter ved bruk av metoden. Jacobsen skriver at slike undersøkelser kan være ressurskrevende, generaliserende, eller ha en for stor grad av kompleksitet eller nærhet. [19] I tillegg kan undersøkelseseffekten påvirke funnene, og fleksibilitetsutfordringer kan føre til at problemstillingen flyter utenfor rammene sine. [20]

18 Jacobsen (2015) s. 148.
19 Jacobsen (2015) s. 131-132.
20 Jacobsen (2015) s. 131-132.

Vi har særlig opplevd at kvalitative undersøkelser er ressurskrevende. For å svare på forskningsspørsmålene våre var vi avhengige av detaljert kunnskap om tilgangsstyringen ved KAD. Det andre intervjuet ble derfor langt. Likevel var intervjuet avgjørende for å få frem tilgangsstyringens nyanser.

En potensiell svakhet i avhandlingen er at vi ikke har gjennomført kontrollen med flere ansatte i Helseetaten. Kontrollen vi har gjennomført er derfor basert på svarene fra én person. Alle har subjektive oppfatninger av virkeligheten. Det gjelder også for fenomenet vi undersøker. Svarene som gis vil naturlig nok farges av intervjuobjektets kunnskap og meninger om fenomenet, og vil ikke alltid samsvare med hva andre ville vektlagt. Vi vil imidlertid påpeke at svarene i hovedintervjuet ble gitt i samråd med informantens overordnede. Svarene er derfor preget av at to ansatte i organisasjonen med dyptgående kunnskap om temaet har undersøkt spørsmålene og utarbeidet svar. Tidlig i prosessen ønsket vi å intervjue helsepersonell for å få deres synspunkter og innspill, samt å se Profdoc Vision i bruk hos KAD. Dette ble skrinlagt på grunn av avhandlingens omfang. På grunn av covid-19-utbruddet var det heller ikke mulig å være fysisk tilstede for å studere Profdoc Vision i bruk. Vi ønsket heller ikke å belaste helsepersonell ytterligere i en allerede presset situasjon.

På grunn av store datamengder har vi sett behovet for å lage kvantitative oversikter over funnene våre. Se kapittel «5.5. Statistikk til tabell». Dette gjorde vi både for hjelp i egen analyse av etterlevelsen av Normens krav, men også for å kunne gi en visuell, oversiktlig fremstilling av funnene. Vi har vært bevisste på verdien av de kvantitative oversiktene. De kan gi et overblikk, men viser samtidig ikke nyansene. Oversikten viser for eksempel ikke alvorligheten av det enkelte brudd. Oversiktene er dermed kun et supplement og ville ikke vært tilstrekkelige alene.

1.3.3 Kildekritikk og forskningsetikk

Vi har brukt et variert og stort utvalg av kilder. I dokumentundersøkelsen har vi som tidligere nevnt benyttet en rekke kildetyper. Ved valg av kilder må det alltid vurderes i hvilken grad en kan stole på kilden. Utvalget av kilder blir i så måte helt sentralt for reliabiliteten i avhandlingen.[21]

Jacobsen skriver at den generelle kildekvaliteten særlig er knyttet til hvilken kunnskap og kompetanse den som har skrevet ned informasjonen innehar.[22] På bakgrunn av dette har vi forsøkt å velge kilder med høy generell kvalitet. Vi har for eksempel kontrollert normkravene opp mot de aktuelle lovkravene og aner-

21 Jacobsen (2015) s. 188.

22 Jacobsen (2015) s.190.

kjent faglitteratur på området. På denne måten har vi vurdert flere synspunkter, og ikke kun lent oss på én kilde.

Vi valgte informantene fordi vi mente at de ville tilføre avhandlingen verdifull og god informasjon. Begge intervjuobjektene er kunnskapsrike om fenomenet vi har undersøkt, og innehar sentrale roller i systemet. Jacobsen skriver at ved bruk av institusjonelle kilder må troverdigheten til institusjonen vurderes. Det må vurderes hvorvidt institusjonen har en egeninteresse av å forvrenge informasjonen. [23] Vi mistenker ikke at Helseetaten har hatt et ønske om å gjøre dette. Likevel må vi som forskere være bevisste på lojaliteten mellom arbeidstaker og arbeidsgiver ved denne typen undersøkelser. Vi må derfor alltid vurdere om intervjuobjektene holder igjen eller forvrenger informasjon for å beskytte enten seg selv eller arbeidsgiver, bevisst eller ubevisst. Vi gjennomførte derfor enkelte stikkprøver for å kontrollere informasjonen.

1.4 Oversikt over den videre fremstillingen

Avhandlingen er bygd opp på følgende måte:

I kapittel 2 presenterer vi avgjørende elementer som vi mener at leseren bør ta med seg videre inn i avhandlingen for å få fullt utbytte av den. For det første beskriver vi pasientjournalsystemet Profdoc Vision. Vi beskriver også hvilke krav og retningslinjer for informasjonssikkerhet som fantes i 1995, da systemets grunnarkitektur ble skapt. Pasientjournalsystemet spiller hovedrollen gjennom hele avhandlingen. Vi forklarer også begrepene konfidensialitet og tilgjengelighet, og hvorfor avveiningen mellom disse kan være vanskelig, men høyst nødvendig, og hvorfor de er så viktige for helsevesenet og pasientjournalsystemene. I kapittel 2 blir også tilgangskontroll beskrevet i korte trekk, og vi tydeliggjør hvilken rolle en slik løsning kan spille for ivaretakelsen av konfidensialiteten og tilgjengeligheten.

I kapittel 3 gjennomgår vi viktige momenter i Normen. Vi fokuserer særlig på den delen som omhandler tilgangskontroll. Som kapittelet vil vise oppstiller Normen en rekke krav til hvordan informasjonssikkerheten og personvernet i helsesektoren skal håndteres. Vi retter fokuset mot tilgangskontroll for å understøtte konfidensialiteten i pasientjournalsystemet Profdoc Vision, og benytter Normens krav for å kontrollere pasientjournalsystemet. Vi holder også Normens krav opp mot lovkravene de er utledet fra, samt relevant faglitteratur, for å

23 Jacobsen (2015) s.191.

forsikre oss om at vi tolker kravene korrekt. Kapittel 3 vil derfor danne grunnlaget for å forstå hvor kontrollene vi benytter stammer fra.

I 2016 gjennomførte Kommunerevisjonen en kontroll av tilgangsstyringen i pasientjournalsystemet Profdoc Vision. I kapittel 4 beskriver vi hva som ble kontrollert ved revisjonen, og vi gjennomgår kontrollens konklusjon. Kommunerevisjonens rapport og kapittel 4 danner et grunnlag for å forstå hvordan informasjonssikkerheten har blitt ivaretatt i Profdoc Vision ved KAD tidligere. Sammen med våre videre funn danner kapittelet og funnene fra revisjonen et bilde av utviklingen i informasjonssikkerheten i pasientjournalsystemet. Dette viser oss hva som er utfordrende ved informasjonssikkerhetsarbeid i helsesektoren. Kapittelet danner også et grunnlag for forståelse av tilgangskontrollen i Profdoc Vision og det arbeidet som er gjort her, og har gitt oss et solid fundament for videre undersøkelser.

I kapittel 5 viser vi hvilke undersøkelser vi har gjort og hvordan vi har arbeidet for å avdekke informasjonssikkerhetsstatusen, og særlig tilgangskontrollen, i Profdoc Vision våren 2020. Med utgangspunkt i Normens krav gjennomførte vi omfattende intervjuer og stikkprøvekontroller for å kartlegge hvorvidt Helseetaten, KAD og Profdoc Vision etterlever kravene fra Normen. Vi har gjort et utvalg av kravene som vi mener er best egnet til å kontrollere tilgangsstyringen i pasientjournalsystemet, og vi har kontrollert Profdoc Vision opp mot disse. I kapittelet presenterer vi også en tabell med funn fra kontrollen vi har gjennomført. Tabellen viser dagens etterlevelse av Normens krav, og den stiller dagens etterlevelse opp mot etterlevelsen ved kommunerevisjonens kontroll i 2016. Den viser tydelig progresjon, men samtidig avdekker den et forbedringspotensial.

I kapittel 6 bygger vi videre på funnene fra vår kontroll av Profdoc Vision. Vi gjennomgår her de mest betydningsfulle manglene i tilgangskontrollen og konfidensialiteten. Videre i kapittelet presenterer vi en rekke tiltak vi har utviklet. Tiltakene skal bistå Helseetaten med utbedring av manglene vi avdekket i kapittel 5.

I kapittel 7 presenterer vi en avsluttende konklusjon og anbefaling. Vi ønsker at funnene og tiltakene vi har utviklet faktisk skal være til hjelp, og vi har derfor utformet klare anbefalinger og «neste steg» for kommunen, for å hjelpe til med å strukturere det videre arbeidet med utbedringer av pasientjournalsystemet. Vårt håp er at avhandlingen skal bidra med noe positivt for pasienter, helsepersonell og kommunen, og vi har derfor lagt opp til at avhandlingen er et solid første steg i en lengre utbedringsprosess.

2 Tilgangsstyring for ivaretakelse av konfidensialitet og tilgjengelighet i pasientjournalsystemer

2.1 Profdoc Vision

Pasientjournalsystemet som blir brukt ved Kommunal akutt døgnenhet ved Aker sykehus heter Profdoc Vision og ble produsert av ComuGroup Medical (heretter CGM).[24] CGM ble etablert i 1987 og formålet var å utvikle programvare til helsevesenet slik at leger skulle bruke mindre tid på administrative oppgaver og mer tid på behandling av pasienter.[25] CGM har ifølge sine nettsider 4200 ansatte fordelt i 19 land.[26] Selskapet har utviklet en rekke tjenester innen e-helse. E-helse er en samlebetegnelse for bruk av informasjons- og kommunikasjonsteknologi for å forbedre effektivitet, kvalitet og sikkerhet i helse- og omsorgssektoren.[27] CGM tilbyr blant annet e-helse-systemer til legevakt, spesialisthelsetjenesten og helsestasjoner. Profdoc Vision er et pasientjournalsystem utviklet av CGM i 1995, og grunnarkitekturen er den samme i dag som da systemet først ble utviklet.[28] Systemet behandler personopplysninger av særlige kategorier, og spesielt gjelder dette opplysninger om personers helsetilstand.[29] Driftsansvaret for Profdoc Vision-systemet hos Helseetaten i Oslo kommune ble i 2018 overtatt av Sopra Steria. Tidligere var det EVRY som hadde dette ansvaret. Oppdraget består i å bistå Helseetaten med database-, server- og applikasjonsdrift av Profdoc Vision.[30]

Formålet med bruken av et elektronisk pasientjournalsystem er å gi helsepersonell rask, enkel og sikker tilgang til nødvendige opplysninger. Pasientjournalen er et av helsepersonellets viktigste arbeidsverktøy.[31] Helseetaten har ikke etablert et overordnet formål for bruken av Profdoc Vision, men henviser til formålene brukt i *Lov om behandling av helseopplysninger ved ytelse av helsehjelp* (heretter pasientjournalloven) og *Lov om helsepersonell m.v.* (heretter helsepersonelloven).

24 Kommunerevisjonen (2017).
25 CGM (Udatert).
26 CGM (Udatert).
27 Braut (2019).
28 Kommunerevisjonen (2017)
29 Jf. personvernforordningen artikkel 9(1).
30 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
31 Helse- og omsorgsdepartementet (2016).

Det fremkommer av pasientjournalloven § 1 at formålet med loven er todelt. Behandling av helseopplysninger skal for det første skje på en måte som gir pasienter og brukere helsehjelp av god kvalitet ved at relevante og nødvendige opplysninger på en rask og effektiv måte blir tilgjengelige for helsepersonell. I tillegg skal de vernes mot uvedkommende, og sikre pasienter og brukeres personvern, pasientsikkerhet, samt rett til informasjon og medvirkning.

Formålet til Helsepersonelloven er fastsatt i lovens § 1, og bestemmer at lovens formål er å bidra til sikkerhet for pasienter og kvalitet i helse- og omsorgstjenesten. I tillegg skal loven bidra til tillit til helsepersonell og helse- og omsorgstjenesten som helhet.

Vi tolker det dithen at formålet med Helseetatens bruk av Profdoc Vision er å understøtte formålene til de to lovene ovenfor. Profdoc Vision skal dermed bidra til å styrke etterlevelsen av verdiene som blir fremstilt i formålsparagrafene.

2.1.1 Krav til system i 1995 mot dagens krav

Grunnarkitekturen[32] i Profdoc Vision stammer fra 1995.[33] CGM, Helseetaten, Evry og Sopra Steria har siden den gang utviklet og utbedret systemet til slik det er i dag. Da systemets grunnarkitektur ble utviklet eksisterte det andre krav til informasjonssystemer, personvern og behandling av helseopplysninger enn hva det gjør i dag. Blant annet tok det 11 år før Normen formelt ble lansert.[34] Innebygget personvern[35] ble først omtalt i august 1995, og var ikke et lovkrav i 1995. Lover som direkte omhandlet behandling av helseopplysninger i pasientjournallover eksisterte ikke i 1995, og helsepersonelloven, som blant annet omtaler journalføringsplikten, trådte i kraft 1. januar 2001. I det hele tatt har det skjedd veldig mye på digitaliseringsfronten siden 1995.

Siden systemet opprinnelig ble bygget har det blitt vedtatt en rekke endringer innen helse- og personvernrett som stiller krav til systemet. Også Normens krav har blitt innført senere. Det er likevel viktig å understreke at vi ikke har noen holdepunkter for å si at manglende etterlevelse av enkelte krav fra Normen skyldes gammel grunnarkitektur bygget før Normen trådte i kraft, eller før innebygget personvern ble innført ved lov. Systemet har endret seg mye siden 1995, og det endres og oppdateres fortsatt. Helseetatens systemforvaltere utbedrer og tilpasser systemet jevnlig.

---

32 Encyclopædia Britannica (2017).

33 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

34 Direktoratet for e-helse (2020 A).

35 Datatilsynet (2018).

Vi har ikke sammenlignet systemet med nyere pasientjournalsystemer. Dette faller utenfor formålet med avhandlingen. Som en generell bemerkning, før vi går i gang med gjennomgangen av funnene fra våre undersøkelser, vil vi likevel påpeke at Oslo kommune, og særlig Byråd for finans, bør vurdere potensielle ulemper og konsekvenser av å fortsatt benytte et 25 år gammelt system. Denne vurderingen er særlig viktig når systemet behandler opplysninger som er så viktige både for pasienter og helsevesen.

2.2 Konfidensialitet og tilgjengelighet i pasientjournalsystemer

2.2.1 Hva er konfidensialitet og tilgjengelighet?

2.2.1.1 Konfidensialitet og taushetsplikt

Alt helsepersonell er underlagt taushetsplikt, både i helsepersonelloven §§ 21 og 21a, samt i pasientjournalloven §§ 15 og 16. Taushetsplikten er delt inn i både en passiv og en aktiv taushetsplikt, samt et forbud mot snoking. Både den passive og den aktive taushetsplikten finner du i helsepersonelloven § 21 og i pasientjournalloven § 15. Bestemmelsene er for øvrig identiske. Bestemmelsene sier at helsepersonell skal hindre andre i å få kjennskap eller adgang til helseopplysninger de får tilgang til gjennom sin rolle som helsepersonell. Dette innebærer både helseopplysninger de får kjennskap til gjennom jobb, og opplysninger de kan få kjennskap til på fritiden, dersom de fikk tilgang til dette på grunn av sin rolle. Et eksempel på det sistnevnte kan være at en venn spør deg om noe om sin egen helse, fordi vedkommende vet du er lege og muligens har svaret.

Den passive delen av taushetsplikten innebærer at du som helsepersonell ikke skal dele opplysninger med andre, eller hjelpe noen med å få tilgang til slikt. Den aktive delen av taushetsplikten innebærer at du skal hindre andre i å få tilgang. Dette betyr at du har en plikt til å aktivt gripe inn og stanse noen fra å få tilgang. Et eksempel på etterlevelse av den aktive taushetsplikten vil være at helsepersonellet låser datamaskinen sin hver gang de forlater den, eller at de makulerer papirnotater så snart de ikke har et tjenstlig formål. Et annet eksempel fremkommer i den såkalte «Narkotikapose-dommen».[36] En sykehuslege gnidde en pose med narkotika mellom hendene for å beskytte identiteten til en pasient ved å ødelegge DNA-spor, samtidig som at politiet stod ansikt til ansikt med legen og ba om å få overlevert posen. Denne hendelsen er et godt eksempel på en lege som går langt i å etterleve kravene i den aktive taushetsplikten, ved å hindre andre i å få kjennskap til taushetsbelagte opplysninger.

36 HR-2013-2333-A (Narkotikapose-dommen).

Offentlig ansatte helsepersonell er også underlagt taushetsplikten i *Lov om behandlingsmåten i forvaltningssaker* (heretter forvaltningsloven) §§ 13 – 13 f. Dette gjelder ikke for helsepersonell i private foretak. Taushetsplikten i forvaltningsloven er mer generell enn de i helselovgivningen. Den forvaltningsmessige taushetsplikten gjelder for personopplysninger generelt, og ikke konkret for helseopplysninger. I forvaltningsloven § 13 b første ledd nr. 3 åpnes det også for at opplysningene kan benyttes innad i forvaltningsorganet i større grad enn hva taushetsplikten i helsepersonelloven åpner for. I tillegg åpner taushetsplikten i forvaltningsloven § 13 b første ledd nr. 6 for at forvaltningsorganet anmelder eller gir opplysninger til politiet om lovbrudd der det er ønskelig etter blant annet allmenne hensyn. En slik vid åpning i taushetsplikten finnes ikke i helselovgivningen. Helsepersonell kan ha opplysningsrett, og i noen tilfeller opplysningsplikt, dersom de får kjennskap til enkelte opplysninger av alvorlig karakter. Opplysningsrett gir helsepersonellet en diskresjonær anledning til å videreformidle opplysninger de har fått kjennskap til. Opplysningsplikten vil på sin side ikke åpne for slikt skjønn, men pålegger i stedet helsepersonellet å dele opplysninger i visse tilfeller. Helsepersonells opplysningsrett og opplysningsplikt er hovedsakelig hjemlet i henholdsvis kapittel 5 og 6 i helsepersonelloven.

Den enkelte ansatte ved et helseforetak er som oftest en del av et større system. Det er også viktig at dette systemet er utformet på en måte som muliggjør at den ansatte kan overholde sin taushetsplikt. Virksomheter som yter helse- og omsorgstjenester er ansvarlig for å sørge for å organisere seg på en måte som gjør de ansatte i stand til å overholde taushetsplikten. Dette er lovpålagt etter helsepersonelloven § 16 første ledd. Også *Europaparlaments- og rådsforordningen (EU) 2016/679 av 27. april 2016* (heretter personvernforordningen)[37] krever gjennomførte tekniske og organisatoriske tiltak som sørger for tilstrekkelig sikkerhet for personopplysninger, jf. personvernforordning artikkel 5(1) f. Derfor er det viktig å skape en arbeidshverdag som tilrettelegges slik at de ansatte kan overholde taushetsplikten. Eksempler på slik tilrettelegging kan være at arbeidsplassen tar i bruk PC-skjermer som hindrer at sidemannen kan titte på skjermen din, eller at det blir satt av nok tid mellom pasienter til at legene kan rydde bort dokumenter som kan avsløre informasjon om pasienten som var inne til kontroll rett før. Det kan også være det vi retter særlig fokus mot i avhandlingen vår, nemlig at pasientjournalsystemet legger til rette for at de ansatte kan overholde kravene til konfidensialitet.

37 EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF.

2.2.1.2 Tilgjengelighet

Alt helsepersonell som yter helsehjelp i Norge er underlagt helsepersonelloven.[38] Helsepersonell defineres i lovens § 3 som personell med autorisasjon eller lisens etter § 48 eller § 49, eller annet personell som utfører helsehjelp. Elever og studenter som utfører helsehjelp er også inntatt i definisjonen. Helsepersonellovens forsvarlighetskrav, som finnes i lovens § 4, oppstiller krav til at helsepersonellet skal handle forsvarlig i sitt virke, og at de skal ta høyde for situasjonen og sin faglige kompetanse i det de yter helsehjelp. Forsvarlighetskravet er den mest sentrale bestemmelsen i helsepersonelloven, og har stor praktisk betydning for vurdering og tolkning av andre bestemmelser innen helseretten. Eksempelvis vil det være nødvendig med innhenting av informasjon om pasientens helsetilstand for å kunne stille diagnose. Dette kravet skjerpes i takt med inngrepets alvorlighetsgrad for pasienten og usikkerheten knyttet til indikasjonene helsepersonellet sitter på.[39]

For å kunne yte så god helsehjelp som mulig er helsepersonellet avhengig av å innhente informasjon om pasientene. Både epikrise,[40] medisinallergier, tidligere sykdom og sykdom i familie er eksempler på informasjon helsepersonellet kan dra nytte av i diagnostisering, behandling og rehabilitering av pasienter. Helsepersonellet fører journal for hver enkelt pasient,[41] og slike journaler (historikk) er viktig for videre behandling i det samme sykdomsforløpet eller ved en senere anledning. Dokumentasjonen i slike journaler består av opplysninger om en navngitt persons sykdomshistorikk, pasientens beskrivelse av situasjonen, behandlingsplan, opplysninger om behandling med legemidler, i tillegg til en rekke andre opplysninger.[42] Opplysningene i slike journaler kan ha stor nytteverdi for pasienter og helsepersonell, men det kan være svært belastende for pasienten dersom opplysningene kommer på avveie.

Helsepersonell er lovpålagt å behandle helseopplysninger om pasientene de yter helsehjelp[43] til. Alle som behandler helseopplysninger er underlagt taushetsplikt, i henhold til helsepersonelloven § 21, *Lov om helseregistre og behandling av helseopplysninger* (helseregisterloven) § 17, samt i pasientjournalloven § 15. Både helsepersonell og systemene opplysningene oppbevares i skal ivareta kravene til konfidensialitet etter helsepersonelloven § 21 mv.

38 Helsepersonelloven § 2, første ledd.
39 Befring og Ohnstad (2019) s. 43.
40 Braut (2020).
41 Jf. helsepersonelloven § 39.
42 Jf. pasientjournalforskriften § 6.
43 Jf. helsepersonelloven § 3 tredje ledd.

Den dataansvarlige[44] skal sørge for at relevante opplysninger gjøres tilgjengelig for helsepersonellet når dette er nødvendig for å kunne gi god helsehjelp.[45] Dette skal også gjøres overfor samarbeidende helsepersonell. Tilgjengeliggjøringen skal skje innenfor rammene av taushetsplikten (konfidensialitet), og den dataansvarlige er ansvarlig for å bestemme på hvilken måte opplysningene skal tilgjengeliggjøres.[46] Pasienten kan motsette seg deling og behandling av helseopplysninger om seg selv.[47] Reglene for samtykkekompetanse gjelder også i slike tilfeller.[48]

2.2.1.3 Avveining mellom konfidensialitet og tilgjengelighet

Både opplysningers tilgjengelighet og konfidensialitet er viktig i helsevesenet. Opplysninger må være tilgjengelig ved behov, slik at helsepersonellet kan yte forsvarlig helsehjelp,[49] samtidig som opplysningene må beskyttes mot urettmessig tilgang eller misbruk. Tilgjengelighet og konfidensialitet kan oppfattes som motsetninger som ikke kan innfris samtidig. Denne oppfatningen kan stamme fra en idé om at *tilgjengeliggjøring* handler om åpenhet, og at *konfidensialitet* handler om taushet. Dersom man legger den forståelsen til grunn vil tilgjengelighet og konfidensialitet være uforenlige verdier. Verdiene er derimot mer nyanserte enn som så, og nyansene muliggjør etterlevelse av begge deler samtidig.

Enkelt forklart handler konfidensialitet om å beskytte opplysninger mot eksponering for uvedkommende. Tilgjengelighet innebærer å sørge for at autoriserte brukere har tilgang til de opplysningene de behøver, når de trenger det. I helsevesenet er det et stort behov for tilgang til opplysninger slik at beslutningsgrunnlaget i enhver behandling er så godt som nødvendig. Samtidig er opplysningene som behandles så sensitive at de kan gjøre stor skade dersom de havner på avveie eller blir misbrukt.

Vi har utformet «Figur 2: Avveining mellom tilgjengelighet og konfidensialitet» nedenfor for å illustrere hvordan ulike hensyn kan tale for tilgjengelighet og konfidensialitet.

Figuren viser balansen mellom tilgjengelighet og konfidensialitet. I dette tilfellet er vektskålen i vater. Det er selvfølgelig ikke slik at tilgjengelighet og konfidensialitet alltid skal vektes likt, og ulike situasjoner kan tale for at vekten flyttes i

44 Tilsvarer «behandlingsansvarlig» i personvernforordningen. Se personvernforordningen art. 4(7).
45 Pasientjournalloven § 19.
46 Pasientjournalloven § 19 annet ledd.
47 Jf. pasientjournalloven § 17, helsepersonelloven §§ 25 og 45, samt pasient- og brukerrettighetsloven § 5-3.
48 Pasient- og brukerrettighetsloven §§ 4-3 til 4-7.
49 Befring og Ohnstad (2019) s. 43.

Figur 2: Avveining mellom tilgjengelighet og konfidensialitet

den ene eller andre retningen. Det kan oppstå situasjoner hvor liv står på spill, og hvor tilgjengelighet i den aktuelle situasjonen må gå foran kravet til konfidensialitet. På en annen side kan man se for seg situasjoner hvor noen ønsker tilgang til et sett med opplysninger, mens tungtveiende hensyn tilsier at opplysningene ikke skal deles.

Hensyn til et effektivt helsevesen og effektive behandlinger taler for at opplysninger bør være lett tilgjengelig for helsepersonell. Effektivitet innebærer her både tid spart ved innhenting av informasjon og tid spart i vurderingsprosesser som krever at man tar høyde for mange faktorer. Et godt beslutningsgrunnlag kan gjøre vurderinger enklere og mer effektive. Ikke minst vil et godt beslutningsgrunnlag (tilgang til riktige opplysninger) bidra til økt forsvarlighet gjennom at beslutninger fattes på informert grunnlag, og at all rimelig informasjon blir hensyntatt.

Andre tungtveiende hensyn taler for konfidensialitet. Blant annet kan tillit svekkes dersom man oppfatter at helsevesenet ikke har faglig kompetanse, eller dersom man oppfatter at hemmeligheter man deler med helsepersonell blir brukt til annet enn helsehjelp, blir snoket i eller spredd. Dette kan i sin tur føre til at man ikke tør å oppsøke helsehjelp i frykt. Tillit er også avgjørende for at pasienter tør å dele alle potensielt relevante detaljer om helsesituasjonen sin, og at helsehjelpen dermed kan gis med så godt beslutningsgrunnlag som mulig. Pasientens person- og integritetsvern er også viktige hensyn som taler for ivaretakelse av konfidensialitet.

I helsevesenet bør ikke avveiningen mellom konfidensialitet være en «enten, eller»-vurdering, hvor man velger mellom konfidensialitet eller tilgjengelighet. Vurderingen bør tvert imot forsøke å balansere de to hensynene, eller aller helst finne løsninger som styrker begge. Styrking av konfidensialitet behøver ikke innebære en svekking av tilgjengeligheten. I så måte er vektskål-illustrasjonen ovenfor noe misvisende. Det finnes tekniske og organisatoriske rutiner og løsninger som kan bidra til styrking av begge hensyn. Et godt eksempel på et slikt verktøy er den såkalte «blålystilgangen».[50] Begge hensyn er avgjørende for et godt og trygt helsevesen, og det er viktig at systemutviklere og beslutningstakere evner å hensynta begge når nye rutiner og systemer skal settes opp eller endres.

2.2.2 Hva er tilgangskontroll?

2.2.2.1 Formålet med tilgangskontroll

Både fysiske og digitale registre kan inneholde informasjon som ikke skal deles med hvem som helst. Generelt kan man snakke om at en del opplysninger eller samlinger av opplysninger er skjermingsverdige og skal behandles konfidensielt, og at de dermed ikke skal deles med uvedkommende.[51] Dette kan for eksempel innebære at bedriftshemmeligheter ikke skal deles med konkurrerende virksomheter, at personopplysninger skal krypteres eller at en lege ikke skal snakke høylytt om pasienter i korridorene slik at andre kan høre det. I det følgende vil vi forklare hvordan tilgangskontroll i pasientjournalsystemer kan bidra til å styrke konfidensialiteten og tilgjengeligheten.

2.2.2.2 Autentisering som kontrollmetode for tilgang

I informasjonssystemer kan man iverksette en rekke tiltak for å ivareta konfidensialiteten. Tilgangskontroll er ett slikt tiltak. Tilgangskontroll innebærer å kun tildele godkjent personell, brukere eller maskiner tilgang til et system, et domene eller til konkrete sett med opplysninger.[52] Et regelsett må opprettes for å kunne fastsette *hvem* som skal få se eller redigere *hva*. Eksempler på en slik regel kan være at det kun er den økonomiansvarlige i en virksomhet som har tilgang til de ansattes lønnsnivå og egenmeldingsbruk, begrunnet i et tjenstlig behov for slik tilgang i vedkommendes daglige virke. For å kunne sikre at kun rett personell får tilgang i henhold til regelsettet som fastsetter roller og tilgang, må en form for *autentisering* benyttes.[53] Ved fysisk sikring av fysiske arkiver kan det være snakk om et kontrollpunkt, hvor identitet bekreftes, for eksempel ved hjelp av en kortleser på en dør.

---

50 Se kapittel «4.1.3. Brukeradministrasjon».
51 Digitaliseringsdirektoratet (Udatert).
52 Nätt (2019 A).
53 Nätt (2019 B).

I informasjonssystemer vil autentisering typisk bestå i at et brukernavn oppgis (brukeren påstår at han er en konkret person) og at systemet deretter vil be om et bevis for at det faktisk er den aktuelle brukeren som forsøker å få tilgang.

Brukeren vil typisk måtte bevise sin identitet på en av de følgende måtene:[54]

- Ved å fremvise noe bare brukeren *vet*.
- Ved å fremvise eller benytte noe bare brukeren *har*.
- Ved å fremvise eller benytte noe bare brukeren *er*.

Et passord eller et svar på et konkret spørsmål kan benyttes for å bekrefte identiteten, ved å få brukeren til å gi fra seg informasjon som bare den personen skal kunne kjenne til.

En kodebrikke eller et annet verktøy kan benyttes for at brukeren beviser sin identitet gjennom å fremvise eller benytte et verktøy kun vedkommende har tilgang til.

Et fingeravtrykk, en irisskanning eller en DNA-prøve kan benyttes for å kontrollere at brukeren er den han utgir seg for å være, ved å undersøke noe brukeren er alene om å være.

Dersom brukeren kan bevise at han faktisk er den han utgir seg for, og dersom vedkommende skal gis tilgang til den aktuelle informasjonen, skal brukeren gis tilgang til opplysningene eller systemet i henhold til reglene for tilgang.

2.2.2.3 Tilgangskontroll i helsevesenet

Det er flere bestemmelser som direkte eller indirekte omhandler og regulerer tilgangsstyring til pasientjournalsystemer i helsevesenet. Tilgangskontroll reguleres direkte *av Forskrift om pasientjournal* (heretter pasientjournalforskriften) § 13, og hjemles også i de generelle informasjonssikkerhetsbestemmelsene i pasientjournalloven § 22, helseregisterloven § 21 samt personvernforordningen artikkel 32. Alle bestemmelsene fastslår at virksomheten skal innføre tekniske og organisatoriske tiltak som skal sørge for konfidensialitet og tilgjengelighet i systemet. Helsepersonelloven § 16 fastslår i tillegg at virksomheten som yter helse- og omsorgstjenester skal innordnes slik at helsepersonellet er i stand til å overholde sine lovpålagte plikter, herunder taushetsplikten. Dette kan blant annet innebære at pasientjournaler kun er tilgjengelige for autorisert personell med tjenstlig behov, slik at ikke helsepersonellet bryter taushetsplikten sin ved å etterleve journalføringsplikten.[55]

54 Nätt (2019 B).

55 Helsepersonelloven § 39.

Pasientjournalforskriften § 13 sier at tilgang til pasientjournaler skal være basert på bestemte tillatelser til å lese, redigere eller på annen måte behandle opplysningene i pasientjournalen. Å tildele noen en bestemt tillatelse til tilgang kalles autorisasjon, eller å autorisere noen. Ved hjelp av fastsatte kriterier bestemmes det hvem som skal ha tilgang til hva. En bestemt ansatt eller systembruker blir autorisert, og skal deretter få tilgang til de opplysningene eller de delene av systemene han er autorisert for.

Ulike roller og ulike ansatte kan ha behov for ulike tilganger, og autoriseres derfor ulikt. Her er to tenkte eksempler:

Rolle	Tilgang
Akuttsykepleier ved akuttmottak	Full tilgang til alle journaler ved behov
Tannlege	Tilgang til enkelte deler av journal ved behov

Eksemplene er ikke basert på situasjonen slik den faktisk er, men er ment å illustrere hvordan ulike roller i helsevesenet kan ha ulike tilgangsbehov. Taushetsplikten og snokeforbudet[56] forbyr tilgang utover hva som er tjenstlig nødvendig, og autorisasjonen skal reflektere dette. Akuttsykepleieren kan ha behov for å kunne tilegne seg umiddelbar tilgang til enhver pasientjournal, fordi det på forhånd er vanskelig å forespeile hvem som kan trenge hjelp av vedkommende. Det kan med andre ord være vanskelig å lage en autorisasjon som gir tilgang til konkrete journaler eller kategorier av journaler. For tannlegens del kan autorisasjonen for eksempel gi vedkommende tilgang til bare enkelte deler av en pasientjournal, og kun til pasientjournaler for pasienter som på forhånd er registrert som pasienter hos den aktuelle tannlegen. Tannlegens tilgangsbehov er ofte lettere å forutse, og det er i de fleste tilfellene ikke snakk om akuttsituasjoner hvor brede tilganger må ligge for hånden.

Autorisasjonen skal ta høyde for både kravene til konfidensialitet (taushetsplikt, snokeforbud) og tilgjengelighet.[57] Helsepersonellet skal ha tilgang til opplysninger slik at de kan yte forsvarlig helsehjelp,[58] samtidig som tillit[59] og konfidensialitet[60] bevares. Se kapittel 2.2.1.3. om avveining mellom konfidensialitet og tilgjengelighet.

56 Helsepersonelloven §§ 21 og 21 a, helseregisterloven §§ 17 og 18, pasientjournalloven §§ 15 og 16.
57 Se kapittel «2.2.1.2. Tilgjengelighet».
58 Helsepersonelloven § 4.
59 Helsepersonelloven § 1.
60 Helsepersonelloven §§ 21 og 21 a, helseregisterloven §§ 17 og 18, pasientjournalloven §§ 15 og 16.

3 Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren

3.1 Om Normen

I helse- og omsorgssektoren behandles det store mengder pasientopplysninger og andre personopplysninger. Opplysninger om straffbare forhold hos en pasient er også et eksempel på opplysninger som helsepersonell og journalsystemer må håndtere.[61] I Oslo var det rett i underkant av 168.000 konsultasjoner ved legevaktene i 2018.[62] Opplysningene som samles inn gjennom slike konsultasjoner benyttes i hovedsak til å sikre forsvarlige[63] helsetjenester til pasienter. Helseopplysninger skal regnes som «særlige kategorier av personopplysninger»,[64] og er underlagt taushetsplikt.[65] En slik taushetsplikt er avgjørende for at pasienter og brukere[66] skal ha tillit til helsevesenet. Slik tillit er viktig for den enkelte og for folkehelsen. Ved at pasienter og brukere tør å oppsøke hjelp uten frykt for at opplysninger de gir blir brukt til annet enn helsehjelp, bidrar taushetsplikten (og øvrig beskyttelse av personopplysninger) til at flere tør å søke helsehjelp, og på den måten unngår man for eksempel at smitte sprer seg i befolkningen, eller at sårbare grupper unnlater å søke hjelp.[67] Formålsparagrafen i pasientjournalloven fastslår at tillit til helse- og omsorgssektoren og til helsepersonell er et grunnleggende mål.[68]

I de senere år har mediebildet vært preget av et stadig økende fokus på personvern. Private og offentlige virksomheter har både gjennom sitt arbeid og sin mediestrategi satt søkelyset på viktigheten av personvern for sine brukere. I 2018 ble ny personopplysningslov innført i Norge, på bakgrunn av innføringen av EUs personvernforordning.[69] Et enkelt nettsøk på forkortelsen «GDPR» (General Data Protection Regulation) viser hvor brennaktuelt personvern har vært rett i forkant av og etter innføringen av personvernforordningen. Det samme gjelder også for generell informasjonssikkerhet. Noen få, store informa-

61 Duvaland (2016) s. 135.
62 Kombinasjon av statistikk fra Statistisk sentralbyrå (2020 A) og Statistisk sentralbyrå (2020 B).
63 Jf. helsepersonelloven § 4 om forsvarlighetskravet.
64 Jf. personvernforordningen artikkel 9(1).
65 Jf. helsepersonelloven § 21 og pasientjournalloven § 15.
66 Pasient- og brukerrettighetsloven § 1-3 bokstav A og F.
67 Duvaland (2016) s. 136.
68 Helsepersonelloven § 1.
69 Personvernforordningen.

sjonssikkerhetshendelser har preget mediebildet de senere årene.[70] Blant disse har saken om at utenlandske IT-arbeidere hadde potensiell tilgang til pasientdata til så mange som 2,8 millioner nordmenn fått mye medieomtale, og ytterligere aktualisert informasjonssikkerhet i helsesektoren.[71]

Normen er et sett med regler, veiledere og styringsdokumenter[72] for hvordan helse- og omsorgssektoren skal arbeide med informasjonssikkerhet og personvern, primært *personopplysningsvern*. Den ble lansert i 2006 på initiativ fra Helsedirektoratet, og har blitt oppdatert og skrevet om med jevne mellomrom siden den gang.[73] Normen har hatt sekretariat hos Direktoratet for e-helse siden 2016. Revisjoner har blitt gjort av en rekke representanter for ulike aktører i helsesektoren, deriblant Folkehelseinstituttet, regionale helseforetak (RHF), Helsedirektoratet, Den norske legeforening, Norsk sykepleierforbund mv.[74]

Den nåværende versjonen av Normen, 6.0, ble vedtatt 4. februar 2020, og er tilgjengelig på Direktoratet for e-helse sine nettsider.[75] Den gjelder for virksomhetene som har forpliktet seg til den, og ikke andre. Versjon 6.0 har ikke status som såkalt *atferdsnorm* etter personvernforordningen artikkel 40.[76] Alle som er tilkoblet Norsk helsenett forplikter seg til å følge Normen.[77] Dette gjelder for Helseetaten og Profdoc Vision.[78]

Normens overordnede formål er å bidra til at virksomheter kan etterleve krav til informasjonssikkerhet og personvern. Den legger også opp til samhandling mellom helsevirksomheter, ved å skape tillit mellom virksomheter som har forpliktet seg til å etterleve den. Dersom du forplikter deg til etterlevelse av Normen, og dersom du faktisk etterlever den, bør det være sikkert å samhandle med virksomheten din.[79]

70 NRK (2018).
71 NRK (2017).
72 Overordnede regler som setter rammene for og staker ut retningen i et gitt prosjekt. Digitaliseringsdirektoratet (2019).
73 Direktoratet for e-helse. (2020 A).
74 Direktoratet for e-helse (2020 A).
75 Direktoratet for e-helse (2020 B).
76 Direktoratet for e-helse (2020 B) punkt 1.2.
77 Norsk helsenett (Udatert B).
78 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
79 Direktoratet for e-helse (2020 B) punkt 1.2.

3.2 Overordnet om Normens innhold

Innledningsvis blir Normen presentert, og en rekke begreper blir definert. Informasjonssikkerhet blir fastsatt som det å håndtere risikoer knyttet til behandlingen av personopplysninger og annen informasjon. Videre presiseres det at nøkkelbegreper her er *konfidensialitet, integritet og tilgjengelighet*. En vanlig forkortelse for disse samlebegrepene er KIT.[80] Integritet innebærer at helse- og personopplysninger skal beskyttes mot uønsket endring eller sletting. Tilgjengelighet fastsettes her som et ønske om at helse- og personopplysninger skal være tilgjengelig for helsepersonellet til rett tid og på rett sted når behovet for opplysningene melder seg. Konfidensialitet har vi forklart i kapittel «2.2.1. Konfidensialitet og tilgjengelighet». I Normen fastsettes konfidensialitet som et ønske om å sikre seg mot at uvedkommende får kjennskap til opplysningene. Helsevesenets ønske og krav[81] om opprettholdelse av tilliten fra befolkningen tydeliggjør behovet for ivaretakelse av konfidensialitet. I tillegg til KIT-begrepene nevnes begrepet *robusthet*. Dette begrepet er hentet fra personvernforordningen, og definisjonen er dermed også den samme. I Normen siktes det til en organisasjons eller et informasjonssystems evne til å gjenoppta normal drift og virksomhet etter en hendelse.

Normens krav skal tilpasses virksomhetens kompleksitet, størrelse, samt mengde med helseopplysninger som behandles.[82] [83] Den er ikke en fullstendig redegjørelse eller uttømmende gjengivelse av all relevant lovgivning på områdene personvern og informasjonssikkerhet, og fokuserer hovedsakelig på informasjonssikkerhet i tjenester og virksomheter som yter helse- og omsorgstjenester.[84] I grove trekk er Normen inndelt i «skal»- og «bør»-krav. Skal-krav skal følges av alle. Bør-krav legger opp til større grad av skjønn, og vurderinger og skjønnsutøvelsen flyttes over på den enkelte virksomhet. Virksomheten skal selv velge og tilpasse tiltak som passer til sin behandling av helseopplysninger.[85]

3.3 Tilgangskontroll i Normen

3.3.1 Generelt

Prosjektet vi har satt i gang har til hensikt å gjennomgå KADs (og nærmere bestemt pasientjournalsystemet de benytter, Profdoc Vision) etterlevelse av krav

80 Nätt (2019 A).
81 Helsepersonelloven § 1.
82 Personvernforordningen art. 4(1).
83 Direktoratet for e-helse (2020 B) punkt 1.5.
84 Direktoratet for e-helse (2020 B) punkt 1.5.
85 Direktoratet for e-helse (2020 B) punkt 1.5.

til tilgangskontroll og konfidensialitet. I Normen fremkommer det en rekke krav til hvordan tilgangskontroll og konfidensialitet skal ivaretas hos virksomheter. I det følgende gir vi en oversikt over de delene av Normen som direkte eller indirekte er ment å ivareta tilgangskontroll. Vi vil samtidig vise til lovhjemmel for de enkelte tiltakene, og diskutere konsekvensene av tiltakene.

3.3.2 Risikoappetitt

Overordnet fastslår Normen at virksomheten for egen del skal fastsette egen akseptabel risiko (risikoappetitt).[86] Innen informasjonssikkerhetsfeltet brukes risikoappetittbegrepet som en fastsatt grense for hvor mye risiko eller potensielle negative konsekvenser en virksomhet er villig til å akseptere for å nå et mål. Det er forbundet en viss risiko ved enhver virksomhet eller oppgave. For eksempel er det alltid en *viss* risiko for at et strømbrudd som stanser oppvarmingen av en leilighet i en viss periode vil inntreffe. For de fleste vil en slik risiko være akseptabel, både fordi sannsynligheten for at den inntreffer er lav, og fordi de antatte konsekvensene av et kortvarig strømbrudd er lave, særlig i sommerhalvåret. Dersom du driver et sykehus vil derimot risikoappetitten for strømbrudd være betydelig lavere, først og fremst fordi konsekvensene av et slikt strømbrudd kan bli svært høye. Livsnødvendig utstyr kan slutte å fungere, oppvarmingen og belysningen i bygget vil slutte å fungere, og i ytterste konsekvens kan liv gå tapt. Dersom slike risikoer ikke kan aksepteres, må virksomheten enten avvikle drift, eller de må innføre tiltak som lemper på sannsynligheten for eller konsekvensene av hendelsen. Et sykehus kan for eksempel installere en dieselgenerator for å sikre strømtilførsel, og på den måten minsker konsekvensen av et strømbrudd. Konsekvensen kan derfor kanskje aksepteres. Informasjonssikkerhet handler hele tiden om å vurdere konsekvenser og sannsynlighet, og å innføre tiltak som utbedrer situasjonen og bidrar til at risikoen blir akseptabel. Selv om virksomheten kommer til at risikoene de møter er akseptable, må Normens minimumskrav for informasjonssikkerhet fortsatt etterleves.[87] Selv om ordet *risikoappetitt* eller begrepet *akseptabel risiko* ikke direkte brukes i personvernforordningen, er formålet dekket av forordningens artikkel 32(1). I artikkelen legges det opp til at det skal gjennomføres en vurdering av hvor sannsynlig og hvor alvorlig en hendelse vil kunne være, og deretter treffe tiltak som er egnet til å oppnå et sikkerhetsnivå som «er egnet med hensyn til risikoen».

De generelle minimumskravene til informasjonssikkerheten er listet opp i Normens punkt 3.2. I avhandlingen skal vi kartlegge bruken av tilgangskontroll i KADs pasientjournalsystemer, samt vurdere hvorvidt den i tilstrekkelig grad og på rett måte bidrar til helseopplysningenes konfidensialitet. I det følgende skal

86 Aven (2019).

87 Direktoratet for e-helse (2020 B) punkt 3.2.

vi se nærmere på hvilke av minimumskravene som kan sies å angå konfidensialiteten, og nærmere bestemt tilgangskontrollen i pasientjournalsystemer.

3.3.3 Tilgangskontroll

I punkt 3.2 av Normen deles de overordnede kravene til informasjonssikkerheten inn i de velkjente KIT (konfidensialitet, integritet og tilgjengelighet). I tillegg er *robusthet* tatt med, hentet fra personvernforordningen art. 32(1) bokstav b. Robusthet handler om en virksomhets evne til å motstå hendelser, for eksempel målrettede angrep eller andre uønskede sikkerhetshendelser som kan ramme personopplysningssikkerheten. Robusthet dreier seg også om en virksomhets evne til å gjenopprette normaldrift etter en slik hendelse.

3.3.4 Hindre uautorisert tilgang

For å sikre konfidensialiteten skal virksomheten sørge for at taushetsplikten[88] blir ivaretatt, og sørge for at uvedkommende ikke får tilgang til helse- og personopplysninger. Det samme gjelder for annen informasjon som kan ha betydning for informasjonssikkerheten. Det klargjøres ikke hva man legger i det sistnevnte noe sted i Normen, og vi har ikke klart å tyde dette ut fra relevant helselovgivning. Vi legger derfor til grunn en antakelse om at slik informasjon *kan* innebære informasjon om tekniske og organisatoriske sikringstiltak, og som på avveie kan åpenbare svakheter i informasjonssikkerheten som kan tenkes å bli utnyttet av andre.

For å kunne hindre slik tilgang er det først og fremst nødvendig å klargjøre hvem Normen omtaler som *uvedkommende* og *uautoriserte,* altså hvem som ikke skal få tilgang. I denne sammenhengen er det hensiktsmessig å først finne ut av hvem som skal ha tilgang. Pasientjournalloven gir svar på det, i § 6, «Rett til å behandle helseopplysninger». I paragrafens annet ledd står følgende:

> *«Helseopplysninger i behandlingsrettede helseregistre kan bare behandles når det er nødvendig for å kunne gi helsehjelp, eller for administrasjon, internkontroll eller kvalitetssikring av helsehjelpen.»*[89]

Slik bestemmelsen sier, kan helseopplysninger i behandlingsrettede helseregistre[90] bare behandles når formålet er å gi helsehjelp. Støttefunksjoner slik som administrasjon er også hjemlet, og det samme gjelder for behandling begrunnet

88 Helsepersonelloven §§ 21 og 21 a, pasientjournalloven § 15.

89 Pasientjournalloven § 6 annet ledd.

90 Behandlingsrettet helseregister: Pasientjournal- og informasjonssystem eller annet register, fortegnelse eller lignende, der helseopplysninger er lagret systematisk, slik at opplysninger om den enkelte kan finnes igjen, og som skal gi grunnlag for helsehjelp eller administrasjon av helsehjelp til enkeltpersoner. Hentet fra pasientjournalloven § 2 bokstav d.

i kontroll av eller kvalitetssikring av helsehjelpen. Begrepet «behandling» i sammenhengen behandling av helseopplysninger tilsvarer begrepet behandling av personopplysninger slik dette er fastsatt i personvernforordningen artikkel 4 nr. 2.[91] *Helsehjelp* er definert i pasientjournalloven § 2 bokstav a, og er enhver handling som har forebyggende, diagnostisk eller behandlende formål, og som utføres av helsepersonell.[92] Det blir med dette klart at det kun er helsepersonell og enkelte andre roller som skal ha tilgang til pasient- og personopplysninger i slike registre. Det samme gjelder for opplysninger som kan påvirke informasjonssikkerheten.

For å hindre uautorisert tilgang vil tilgangskontroll (rolledefinert tilgangskontroll) være av betydning, i den grad utenforstående tilegner seg tilgang til systemet som en rolle, for eksempel ved at de får tilgang til en eksisterende brukerkonto. Mer generelt vil sikring av systemet mot angrep og tilgang fra utenforstående være nødvendig, og blant annet vil gode passordrutiner være hensiktsmessig her. Tilgangskontrollen har ikke som primær hensikt å hindre utenforstående fra å få tilgang til pasientjournalsystemet,[93] men snarere å sikre at brukerkontoer som skal ha tilgang til systemet kun får tilgang til de opplysningene og underdomenene de har tjenstlig behov for. Dette kan materialisere seg slik at helsepersonell kun får tilgang til opplysningene om en pasient i et behandlingsløp de er involvert i, og hvor de yter helsehjelp eller støttefunksjoner.[94]

3.3.5 Avgrense tilgang for autorisert personell

Normen stiller en rekke krav til tilgangsstyring for autorisert personell. Det samme gjør lovverket. Kun de med tjenstlig behov for tilgang skal gis tilgang.[95] I dette kapittelet skal vi se nærmere på når, hvordan og hvorfor tilganger skal gis eller trekkes tilbake fra personell som har tjenstlig behov for tilgangen, eller fra personell som tidligere har hatt slik tilgang. Hvordan skal man sørge for at kun et utvalg ansatte på en avdeling får tilgang til en pasientjournal, eller at kun spesifikke roller ved KAD får se en pasients epikrise? Tiltakene som trekkes frem i dette kapittelet vil med andre ord ikke omhandle generell informasjonssikkerhet, og heller ikke tiltak for å hindre at utenforstående får tilgang.

Av praktiske tiltak som nevnes i Normen er blant annet fjerning av tilgang til helse- og personopplysninger så snart et ansettelsesforhold opphører. Vedkommende har ikke lenger tjenstlig behov for tilgangen, og rutiner skal være på plass

91 Personvernforordningen art. 4 nr. 2.
92 Helsepersonell: Se helsepersonelloven § 3 første ledd.
93 Se kapittel «2.2.2. Hva er tilgangskontroll?».
94 Jf. pasientjournalloven § 19 første ledd.
95 Direktoratet for e-helse (2020 B) punkt 3.2.

for å fange opp dette, samt sørge for at tilgangen fjernes. Lagringsmedier (papir, minnepenner, annet digitalt osv.) som kan inneholde helse- og personopplysninger, skal leveres inn. Det samme gjelder for adgangskort som den ansatte har fått utdelt. Tilgang til pasientjournalsystemer eller domener på slike systemer skal trekkes tilbake så snart ansettelsesforholdet opphører. Disse tre tiltakene har hjemmel i pasientjournalloven § 22 og personvernforordningen artikkel 32, i tillegg til den generelle taushetspliktsbestemmelsen i helsepersonelloven § 21. Selv om det ikke står nevnt i Normen, mener vi at pasientjournalforskriften § 13 bokstav d og e tydeliggjør kravet om å tids- og rollebegrense tilgangen til helseopplysninger, og særlig knyttet til tilganger i pasientjournalsystemer. Normen oppstiller også krav til at rutiner for autorisering, endring og avslutning av tilganger skal opprettes. Det innebærer at virksomheten (dataansvarlig) skal tildele, trekke tilbake og endre tilganger i henhold til et etablert system, og ikke etter eget skjønn.

En viktig betraktning når tilgangsstyring etableres i pasientjournalsystemer er forholdet til taushetsplikten og konfidensialiteten. Dette må også ses i lys av helsepersonellets behov for rask og sikker tilgang til helseopplysninger for å kunne yte forsvarlig helsehjelp.[96] [97] Det samme gjelder behovet for å kunne dele helseopplysninger mellom samarbeidende helsepersonell i en behandlingssituasjon.[98] Avveiningen mellom konfidensialitet og tilgjengelighet omtaler vi også i kapittel «2.2.1.3. Avveining mellom konfidensialitet og tilgjengelighet». Systemene skal støtte deling og tilgjengeliggjøring av informasjon til de som har tjenstlig behov, og informasjonen skal være tilgjengelig når behovet melder seg.

Normen stiller krav om at det skal fattes en konkret beslutning om å gi helsepersonell tilgang til helseopplysninger i tilfeller hvor det ytes helsehjelp, eller hvor slik hjelp skal ytes. Dette innebærer at generelle blankofullmakter for tilgang ikke godtas. Det må foreligge konkrete vurderinger knyttet til at vedkommende helsepersonell og behandlingen som skal utføres. Det betyr at helsepersonellet gis tilgang til pasientjournalen til pasienten når behandlingen starter, og at helsepersonellet ikke har generell tilgang til alle journaler uten at det foreligger et konkret tjenstlig behov.

Autorisasjon skal gis til personell som har tjenstlig behov for tilgang. Autorisasjonen skal:

96 Forsvarlighetskravet: Helsepersonelloven § 4.
97 Pasientjournalloven § 19.
98 Helsepersonelloven § 25.

- Sørge for at personellet har tilgang til de opplysningene de behøver for å yte helsehjelp.[99]
- Vurderes på nytt ved endringer i ansettelsesforhold eller ansvarsområder.[100]
- Være tidsbegrenset.
- Angi hvilke virksomheter autorisasjonen omfatter.
- Beskrive rettighetene og pliktene som autorisasjonen omfatter.

Autorisasjonen skal også dokumenteres, slik at virksomheten har en oppdatert oversikt over tildelte autorisasjoner. Oversikten skal vise hvem som har tilgang til hva. Det skal i ettertid kunne kontrolleres hvem som faktisk har tilegnet seg tilgang til hva.[101] Det er derfor nødvendig med loggføring av tilgangene.[102]

Virksomheten (dataansvarlig, jf. pasientjournalloven § 2 bokstav e) skal understøtte helsepersonellets lovpålagte plikter, herunder taushetsplikten, gjennom sine systemløsninger, og systemperspektivet er følgelig tatt inn i helsepersonelloven § 16. Du finner også dette systemperspektivet i pasientjournalloven § 7 første ledd bokstav a.

Tilgangskontroll i pasientjournalsystemer er et av flere verktøy dataansvarlig har tilgang til for å understøtte kravene om konfidensialitet og tilgjengelighet. Tilgang basert på tjenstlig behov understøtter både den passive og den aktive taushetsplikten, slik de er hjemlet i helsepersonelloven § 21. Helsepersonell plikter å ikke dele taushetsbelagte opplysninger med andre enn de som har rett på slik tilgang. I et pasientjournalsystem uten tilstrekkelig tilgangsstyring er det sannsynlig at du ved å fylle inn taushetsbelagte opplysninger bidrar til at andre får se disse. Tilgangskontroll vil kunne motvirke en slik utilsiktet spredning av opplysninger. Tilgangskontrollen understøtter også forbudet mot å tilegne seg taushetsbelagte opplysninger uten tjenstlig behov, jf. helsepersonelloven § 21 a. Dette forbudet forbyr ikke bare videreformidling av opplysninger, men også det å selv oppsøke eller tilegne seg slik informasjon. Snoking eller annen form for urettmessig tilegnelse blir vanskeligere når den reelle tilgangen til opplysningene begrenses eller fjernes. Taushetspliktsbestemmelsene finnes også i pasientjournalloven § 15 og 16. Se kapittel «2.2.1.1. Konfidensialitet og taushetsplikt» for detaljer om taushetsplikt for helsepersonell, og hvordan dette kan påvirke pasientjournalsystemer.

99 Pasientjournalloven § 19.
100 Pasientjournalforskriften § 13 første ledd bokstav e.
101 Pasientjournalforskriften § 13 tredje ledd.
102 Pasientjournalforskriften § 14.

4 Kommunerevisjonens funn vurdert etter Normens krav

4.1 Kommunerevisjonens kontroll av Profdoc Vision

Kommunerevisjonen er Oslo kommunes interne revisor, og er organisert som en egen etat.[103] I 2016 gjennomført de en revisjon av Barne- og familieetatens fagsystem BiRK, og Helseetatens pasientjournalsystem Profdoc Vision. Rapporten ble offentliggjort i 2017. Nedenfor redegjør vi for funn som har betydning for vår vurdering av konfidensialitet og tilgjengelighet i Profdoc Vision.

Pasientjournalsystemet hadde i 2016 rundt 1300 aktive brukere. Pasientjournalsystemets tekniske begrensninger førte til at Helseetaten ikke klarte å fremskaffe en oversikt over hvor mange pasientjournaler som totalt var registrert i pasientjournalsystemet. Pasientene som var registrert i systemet var ikke sortert etter hvilken avdeling de mottok behandling ved. [104]

Informasjonssikkerhet var et vanskelig område, ifølge Helseetaten. De forteller til kommunerevisjonen at balansegangen mellom kravene til IKT-systemenes tilgjengelighet og konfidensialitet var en av hovedutfordringene de stod overfor. Helseetatens etatsdirektør var systemeier for Profdoc Vision, mens det var avdelingsdirektørene for Allmennlegevakten og Aker som var operative systemeiere. Videre var det ikke beskrevet hvilke oppgaver som var underlagt de ulike rollene. Systemforvalter i Profdoc Vision var fagansvarlig i fagsystemavdeling. Oppgavene som tilhørte rollen var ikke fullt ut beskrevet og var heller ikke samlet på ett sted. Helseetaten kunne ikke vise til en overordnet risikovurdering ved tilsynet fra kommunerevisjonen. Etaten hadde heller ikke gjennomført en risikovurdering av pasientjournalsystemet Profdoc Vision.

En av hovedutfordringene med informasjonssikkerheten var ifølge Helseetaten at Profdoc Visions grunnarkitektur er fra 1995. I tillegg opplyser de at pasientjournalsystemet ikke er Windows-basert.[105] Byrådsavdelingen for eldre, helse og sosiale tjenester hadde definert Profdoc Vision som et utdatert system, og mente

103 Oslo kommune (Udatert B).

104 Kommunerevisjonen (2017).

105 Et Windows-basert program er et program som er designet for å kjøre på maskiner som benytter seg av Microsoft Windows-operativsystemet. Programmer som ikke er Windows-baserte må spesialtilpasses for å kunne kjøre på maskinene.

at systemet var modent for utskiftning. Profdoc Vision ble heller ikke videreutviklet fra systemleverandørens side, og Helseetaten var klar over dette.

Rutinene for tildeling, administrering og oppfølging av tilganger i Profdoc Vision var skriftlige. Dette skulle også gjelde for KAD, men rutinene var ikke kjent der. KAD kunne heller ikke vise til andre eller tilsvarende rutiner for håndtering av tilganger.

4.1.1 Passord

Helseetaten hadde utarbeidet en systemhåndbok for Profdoc Vision, men denne hadde flere mangler og var utdatert på flere områder. I systemhåndboken fremkom Helseetatens passordrutiner. For å få tilgang til Profdoc Vision måtte innlogging skje via kommunens driftsplattform AKS. Her kunne autoriserte brukere av Profdoc Vision få tilgang til pasientjournalsystemet. Ifølge Helseetatens passordrutiner måtte passordet være minst åtte tegn langt, og bestå av en kombinasjon av små og store bokstaver, i tillegg til tall eller spesialtegn. Tvunget passordskifte var skrudd av for brukere av Profdoc Vision. Terminalene[106] ved KAD ble automatisk sikret med skjermlås etter 15 minutters inaktivitet, men det forelå ikke skriftlige rutiner for dette.

Innlogging ved bruk av tofaktorautentisering og ID-kort med passord i tillegg til å være innlogget på kommunens driftsplattform, var også tidligere en mulighet. Problemer med ID-kortene hadde ifølge Helseetaten ført til at dette i liten grad ble benyttet.

Dersom brukeren var pålogget kommunens driftsplattform AKS kunne brukerne logge seg videre inn i Profdoc Vision med et eget brukernavn og passord. Denne innloggingen hadde ikke skriftlige nedfelte rutiner og ble ifølge Helseetaten benyttet i liten grad. Det var ingen krav til passordkompleksitet utover at passordet måtte bestå av seks tegn. Passordskifte måtte skje etter 90 dager. Gjenbruk av samme passord kunne skje etter en måned.

4.1.2 Misbruk av identitet

I sin rapport skriver kommunerevisjonen at de fikk opplyst at det var en risiko for at medarbeiderne benyttet systemet innlogget som andre brukere. Dette skjedde for eksempel ved at medarbeidere lot skjermen stå åpen og lot kolleger registrere opplysninger i systemet uten at de logget på med sin egen bruker. De ansatte begrunnet praksisen med at pålogging i systemet var for tidkrevende. Mange unnlot derfor å logge ut ved kortere fravær fra terminalen.

106 Datamaskiner som de ansatte benytter ved KAD for blant annet å få tilgang til pasientjournaler.

4.1.3 Brukeradministrasjon

Det var vaktkoordinatorene på KAD som var ansvarlige for å opprette tilganger i Profdoc Vision. Medarbeidere som ønsket tilgang, måtte først være registrert i kommunens person- og ressurskatalog (PRK) for at vaktkoordinatoren kunne gi tilgang. Opprettelse av tilgang krevde en opprettelse av et autorisasjonsskjema som ble fylt ut av brukerens nærmeste leder. Skjemaet var av eldre dato. Helseetaten hadde utviklet nyere autorisasjonsskjemaer, men de var ikke tatt i bruk på avdeling Aker da kommunerevisjonen utførte sin kontroll. Autorisasjonsskjemaet gjaldt både for nye brukere og dersom eksisterende brukere skulle ha endret tilgang. Skjemaet inneholdt informasjon om hvilken yrkesgruppe eller tittel vedkommende hadde, men ikke informasjon om hvilken brukergruppe medarbeideren skulle ha tilgang til. Det var fem faste yrkesgrupper i Profdoc Vision:

- Lege ansatt
- Privatpraktiserende lege
- Sosionom
- Sykepleier
- Sykepleier SO

Vaktkoordinatorene var ansvarlig for å kontrollere at skjemaet var utfylt og at brukeren var registrert i kommunens person- og kontaktregister. Etter at vaktkoordinatoren hadde gitt autorisasjon ble det sendt en melding til den ansattes nærmeste leder. Autorisasjonsskjemaene ble arkivert hos vaktkoordinatorene.

Med unntak fra det sentrale overgrepsmottaket hadde alle brukergruppene tilgang til all informasjon om pasienter på tvers av alle avdelingene i Helseetaten. Likevel fantes det sperrer på enkelte pasienter. Dette gjaldt for eksempel kjente personer, ansatte og andre personer med et behov for å bli sperret. Avdelingsdirektøren ved Allmennlegevakten var ansvarlig for å gi brukere tilgang til opplysningene i sperret avdeling. I utgangspunktet kunne alle med tilgang til brukeradministrasjonen dele ut tilganger også til sperret avdeling. Dersom dette ble gjort, ble det klassifisert som ureglementert tilgangsdeling.

Tidligere ble det gitt individuelle og utvidede tilganger til ansatte innen hver av brukergruppene ved behov. Dette gjaldt i hovedsak skrive- og endringsrettigheter. Blant annet ble tilganger til brukeradministrasjon eller rapporter gitt ut på individuell basis. Totalt hadde 32 brukere tilgang til brukeradministrasjon. Systemforvalter oppga til kommunerevisjonen at det forelå mange individuelle tilganger innen hver av brukergruppene, og dette gjorde det vanskelig å fremskaffe en fullstendig oversikt over hvilke tilganger som var blitt gitt i Profdoc

Vision. Systemforvalter oppga videre at dette var noe de jobbet med å få orden på, ved å opprette nye og mer tilpassede brukergrupper. Det hadde blitt opprettet 15 nye brukergrupper utover de fem opprinnelige brukergruppene. Systemforvalter holdt også på med å plassere medarbeidere med individuelle tilganger inn under de nye brukergruppene. Dette arbeidet ble ifølge etaten fullført i desember 2016.

Helseetatens nye autorisasjonsskjema for tildelinger av tilganger i Profdoc Vision ble utarbeidet i november 2016. Skjemaet kunne fylles ut elektronisk, der skulle det opplyses om hvilken brukergruppe vedkommende skulle ha tilgang til. Skjemaet var ikke tatt i bruk ved KAD på kommunerevisjonens undersøkelsestidspunkt.

Helseetaten la ved kommunerevisjonens kontroll frem fem kontrolltiltak tilknyttet brukeradministrasjon. Det første var en månedlig kontroll som besto i å kontrollere at tildeling av tilganger stemte overens med innsendte autorisasjonsskjemaer. Denne kontrollen ble ifølge systemforvalter ikke gjennomført før desember 2016. I tillegg skulle brukere kontrolleres halvårlig dersom de var definerte som systemadministratorer og dermed hadde utvidede tilganger. Det ble her kontrollert at de som hadde utvidede tilganger hadde korrekte tilganger. Den halvårlige kontrollen fungerte ikke før i desember 2016 ettersom systemet ikke kunne generere en slik oversikt. Etter at de hadde fått kategorisert medarbeidere med individuelle tilganger inn under de nye brukergruppene startet Helseetaten med den halvårlige kontrollen.

Helseetaten oppga også at de kjørte et månedlig skript[107] i systemet for å identifisere brukere som hadde vært inaktive i 365 dager. Rutinene tilsa at skriptet skulle slette brukere som ikke hadde vært aktive på seks måneder.

Profdoc Vision inneholdt også en såkalt blålysfunksjonalitet. Funksjonen kunne benyttes slik at personell kunne få tilgang til journaler og mapper de normalt sett ikke hadde tilgang til. Funksjonaliteten ga også personell tilgang til opplysninger om pasienter i sperret avdeling. Blålysfunksjonaliteten ble gitt ved at en ansatt trykket på en knapp for blålysfunksjonalitet i Profdoc Vision. Deretter måtte den ansatte oppgi en begrunnelse, og det ble sendt et varsel til avdelingsdirektøren på Allmennlegevakten. Det var ingen rutiner beskrevet for hvordan avdelingsdirektøren skulle følge opp bruk av blålysfunksjonaliteten. Bruk av funksjonaliteten ville fremkomme i systemets sikkerhetslogg. Der ble det også registrert hvilke brukere som logget seg inn og ut av pasientjournaler og hvilke pasientjournaler dette gjaldt. Det fantes ingen rutiner for kontroll av sikkerhetsloggen utover kon-

107 Rossen (2019).

troll av blålysfunksjonaliteten. Systemforvalter oppga til kommunerevisjonen at det ble gjennomført en månedlig sjekk i sikkerhetskontrollen for bruk av blålysfunksjonen. Kontrollen ble dokumentert i skjemaet *Kontroll av tilganger i Profdoc Vision*. Systemforvalter oppga også at funksjonen sjelden ble benyttet.

4.1.4 Roller i Profdoc Vision

Ved revisjonstidspunktet til kommunerevisjonen var det omtrent 1320 brukere i Profdoc Vision i Helseetaten. Av disse fikk kommunerevisjonen tilgang til en oversikt som viste at 1270 aktive brukere hadde tilgang til pasientjournaler og helseopplysninger ved KAD. Den totale oversikten var vanskelig å få da det forelå mange individuelle tilganger i de ulike brukergruppene. I tillegg hadde brukergruppene tilgang på tvers av avdelinger, med unntak av det sentrale overgrepsmottaket og sperret avdeling. Legene arbeidet på tvers av legevaktene (KAD og legevakten i Storgata), og ifølge Helseetaten var det utfra et tjenstlig behov nødvendig med tilgang på tvers av avdelingene. I tillegg til dette var det stor pasientflyt mellom legevaktene.

4.1.4.1 Elektronisk meldingsboks

KAD samarbeider med spesialisthelsetjenesten og den kommunale pleie- og omsorgstjenesten. Det ble benyttet elektroniske meldinger i kommunikasjonen dem imellom. Meldingene inneholdt for eksempel informasjon om hvorfor pasienten var innlagt, pasientens funksjonsnivå og eventuelle hjelpebehov. Helsepersonell som hadde tilgang til Profdoc Vision hadde tilgang til meldingene uavhengig av brukergruppe. Det ble heller ikke logget oppslag i meldingene.

4.1.4.2 Leverandør og drift

CGM hadde leverandørtilgang til systemets utviklingsmiljø. I utviklingsmiljøet forelå det også personsensitive data. Helseetaten hadde innhentet taushetserklæring for de tre ansatte i selskapet som ifølge Helseetaten hadde tilgang til utviklingsmiljøet. Det var ikke inngått noen databehandleravtale mellom Helseetaten og systemleverandør, og Helseetaten hadde heller ikke beskrevet hvem som var autorisert til å godkjenne eksterne tilganger.

EVRY var ansvarlig for drift av Profdoc Vision og hadde tilgang til databasen.[108] Helseetaten visste ikke hvor mange og hvem fra EVRY som hadde databasetilgang. Det var ifølge Helseetaten opprettet en egen gruppe for teknikere fra EVRY som hadde sykepleiertilgang.[109] Helseetaten oppga at årsaken til at de ble gitt denne tilgangen var at ansatte i EVRY måtte ha mulighet til å feilsøke ved kritiske feil. Mellom Utviklings- og kompetanseetaten og EVRY forelå det en

108 Bratbergsengen (2019).

109 Se oversikt over roller i kapittel 4.1.3 om Brukeradministrasjon.

databehandleravtale. Utviklings- og kompetanseetaten er Helseetatens interne IKT-leverandør. Utover CGM og EVRY var det ifølge Helseetaten ikke flere eksterne brukere av Profdoc Vision.

4.1.4.3 Systemadministratorer

Helseetaten kunne ikke fremskaffe oversikt over systemadministratorer ved oppstarten av revisjonsarbeidet. Da kommunerevisjonens undersøkelser nærmet seg ferdig, utarbeidet Helseetaten en ny oversikt over systemadministratorrettigheter i Profdoc Vision. I den nye oversikten var det definert to brukergrupper med systemadministratorrettigheter. «Systemadministrator – forvalter» og «systemadministrator – lege». Tre brukere var plassert i brukergruppen «systemadministrator – forvalter», og ni brukere var plassert i brukergruppen «systemadministrator – lege». Sistnevnte gruppe hadde tilgang til alt i systemet, inkludert redigering og sletting av journalnotater.

4.1.5 Kommunerevisjonens vurderinger

4.1.5.1 Oppsummering av kommunerevisjonens funn

Kommunerevisjonen har gjort en rekke interessante funn som berører tilgangskontrollen i Profdoc Vision ved KAD. Undersøkelsene som er gjort viser:

- Manglende implementering av skriftlige rutiner for tilgangskontroll ved KAD.
- Manglende beskrivelser av hvem som hadde myndighet til å autorisere systemleverandørens tilganger.
- Manglende jevnlig kontroll og gjennomgang av om tildelte tilganger var korrekte.
- Mangelfulle krav til passordkompleksitet og -lengde i alternativ påloggingsmetode i Profdoc Vision.
- Et manglende krav til jevnlig passordskifte i AKS for brukere av Profdoc Vision.
- For lang tid før terminalen ble automatisk låst med skjermlås.
- Utfordringer med ureglementert intern deling av systembrukere.
- Tildeling av tilganger utover hva brukergruppene tilsier at den aktuelle brukeren skal ha.
- Manglende oversikt over hvilke tilganger som var tildelt og hvem som hadde tildelt tilgangene.
- Helsepersonell som hadde tilgang til Profdoc Vision ville også ha tilgang til alle elektroniske meldinger uavhengig av hvilken brukergruppe de tilhørte. Oppslag i de elektroniske meldingene ble ikke logget.
- Stor bruk av utvidede tilganger uten at det var innført noen kompenserende kontrolltiltak.

Kommunerevisjonen påpeker også at Helseetaten ikke har en databehandleravtale med systemleverandør. Dette medfører at Helseetaten mangler et styringsverktøy for å sørge for at leverandøren behandlet personopplysningene i tråd med lov og forskrift.

4.1.5.2 Kommunerevisjonens konklusjon

Samlet sett vurderer kommunerevisjonen at det er avdekket betydelige svakheter ved tilgangskontrollen i Profdoc Vision. Dette medfører at sensitive personopplysninger ikke var beskyttet tilfredsstillende og at det eksisterer en risiko for at de kunne bli tilegnet av personer uten tjenstlig behov. Det medførte også en risiko for at opplysningene i systemet ikke var korrekte og pålitelige og at de ikke ville være tilgjengelige på rett tidspunkt. I tillegg bemerket kommunerevisjonen at det var nødvendig å vurdere å bruke kompenserende tiltak ved bruk av vide tilganger.

5 Helseetatens etterlevelse av utvalgte normkrav

I kapittel 4 har vi gjennomgått kommunerevisjonens revisjon av Profdoc Vision ved Kommunal akutt døgnenhet (KAD). I det følgende kapittelet skal vi gjennomgå funnene fra kommunerevisjonens rapport, samt funnene fra vår egen kontroll av Profdoc Visions etterlevelse av Normen i dag. Vi skal deretter holde funnene opp mot kravene til informasjonssikkerhet og personvern i Normen.

Kommunerevisjonen har ikke på noe tidspunkt uttalt at de har vurdert Profdoc Visions etterlevelse av Normen. Virksomheter som er tilknyttet Norsk helsenett[110] forplikter seg gjennom kontrakt til å følge denne.[111] Helseetaten, gjennom Profdoc Vision, er tilknyttet Norsk helsenettet, og er således forpliktet til å etterleve kravene i Normen. Vi har benyttet oss av Direktoratet for e-helses tilleggsdokument, «Oversikt over Normens krav», som et utgangspunkt for vår vurdering av om Helseetaten og Profdoc Vision etterlever kravene i Normen.[112]

5.1 Utvalgskriterier for kravene fra Normen

Vi har gjort et utvalg av kravene fra Normen da ikke alle omhandler eller er relevante for vår kontroll av Helseetatens tilgangskontroll i Profdoc Vision. Utvalget har blitt gjort basert på krav som vil gi et grunnlag for at vi skal kunne svare på problemstillingen vår. Vi har særlig lagt vekt på konfidensialitet i tilgangsstyringen, men har også med krav som omhandler tilgjengelighet. Årsaken til dette er at verdiene ofte har innvirkning på hverandre, og henger tett sammen.

Generelt kan vi dele Normens krav inn i to. *Tematiske kontroller* og *spesifikke kontroller*. De tematiske kontrollene er overordnede, brede kontroller som tar sikte på å avdekke etterlevelsen innenfor et bredt felt. For eksempel kan en tematisk kontroll stille følgende spørsmål:

> *«Sørger virksomheten for at krav til konfidensialitet etterleves?»*

110 Norsk helsenett (Udatert A).
111 Norsk helsenett (Udatert B).
112 Direktoratet for e-helse (2020 C).

En spesifikk kontroll er spissere i sin spørsmålsformulering, og kontrollerer i de fleste tilfellene konkrete deler av for eksempel konfidensialiteten. En spesifikk kontroll av konfidensialitet kan se slik ut:

«Innhenter virksomheten taushetserklæring for den enkelte medarbeider?»[113]

Flere spesifikke kontroller kan gjerne gi oss et bilde av om de tematiske kontrollene etterleves. De tematiske kontrollene er mindre hensiktsmessige å stille i et intervju, men de kan benyttes av revisor eller kontrollør for å huke av for etterlevelse av større områder i Normen etter at de spesifikke kontrollene har blitt undersøkt.

I vår undersøkelse har vi forsøkt å benytte så få tematiske kontroller som mulig. Vi stiller så konkrete spørsmål vi kan, og forsøker etter beste evne å besvare disse. Dette danner et grunnlag for å si noe om etterlevelsen av tilgangsstyringen og konfidensialiteten i Profdoc Vision ved KAD.

5.2 Helseetatens etterlevelse av Normens krav i dag

5.2.1 Om tabellene

5.2.1.1 Tabeller om Helseetatens etterlevelse av utvalgte normkrav

Kapittelet om resultatene fra kommunerevisjonens rapport, samt «Om Kommunerevisjonens rapport og Normen (vedlagt tabell)»[114] omtaler en etterlevelse som ligger opp mot 4 år tilbake i tid. Kommunerevisjonen har ikke konkret undersøkt alle tilgangsstyringskontroller fra Normen. Avhandlingen gir likevel et klart bilde av at det var store utfordringer med tilgangsstyring og konfidensialitet i systemet i 2016, da undersøkelsene ble gjort. Vi ønsker videre å sammenligne resultatene fra kommunerevisjonen med hvordan tilstanden er i dag. Svarene i tabellen vedlagt[115] er basert på tiltakene og rutinene Helseetaten og KAD hadde på plass i 2016, og er altså en *beskrivelse* av tilstanden slik den var. I tabellen er ikke etterlevelsen fastslått som en binær konklusjon. Etterlevelsen, eller mangelen på etterlevelse, er beskrevet. I tabell 1 «Om Helseetatens etterlevelse av utvalgte normkrav» vil vi derimot besvare etterlevelsen med et enkelt «Ja» eller «Nei». I enkelte tilfeller foreligger det ikke nok dokumentasjon til å kunne konkludere. Dette gjelder to av svarene, og i begge tilfeller er begrunnelsen at informantene våre ikke kjente til detaljene vi etterspurte.

113 Normens krav nummer 113.

114 Se vedlegg nr. 1.

115 Se vedlegg nr. 1.

I den vedlagte tabellen om kommunerevisjonens rapport og Normen gir vi en forenklet og praktisk gjennomgang av kommunerevisjonens funn, samtidig som vurderingen av Profdoc Visions etterlevelse av Normen også inngår. Tabellen «Om Kommunerevisjonens rapport og Normen (vedlagt tabell)» ligger kun som et vedlegg til avhandlingen. Dette er fordi vi i tabell 1 «Om Helseetatens etterlevelse av utvalgte normkrav» også inkluderer resultatene fra Kommunerevisjonens rapport. Tabell 1 viser derimot ikke dokumentasjonen eller vurderingene som avgjorde om vi godkjente kravene slik systemet var i 2016. Vi legger derfor til tabellen som et vedlegg slik at informasjonen også er tilgjengelig for leseren.

I tabell 1 «Om Helseetatens etterlevelse av utvalgte normkrav», nedenfor, har vi sammenlignet kommunerevisjonens funn med Normens krav, og avgjort hvorvidt kravene ble oppfylt i 2016. Som nevnt ovenfor blir funnene presentert binært, altså som et enkelt «Ja» eller «Nei».

I tillegg til å binært fastslå Profdoc Visions etterlevelse av Normen i 2016 har vi kontrollert etterlevelsen i dag. Dagens etterlevelse blir presentert ved siden av etterlevelsen i 2016. Ved å oppstille funnene på denne måten blir det tydelig om det har vært utbedringer, om etterlevelsen har stått stille, eller om det har vært en forverring av etterlevelse siden forrige kontroll.

5.2.1.2 Kontrollmetode for å avdekke etterlevelse i april 2020

For å avdekke hvordan Profdoc Vision ved KAD etterlever Normen i dag, kontaktet vi Helseetaten i Oslo kommune, og ba om et intervju med noen med oversikt over tilgangsstyringen i Profdoc Vision. Helseetaten, ved etatsdirektør, er systemeier for Profdoc Vision, og er også behandlingsansvarlig.[116] [117] En systemforvalter ved Helseetaten var intervjuobjekt ved kommunerevisjonens kontroll i 2016.[118]

Vi har intervjuet to personer med teknisk og organisatorisk oversikt over oppbygning og bruk av Profdoc Vision ved KAD. En seksjonsleder ved Fagsystemavdelingen hos Helseetaten i Oslo kommune, samt en systemforvalter ved samme avdeling. Begge har gitt oss verdifull innsikt i informasjonssikkerhetsarbeidet i Profdoc Vision og KAD. Systemforvalteren deltok på hovedintervjuet, hvor alle de utvalgte kravene fra Normen ble kontrollert.[119] Både seksjonsleder og systemforvalter har mottatt de samme spørsmålene, og svarene vi mottok fra

116 Personvernforordningen art. 4(7).
117 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
118 Kommunerevisjonen (2017) s. 24.
119 Se kapittel «5.1. Utvalgskriterier for kravene fra Normen».

systemforvalteren i hovedintervjuet er utarbeidet i samråd med seksjonslederen.

Før gjennomføringen av hovedintervjuet sendte vi over spørreskjemaet til systemforvalter og seksjonsleder, i henhold til deres ønske om å kunne forberede seg. Mange av spørsmålene krevde at intervjuobjektene måtte undersøke saken nærmere, og vi anså det derfor fornuftig at intervjuobjektene fikk anledning til å blant annet hente frem informasjon på forhånd, slik at svarene kunne bli så solide som mulig.

Normens krav, slik vi nevner i kapittel «5.1. Utvalgskriterier for kravene fra Normen», består både av det vi omtaler som *tematiske kontroller* og *spesifikke kontroller.* Vi har i størst mulig grad valgt ut kontroller blant de spesifikke kontrollene. Det er likevel noen av kontrollene som i seg selv er for generelle, og vi så derfor behovet for å ytterligere stykke opp disse. I tillegg til å være generelle, er mange av kontrollene ikke formulert slik at de kontrollerer *hvordan* noe gjøres, men snarere *at det gjøres.* Vi var interesserte i å avdekke *hvordan* noe ble gjort, og i etterkant selv avgjøre hvorvidt kravet kan sies å være oppfylt eller ikke.

Normens krav nummer 150 er et godt eksempel på et spørsmål som ikke avklarer hvordan noe gjøres. Kravet er formulert slik:

«*Bekrefter den autoriserte sin identitet på en sikker måte?*». Dette spørsmålets hensikt er å avgjøre hvorvidt for eksempel autentiseringsmetodikken som anvendes kan sies å være tilstrekkelig i forhold til sannsynlighet for og konsekvens av uønskede hendelser.[120]

Vi ønsket ikke å la det være opp til Helseetaten selv å avgjøre om de oppfyller dette. Vi formulerte derfor et kontrollspørsmål for å finne ut av *hvordan* dette ble gjort. Et av kontrollspørsmålene lyder: «Hvilke krav til passordkompleksitet stilles til de ulike påloggingsalternativene?». Ved å få svar på dette i tillegg til andre kontrollspørsmål ble vi i stand til å avgjøre hvorvidt Helseetaten hadde innført autentiseringsmetodikker som kunne sies å bekrefte den autorisertes identitet «[] … på en sikker måte».[121]

Før vi gjennomførte hovedintervjuet fikk systemforvalteren og seksjonslederen anledning til å se de utformede kontrollspørsmålene. I mange tilfeller er kontrollspørsmålene identiske med Normens krav, mens de i enkelte tilfeller er stykket opp, slik vi beskriver ovenfor. Vi har utfra svarene Helseetaten har gitt

120 Se kapittel «3.3.2. Risikoappetitt».

121 Se Normens krav nummer 150.

oss vurdert om normkravene etterleves. Vi ønsker å understreke at konklusjonene vi trekker er våre egne, basert på vår kjennskap til lovverk, Normens krav, informasjonssikkerhetsteori og -praksis, samt innhentet kunnskap og dokumentasjon om Profdoc Vision og KAD. Helseetatens egne vurderinger av Profdoc Visions etterlevelse av Normen fremkommer ikke av tabellen nedenfor. Vi har ikke kjennskap til hvordan de selv anser egen etterlevelse.

5.3 Tabellens oppbygning

Den første kolonnen i tabellen er vår egen nummerering av Normens krav, for enklere å kunne navigere ved hjelp av en nummerrekke i stigende rekkefølge. Den neste kolonnen i tabellen er Normens nummer. Dette har vi tatt med slik at det blir enkelt å finne spørsmålene igjen hvis leseren ønsker mer informasjon om den enkelte kontrollen. Denne er ikke i stigende rekkefølge. Årsaken er at vi i noen grad har gruppert spørsmålene tematisk, slik at sammenhengene mellom kontrollene kommer tydeligere frem. Deretter følger en kolonne som inneholder de normkravene vi har brukt i kontrollen i Profdoc Vision. Den neste kolonnen heter «Ble dette etterlevd ved kontroll i 2016?». Kolonnen inneholder informasjon om hvorvidt vi anser at kravet ble overholdt i 2016. Konklusjonen vi trekker er basert på tilgjengelig informasjon fra kommunerevisjonen. For å se hva vi har lagt til grunn for konklusjonen anbefaler vi å sammenligne det aktuelle spørsmålet med begrunnelsen fremstilt i «Om Kommunerevisjonens rapport og Normen (vedlagt tabell)». Kolonnen «Nummer» kan brukes til å finne frem til riktig spørsmål da samme spørsmål vil ha samme nummer i de to tabellene. Den siste kolonnen er «Etterleves dette i dag?». Her har vi, basert på informasjonen i kolonnene «Krav fra Normen» og «Oppsummering av svar fra intervju», vurdert om kravene overholdes eller ikke.

Så langt det lar seg gjøre vil hvert av Normens krav besvares med et «Ja» eller «Nei», avhengig av om vår kontroll og kommunerevisjonsrapporten avdekker etterlevelse av kravene eller ikke. «Ja» betyr at kravet etterleves, mens «Nei» betyr at kravet ikke etterleves.

5.4 Tabell 1: Om Helseetatens etterlevelse av utvalgte normkrav

Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etterleves dette i dag?
1.	69.	Sørger virksomheten for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med taushetsplikten?	Dette fremkommer ikke av rapporten.	Ja.
2.	127.	Sikres det at bare autorisert personell med tjenstlige behov får tilgang til helse- og personopplysninger?	Nei.	Nei.
3.	71.	Behandles brudd på taushetsplikten som avvik?	Dette fremkommer ikke av rapporten.	Ja.
4.	77.	Sikrer innsynet også loggen over hvem, og eventuelt fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, på hvilket tidspunkt?	Nei.	Nei.
5.	95.	Dokumenteres det alltid hvem det er gitt opplysninger til, og hvilken virksomhet denne tilhører?	Nei.	Nei.
6.	103.	Oppbevares opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logger) til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem?	Dette fremkommer ikke av rapporten.	Ja.
7.	96.	Gir helsepersonell tilgang til nødvendige og relevante helseopplysninger til samarbeidende personell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte, med mindre pasienten eller brukeren motsetter seg det?	Dette fremkommer ikke av rapporten.	Ja.

Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etterleves dette i dag?
8.	113.	Innhenter virksomheten taushetserklæring for den enkelte medarbeider?	Dette fremkommer ikke av rapporten.	Ja.
9.	115.	Har virksomheten etablert tiltak som ivaretar at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte?	Dette fremkommer ikke av rapporten.	Ja.
10.	118.	Leveres alle medier (herunder digitalt, papir, osv.) som kan inneholde helse- og personopplysninger når et arbeidsforhold opphører?	Dette fremkommer ikke av rapporten.	Ja.
11.	119.	Leveres adgangskort tilbake og deaktiveres ved opphør i arbeidsforhold?	Dette fremkommer ikke av rapporten.	Ja.
12.	120.	Sperres all tilgang ved opphør i arbeidsforhold?	Nei.	Nei.
13.	125.	Er tilgangsstyring etablert for alle informasjonssystemer?	Nei.	Nei.
14.	150.	Bekrefter den autoriserte sin identitet på en sikker måte?	Nei.	Nei.
15.	128.	Gis tilgang til behandlingsrettede helseregistre etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?	Dette fremkommer ikke av rapporten.	Ja.
16.	132.	Vurderes autorisasjonen på nytt når det oppstår endringer i ansvarsområder eller ansettelsesforhold eller langvarig fravær?	Dette fremkommer ikke av rapporten.	Ja.
17.	134.	Er autorisasjonen for tilgang til behandlingsrettede helseregister tidsbegrenset?	Nei.	Nei.

Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etter-leves dette i dag?
18.	135.	Angir autorisasjonen for tilgang til behandlingsrettede helseregister hvilke virksomheter autorisasjonen omfatter?	Nei.	Ja.
19.	136.	Er det etablert tiltak slik at mulig misbruk av autorisert teknisk personell, med særskilt behov for tilgang til større mengder helse- og personopplysninger, skal kunne avdekkes?	Nei.	Ja.
20.	137.	Grunngis og registreres bruk av selvautori-sering?	Ja.	Ja.
21.	160.	Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang? Eksempler på sikkerhetskrav: Behandlings-rettet helseregister må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	Nei.	Ja.
22.	138.	Er det etablert tekniske tiltak slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i informasjonssystemene hvem som har endret og hva som er endret? Eksempler på sikkerhetskrav der det ikke benyttes PKI: Passordfil skal krypteres	Dette fremkommer ikke av rapporten.	Ja.
23.	139.	Registreres all tildeling av autorisasjon i et autorisasjonsregister?	Ja.	Ja.
24.	122.	Har virksomheten rutiner for autorisering, endring og avslutning av tilganger?	Nei.	Nei.
25.	141.	Benytter bruker med administratortilganger personlig separat brukerkonto for administratoroppgaver?	Dette fremkommer ikke av rapporten.	Nei.

Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etterleves dette i dag?
26.	145.	Har virksomheten sørget for at det opprettes et autorisasjonsregister som minimum inneholder: 1. informasjon om hvem som er tildelt autorisasjon 2. til hvilken rolle autorisasjonen er tildelt (om rolle benyttes i virksomheten) 3. formålet med autorisasjonen 4. tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt 5. informasjon om hvilken virksomhet den autoriserte er knyttet til 6. helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk)	Nei.	Ja.
27.	147.	Har virksomheten oversikt over tilgjengeliggjøring av opplysninger til andre virksomheter?	Ja.	Ja.
28.	149.	Har dataansvarlig og virksomhetene som gis tilgang til opplysninger hos dataansvarlig avklart gjennom avtale eller på annen måte: hvordan autentisering skal foregå på en sikker måte hvordan autorisering til helseopplysninger hos dataansvarlig skal foregå hvordan logging og oppfølging av logger skal foregå	Dette fremkommer ikke av rapporten.	Ja.
29.	151.	Besluttes sikker måte på grunnlag av en risikovurdering?	Nei.	Nei.
30.	153.	Sikres det at flere personer ikke benytter samme autentiseringskriteria?	Nei.	Nei.
31.	154.	Tildeles autentiseringskriteria (som brukernavn og passord) på en betryggende måte?	Dette fremkommer ikke av rapporten.	Ja.

Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etterleves dette i dag?
32.	155.	Sikres tilgang fra hjemmekontor og/eller mobilt utstyr (og mobilnettverk) ved sikker autentiseringsløsning?	Dette fremkommer ikke av rapporten.	Ja.
33.	159.	Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)?	Dette fremkommer ikke av rapporten.	Nei.
34.	160.	Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang?	Nei.	Ja.
35.	161.	Foretar den enkelte leder gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner: 1. Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde? 2. Minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)? 3. Ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet?	Dette fremkommer ikke av rapporten.	Uavklart.
36.	162.	Varsles virksomhetens ledelse dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang?	Nei.	Ja.
37.	163.	Dersom kontrollen viser at det har skjedd en urettmessig tilgang, behandles det som et avvik?	Nei.	Ja.
38.	164.	Følges misbruk av selvautorisering opp som avvik?	Dette fremkommer ikke av rapporten.	Ja.
39.	170.	Er det etablert rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?	Dette fremkommer ikke av rapporten.	Uavklart.

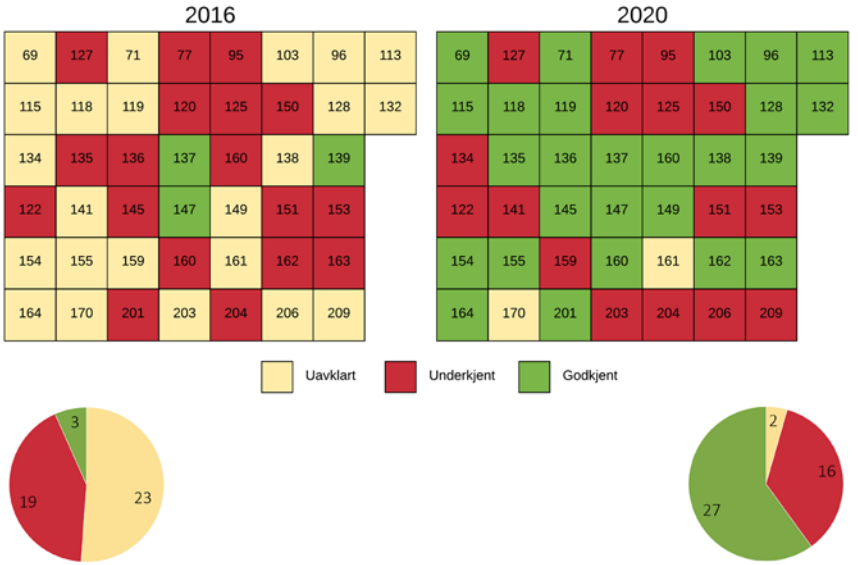
Nr.	Normens nr.	Krav fra Normen	Ble dette etterlevd ved kontroll i 2016?	Etterleves dette i dag?
40.	201.	Registreres som minimum følgende i loggene ved autorisert bruk av behandlingsrettet helseregister: 1. Identitet til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger 2. Organisatorisk tilhørighet 3. Grunnlaget for tilgjengeliggjøringen 4. Tidsperioden for tilgjengeliggjøringen	Nei.	Ja.
41.	203.	Kan loggene enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd?	Dette fremkommer ikke av rapporten.	Nei.
42.	204.	Er det etablert rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser?	Nei.	Nei.
43.	206.	Et det etablert rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister?	Dette fremkommer ikke av rapporten.	Nei.
44.	209.	Lagres logger, som genereres ved ytelse av helsehjelp, til det ikke antas å være bruk for dem?	Dette fremkommer ikke av rapporten.	Nei.

5.5 Statistikk til tabell

I tabell 1 har vi listet opp alle de 44 normkravene vi har kontrollert Profdoc Vision mot. Tabellen viser vår vurdering av Profdoc Visions etterlevelse av kravene, både i henhold til kommunerevisjonens rapport fra 2016 og basert på våre funn i 2020.

I figur 3 nedenfor har vi sortert og bearbeidet dataene fra begge kontroller, og sammenlignet dem. Vi ønsker med dette å avdekke hvorvidt det har vært en positiv, negativ eller ubetydelig endring i etterlevelsen i løpet av de siste fire årene. Statistikken er inndelt etter de samme måleparameterne som vi bruker

i tabellen, nemlig hvorvidt kravene er *uavklart, underkjent* eller *godkjent.* Kravene er sortert i samme rekkefølge som i tabellen, og ikke utelukkende i stigende rekkefølge. Se begrunnelse i kapittel «5.3. Tabellens oppbygning».



Figur 3: Endring av etterlevelse fra 2016 til 2020

Figuren viser to ulike fremvisninger av de samme dataene. *Kvadratdiagrammet* (øverst i figur 3) viser hvert enkelt av Normens krav, og etterlevelsen av disse, både i 2016 og i 2020. Ved å sammenligne de to kvadratdiagrammene kan du spore hvert av normkravene, og se hvorvidt etterlevelsen av det konkrete kravet du undersøker har endret seg siden 2016. *Sektordiagrammene* viser de samme dataene, men i stedet for å vise progresjon, blir dataene presentert som tall, og viser således andelen godkjente, underkjente og uavklarte krav, samt forholdet mellom dem.

Sektordiagrammet viser antallet godkjente, underkjente og uavklarte krav, men viser ikke hvorvidt et konkret krav har gått fra underkjent til godkjent. Som det fremkommer i sektordiagrammet som omhandler etterlevelse i 2016 var det hele 23 uavklarte normkrav. De må regnes som ukjente variabler, da de i realiteten kan være både godkjente og underkjente krav. På grunn av den store andelen ukjente variabler i dette diagrammet er det vanskelig å spore reelle endringer. Vi

har derfor utformet kvadratdiagrammet. Ved å sammenligne de to kvadratdiagrammene kan du spore hvert enkelt normkrav og dets endring i etterlevelse. Diagrammet illustrerer at svært mange av kravene som i 2016 var uavklarte nå er godkjente. Hele 15 krav som i 2016 var uavklarte er nå godkjente. Diagrammet viser også noe annet viktig; nemlig at ingen av de opprinnelig godkjente kravene har hatt negativ utvikling siden 2016. Derimot har 5 krav gått fra å være uavklarte til å bli underkjente. De 5 kravene kan ha vært underkjente også i 2016, selv om kommunerevisjonens rapport ikke avdekket dette. Diagrammet viser også noe annet viktig: 11 av kravene som i 2016 var underkjente, er fortsatt underkjente i 2020.

I kapittel 6 og 7 presenterer vi anbefalinger til tiltak for å utbedre krav som var underkjente ved vår kontroll våren 2020. Vi anbefaler at Helseetaten uavhengig av dette undersøker hvorfor hele 11 normkrav har forblitt underkjente de fire siste årene, på tross av at kommunerevisjonen avdekket dette i sin rapport.

6 Tiltak for utbedring av tilgangskontroll

6.1 Valg av tiltak

I forrige kapittel avdekket vi 16 underkjente normkrav i Profdoc Vision. Vi har sett det nødvendig å gjøre et utvalg av disse. Det er i hovedsak to årsaker til valget. For det første anser vi alvorlighetsgraden ved flere av bruddene som mindre enn ved bruddene vi skal utforme tiltak for. I tillegg vil en del av bruddene allerede bli løst ved tiltakene vi presenterer nedenfor. Vi har valgt ut de kravene vi anser det som viktigst å utbedre først, og vil videre komme med forslag til Helseetaten på hvordan tiltakene kan utbedres slik at normkravet overholdes. Nedenfor kommer individuelle begrunnelser for de normkravene som ikke er godkjent, men som vi likevel ikke vil behandle videre i avhandlingen.

Normens krav 125. Er tilgangsstyring etablert for alle informasjonssystemer?

Vi har ikke vurdert dette bruddet ettersom løsningen i hovedsak ligger i systemet *Pasinfo*.[122] Dette systemet faller utenfor avhandlingens rammer. Vi anbefaler likevel at Helseetaten ser nærmere på dette.

Normens krav 134. Er autorisasjonen for tilgang til behandlingsrettede helseregister tidsbegrenset?

Etter vår oppfatning vil ikke tidsbegrensning av tilganger nødvendigvis være det beste alternativet. Vi mener at tiltaket om deaktivering av brukere,[123] i tillegg til gode sletterutiner bør være tilfredsstillende. Vi anser det derfor som hensiktsmessig at Helseetaten mer direkte kobler tilganger opp mot ansettelsesforhold. På den måten kan brukerkontoene til ansatte som slutter enten slettes eller deaktiveres.

122. Har virksomheten rutiner for autorisering, endring og avslutning av tilganger?

122 Pasinfo: Helseetatens egenutviklede verktøy for uthenting av pasientinfo fra ulike systemer. Brukes gjerne ved flytting av pasienter fra et helsetilbud til et annet. Helseopplysningene om pasienten blir da hentet ut av et system (for eksempel Profdoc Vision) og kopiert over til informasjonssystemet ved det nye helsetilbudet.

123 Se kapittel «6.7.2.1. Deaktivering av brukere».

Kravet om rutiner for autorisering og endring av tilganger er godkjent i henhold til kravet. Det er rutiner for avslutning av tilganger som er manglende, og kravet er derfor underkjent. Ved å beholde de eksisterende rutinene, og i tillegg innføre deaktivering av brukere, anser vi kravet som overholdt.

141. Benytter bruker med administratortilganger personlig separat brukerkonto for administratoroppgaver?

Vi ser i likhet med Helseetaten ikke de helt store informasjonssikkerhetsfordelene med at en bruker med administratortilganger skal ha en personlig separat brukerkonto for administratoroppgaver. Vi anbefaler likevel at Helseetaten ser nærmere på problemstillingen.

159. Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)?

Kun dersom brukere ønsker tilgang til nasjonale komponenter kreves det forskjellig pålogging. I slike tilfeller vil nivå 4-pålogging være nødvendig. [124] De ulike rollene i Profdoc Vision har i stor grad like tilganger, og det vil derfor i første omgang være mer interessant å se på muligheten for å differensiere tilganger i større grad mellom ulike roller. Vi ser det naturlig at en slik vurdering vil inngå i en gjennomføring av risikovurdering, se kapittel «6.4.2.1. Risikovurdering».

209. Lagres logger, som genereres ved ytelse av helsehjelp, til det ikke antas å være bruk for dem?

Problemet her er mangelen på sletterutiner for logger. Vi har i avhandlingen ikke nevneverdig fokus på de ansattes personvern i Profdoc Vision. Logging av de ansatte og tilknyttede personvernkonsekvenser for de ansatte vil derfor ikke bli behandlet. Vi anbefaler likevel at Helseetaten etablerer gode rutiner for sletting av logger.

124 Nivå 4-pålogging: Bruk av bypass-kort og personlig kode.

6.2 Forklaring av figur

Figuren på neste side inneholder de resterende 10 normkravene vi anser som underkjent i dag. For å sortere kravene har vi delt kravene inn i 3 ulike kategorier. Kategoriene er omkranset av en blå rombe til venstre i figuren og er som følger:

Autentisering: Krav om at kun personer som har rett på tilgang får tilgang. [125]

Autorisering: Krav som omhandler hvem som skal få tilgang, typisk tildeling, endring og sletting av tilganger.[126]

Dokumentasjon: Krav som omhandler informasjon om brukeres oppførsel i systemet, samt kontroller av dette.

Fra de rombeformede kategoriene går pilene videre til de tilhørende normkravene. Dette er de røde ovalene i midten av figuren. Normkravene er nummerert etter normnummeret slik at leseren enkelt kan finne tilbake til det aktuelle normkravet i tabellen.[127]

Fra normkravene går pilen videre til de tilhørende tiltakene. De er plassert i de grønne rektanglene til høyre i figuren. Der det finnes piler mellom et normkrav og et tiltak betyr dette at tiltaket skal utbedre problemene identifisert gjennom normkravet. Utbedringene vil bli mer detaljert beskrevet videre i dette kapittelet.

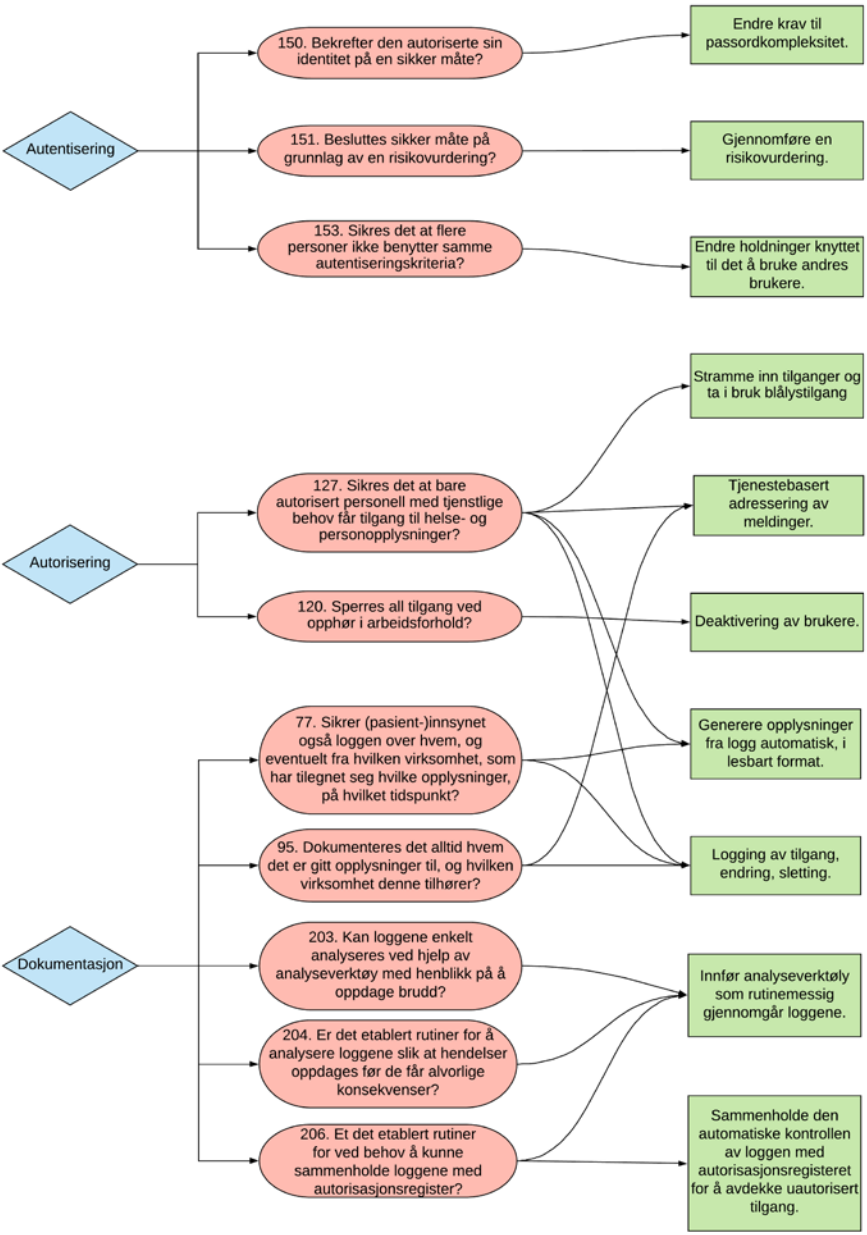
6.3 Normens krav nummer 150

6.3.1 Om kravet og status i dag

6.3.1.1 Den autoriserte skal bekrefte sin identitet på en sikker måte.

Ved pålogging eller forsøk på tilgang til helse- og personopplysninger i et elektronisk pasientjournalsystem må den autoriserte brukeren bekrefte sin identitet på en sikker måte. Kun autoriserte brukere skal gis tilgang til pasientjournalen. Systemet må derfor avklare hvorvidt den som utgir seg for å være en autorisert bruker faktisk er den han utgir seg for å være. Dette kalles autentisering. Det er ikke nok at en autorisert brukerkonto får tilgang til pasientjournalen; det må

125 Se kapittel «2.2.2.2. Autentisering som kontrollmetode for tilgang»
126 Se kapittel «3.3.5. Avgrense tilgang for autorisert personell».
127 Se kapittel «5.4. Tabell 1: Om Helseetatens etterlevelse av utvalgte normkrav».



Figur 4: Tiltak for utbedring av mangelfull etterlevelse av krav

avklares at brukerkontoen benyttes av et individ som faktisk har rett på tilgang. Detaljer om autentisering finnes i kapittel «2.2.2. Hva er tilgangskontroll?».

Hvordan slik autentisering skal gjennomføres avhenger av flere faktorer, deriblant hva den er ment å beskytte.[128] Strengere krav til autentiseringsmekanismene stilles desto mer beskyttelsesverdig et system eller informasjon er. Profdoc Vision inneholder primært sensitive personopplysninger, herunder store mengder helseopplysninger om identifiserte individer. Slik informasjon skal voktes strengt. Kun ansatte med tjenstlig behov skal få tilgang, og autentiseringen må derfor hindre at andre enn den reelle brukeren kan aksessere informasjonen.

6.3.1.2 Hva er sikker måte?

Hva som regnes som sikker måte avhenger som nevnt av hva som skal beskyttes, og hvem du spør. Det er likevel noen generelle føringer som et minimum bør etterleves. Om nødvendig bør man også innføre skjerpede krav for egen virksomhet, dersom man gjennom en risikovurdering kommer frem til at kravene til autentiseringsmetoden bør være ekstra streng for det aktuelle systemet.

Nasjonal sikkerhetsmyndighet (NSM) har utformet en rekke anbefalinger til passordkompleksitet og lengde, og vi mener de bør følges. En kombinasjon av lange passord, med bruk av spesialtegn er anbefalt. Minimum 16 tegn anses for å gi akseptabel beskyttelse.[129] Passord bør også være enkle å huske for brukeren. Passordfraser kan derfor være smart, fordi de er enkle å huske for brukeren, og fordi de enkelt kan tilfredsstille kravet til lengde. Dersom man i tillegg benytter dialektord og spesialtegn i frasen, kanskje også i kombinasjon med mellomrom, vil passordet styrkes ytterligere.

Nasjonal sikkerhetsmyndighet går også langt i å avkrefte den etablerte sannheten om nytten av å bytte passord ofte. En vanlig oppfatning er at man bør skifte passord ofte og regelmessig. Dette stemmer ikke, ifølge NSM. De potensielle konsekvensene av å bytte passord ofte utgjør i sum en større svakhet enn det å beholde passord lenge. Når en bruker tvinges til å bytte passord ofte kan dette føre til at de lager passord som er for korte, for enkle, eller at brukeren benytter ett felles passord for flere tjenester.[130] NSMs anbefaling er derfor å lage lange, komplekse passord som er enkle å huske, samt å ikke bytte oftere enn nødvendig. Man bør bytte passord dersom det mistenkes at passordet har kommet på avveie, eller dersom uvanlig aktivitet på kontoen oppdages. Virksomheten bør følgelig ha rutiner for å oppdage slikt, for eksempel ved å jevnlig gjennomgå

128 Datatilsynet (Udatert).
129 Nasjonal sikkerhetsmyndighet (2018).
130 Nasjonal sikkerhetsmyndighet (2019).

databaser med lekkede passord,[131] og ved å nøye kontrollere systemlogger for å avdekke uvanlig aktivitet.

6.3.1.3 Etterleves kravet i dag?

I kommunerevisjonens rapport fra 2017 avdekkes det at krav til passordkompleksitet er på åtte tegn, med en kombinasjon av store og små bokstaver, samt tall eller tegn.[132] Kommunerevisjonen konkluderte den gang med at det var mangler i kravene til kompleksitet og lengde på passordene. Ved kontroll av etterlevelsen av Normens krav i dag, har vi avdekket at de samme kravene til kompleksitet og lengde fortsatt benyttes i dag, uten at det har blitt foretatt endringer siden kommunerevisjonen publiserte sin konklusjon i 2017. Kravene oppfyller på ingen måte NSMs minimumskrav til passordkompleksitet. I tillegg har det ikke blitt gjennomført risikovurderinger for å kartlegge nødvendig passordkompleksitet. Kravene til passord i systemet i dag er med andre ord ikke basert på en kartlegging av risikobildet (sannsynlighet for og konsekvens av at en uønsket hendelse inntreffer) systemet befinner seg i. I tillegg til manglende passordlengde kan ikke Profdoc Vision tilby multifaktorautentisering, for eksempel ved bruk av adgangskort, kodebrikke eller fingeravtrykk i kombinasjon med brukernavn og passord.

6.3.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 150

6.3.2.1 Passordkompleksitet

Kravene til passordkompleksitet, og særlig lengde, bør skjerpes i Profdoc Vision. Vi anbefaler som minimum at brukere må opprette passord bestående 16 tegn, og som inneholder små og store bokstaver, tall og spesialtegn, i henhold til NSMs krav.[133] Videre bør Helseetaten få gjennomført en risikovurdering av Profdoc Vision, med sikte på å etablere konkrete autentiseringskrav tilpasset det reelle risikobildet. Vi er bevisst på at behovet for tilgang (tilgjengelighet) må veies opp mot kravet til konfidensialitet. Dersom man gjennom en risikovurdering finner at lange passord blir for tidkrevende i en hektisk situasjon, bør etaten innføre alternative autentiseringsmetodikker, slik som multifaktorautentisering, for å bøte på manglende passordkompleksitet.

131 Knudsen (2017).

132 Kommunerevisjonen (2017) s. 23.

133 Nasjonal sikkerhetsmyndighet (2018).

6.4 Normens krav nummer 151

6.4.1 Om kravet og status i dag

6.4.1.1 Besluttes sikker måte på grunnlag av en risikovurdering?

For å kunne fastslå hvilke autentiseringsmetodikker som skal benyttes, for eksempel i et informasjonssystem, må virksomheten ha det klart for seg hva som skal beskyttes og de potensielle konsekvensene av uautorisert tilgang.

6.4.1.2 Hva er en risikovurdering?

Ved å gjennomføre en verdivurdering og en risikovurdering, kan virksomheten kartlegge hvilke verdier de har, slik som sensitive personopplysninger eller forretningshemmeligheter, og hvilke av verdiene som må beskyttes. I tillegg skal en risikovurdering si noe om sannsynlighet for at en uønsket hendelse inntreffer, og hva de potensielle konsekvensene kan innebære. Til sammen skal dette danne et grunnlag for å vurdere om man må sette inn ekstra tiltak for å beskytte seg. Kanskje vil man innse at man må stramme inn rutinene for passordkompleksitet for å minske sannsynligheten for at noen får uautorisert tilgang til systemet.

Både personvernforordningen artikkel 32 og pasientjournalloven § 22 fastslår at man skal innføre egnede informasjonssikkerhetstiltak med hensyn til risikoen. For å kunne implementere egnede tiltak må virksomheten derfor avklare risikobildet, gjennom en risikovurdering.

6.4.1.3 Etterleves kravet i dag?

Kommunerevisjonens rapport fra 2017 fastslår at det ikke har blitt gjennomført en risikovurdering knyttet til Profdoc Vision.[134] Virksomheten hadde heller ikke kartlagt hvilke informasjonsverdier de hadde. Sammenlagt bidrar dette til at virksomheten har liten oversikt over hva som må beskyttes, og hvordan. Det samme ser ut til å være tilfellet også i april 2020. Systemforvalteren i Fagsystemavdelingen forteller at Oslos Byråd for Finans gir retningslinjer om passord, men at retningslinjene ikke er basert på en risikovurdering for hverken Helseetaten eller Profdoc Vision konkret. Basert på informasjonen systemforvalteren gir ser det ut til at kravene til autentiseringsløsning er felles for Oslo kommune, og ikke konkret tilpasset et pasientjournalsystem.[135] Alt i alt vil virksomheten ha et dårlig beslutningsgrunnlag når de fastsetter autentiseringsmetodikker når en risikovurdering eller tilsvarende analyse ikke har blitt utført. Det er også potensielt problematisk at generelle føringer til passordkompleksitet gis til hele kommunen, og ikke er individuelt tilpasset ulike fagområder og systemer.

134 Kommunerevisjonen (2017) s. 21.

135 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

6.4.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 151

6.4.2.1 Risikovurdering

Vi anbefaler at Helseetaten gjennomfører en risikovurdering for bruken av Profdoc Vision i Helseetaten. Det er nødvendig for å beslutte hva pålogging på sikker måte må innebære. Byråd for Finans hadde trolig ikke gjennomført en generell risikovurdering av Oslo kommune og ikke spesifikt av Helseetaten og Profdoc Vision. Vi mener det vil være nødvendig å gjennomføre dette. Årsaken er at systemer og selskaper er ulike, og krav og tiltak som bør innføres vil da også være forskjellige for å tilpasses det enkelte tilfellet. Helseetaten er etter vår mening best skikket til å gjennomføre en risikovurdering av Profdoc Vision ettersom de har best kjennskap til systemet. Kunnskap om systemet og bruken av dette er nødvendig for å gjennomføre en tilstrekkelig risikovurdering. Helseetaten må kartlegge beskyttelsesverdigheten av personopplysningene i Profdoc Vision, for å finne ut hva autentisering på en tilstrekkelig sikker måte vil innebære i Profdoc Vision. Videre må Helseetaten identifisere hvilke uønskede konsekvenser som potensielt kan forekomme i systemet. Det innebærer at de kartlegger på hvilke måter personopplysninger kan komme på avveie. Her må Helseetaten både vurdere hvilke utilsiktede og tilsiktede hendelser som kan forekomme. Deretter må Helseetaten vurdere sannsynligheten for at hendelsene oppstår. Konsekvensene av hendelser og sannsynlighet for at hendelser oppstår danner tilsammen risikoen i systemet.[136] Det står i Normens krav 151 at sikker autentiseringsmetodikk skal fastsettes på bakgrunn av en risikovurdering. Dermed må autentiseringskravene bygge på konklusjonene fra risikovurderingene. En større risiko krever en sikrere autentisering.

6.5 Normens krav nummer 153

6.5.1 Om kravet og status i dag

6.5.1.1 Sikres det at flere personer ikke benytter samme autentiseringskriteria?

I et pasientjournalsystem, som i mange andre typer informasjonssystemer, er det viktig å avklare hvem som skal ha tilgang til hva. Ikke all informasjon skal deles med alle systembrukere. I mange tilfeller er det oppstilt lovkrav som setter generelle føringer for hvem som skal se hva, og hvordan deling kan foregå. For elektroniske pasientjournalsystemer gjelder pasientjournalforskriften § 13. Paragrafen oppstiller krav til tilgangsstyring, og paragrafens annet ledd tydeliggjør at journaloppføringer bare kan gjøres tilgjengelig for personell som kan bekrefte sin identitet på en sikker måte. I tillegg til dette gjelder naturligvis taushetsplikten etter helsepersonelloven § 21 også her. Taushetspliktsbestemmelsen

136 Datatilsynet (2019).

i helsepersonelloven tydeliggjør også at opplysninger kun skal deles med de som har tjenstlig behov for dette. Helsepersonelloven § 21 a oppstiller et forbud mot å tilegne seg opplysninger man ikke har tjenstlig behov for.[137] Bestemmelsen er også kjent som «snokeforbudet».[138] Dette er ment som et tillegg til taushetsplikten, og sammen skal de to paragrafene sørge for at helsepersonell ikke deler opplysninger med andre uten tjenstlig behov, at de aktivt hindrer andre i å få tilgang til taushetsbelagte opplysninger, samt at de ikke selv forsøker å tilegne seg opplysninger. Detaljer om taushetsplikt finner du i kapittel «2.2.1.1. Konfidensialitet og taushetsplikt».

Normens krav nummer 153 sier at virksomheten (dataansvarlig) skal sørge for at flere personer ikke benytter samme autentiseringskriteria. Med dette menes det at for eksempel brukernavn, passord og adgangskort skal være personlig, og ikke benyttes for å gi andre enn den de tilhører adgang. Begrunnelsen for at kun de med tjenstlig behov skal ha tilgang er som nevnt ovenfor at helsepersonell er underlagt taushetsplikt. Ved å dele tilganger mister man raskt oversikt over hvem som ser hva, og konfidensialiteten vil forringes. Kravene til tilgangsstyring, jf. pasientjournalforskriften § 13, er ment å understøtte blant annet taushetsplikten. Tilfredsstillende tilgangsstyring kan kun oppnås dersom dataansvarlig kan kontrollere hvem som ser hva.

Helsepersonell er også underlagt journalføringsplikt, jf. helsepersonelloven §§ 39 og 40. I helsepersonelloven § 40 er det et krav om at det i journal skal fremgå hvem som har ført opplysninger i journalen. Dersom brukernavn, passord og adgangskort benyttes av flere enn den tiltenkte vil oversikten over hvem som har ført i journal miste verdi, da «låneren» kan skjule seg bak en annens identitet i journalen.

6.5.1.2 Etterleves kravet i dag?

I kommunerevisjonsrapporten fra 2017 avdekkes det at det var gjentatte brudd på lovkravene nevnt ovenfor, og også kravet fra Normen. Ansatte benyttet hverandres brukerkontoer for å registrere i journalen. Dette skjedde gjerne ved at ansatte lot datamaskinen sin stå ulåst, og på den måten la til rette for at andre benyttet den til å registrere eller endre i journal. Begrunnelsen for at dette ble gjort var at det tok så lang tid å logge på løsningen at brukerne ofte valgte å ikke logge ut ved kortere fravær fra plassen sin. Det fremkommer ikke av rapporten hva det er som gjør at det tar tid å logge på løsningen.

137 Se også pasientjournalloven § 16.

138 Kanestrøm (2010).

Ved spørsmål om det samme i april 2020, finner vi at den samme praksisen fortsatt eksisterer. Det hender fortsatt at brukere registrerer opplysninger gjennom andres brukerkontoer, og at tilgang til journalen oppnås på denne måten. Det presiseres at det gjerne skjer i situasjoner hvor det er akutt behov for tilgang, der det står om liv og død, og hvor helsepersonellet ikke har tid til å vente. På direkte spørsmål fremkommer det at det også gjøres i situasjoner hvor det ikke dreier seg om liv og død.[139] Årsaken til at dette gjøres er fortsatt fordi det tar tid å logge ut og inn, begrunnet i tregheter i systemet, og ikke på grunn av passordkompleksitet eller annet som har med autorisasjonsløsningen å gjøre.

Helseetaten har understreket overfor brukerne av Profdoc Vision at brukerkontoer ikke skal deles på denne måten. Det er i tillegg tydeliggjort i brukererklæringen de ansatte må signere ved ansettelse.

6.5.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 153

6.5.2.1 Holdningsendringer

Vi anser det nødvendig at KAD har et tydelig fokus på at de ansatte skal benytte sine egne brukerkontoer. Undersøkelsene våre avdekket at det forekom tilfeller der ansatte lot brukerkontoene stå åpne slik at andre kunne benytte seg av dem. Helseetaten bør derfor gjennomføre en kampanje rettet mot ansatte ved KAD for å øke både bevisstheten og kunnskapen omkring viktigheten av å sikre egne brukerkontoer blant de ansatte. Overholdelse av taushetsplikten er en viktig del av en helsearbeiders hverdag, og nettopp å «låne» bort en brukerkonto kan være et brudd på denne plikten. Dersom det er skapt en kultur der dette gjøres for enkelhets skyld eller for å være hyggelig mot andre ansatte, kan en holdningskampanje være effektiv for å endre dette. Vi mener det må tydeliggjøres hvorfor det er viktig at denne type «lån» av brukerkontoer ikke skal forekomme. For det første kan den som «låner» bort brukerkontoen gjøre det enkelt å snoke i pasientopplysninger uten at snokeren legger igjen spor i loggene. Det vil dermed være «utlåneren» sin identitet som blir logget. Ikke bare kan pasientopplysninger da komme på avveie, men du vil altså være ansvarlig for dette ved å ha brutt taushetsplikten. Det samme vil være tilfelle dersom «låneren» av brukeren din redigerer eller sletter innhold ved å bruke din konto. Det vil også være din konto som vil bli logget til hendelsen. Mange av kontrollmekanismene i Profdoc Vision er tilknyttet kontroll og logging av brukere. Dersom flere benytter samme brukerkonto, eller dersom en brukerkonto «lånes» bort, vil slike kontroller være svake og miste sin verdi. Helseetaten vil da ikke kunne spore hvem som faktisk benyttet brukeren. Vi anser det derfor som sentralt at slik praksis ikke forekommer, dersom det ikke er helt nødvendig. Hvordan holdningsendringen skapes vil vi ikke legge klare føringer for. Det viktigste er at kampanjen når helseper-

139 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

sonellet slik at det etableres en praksis og en felles forståelse av at «lån» av brukerkontoer ikke er greit.

6.6 Normens krav nummer 127

6.6.1 Om kravet og status i dag

6.6.1.1 Sikres det at bare autorisert personell med tjenstlig behov får tilgang til helse- og personopplysninger?

Normens krav nummer 127 er tett knyttet til krav nummer 153. Begge krav dreier seg direkte om tilgangsstyring og taushetsplikt, og om at virksomheten (dataansvarlig) skal ha kontroll med at det kun er de med tjenstlig behov som skal få tilgang til helse- og personopplysninger. Der krav nummer 153 konkret dreier seg om autentiseringskriteria, dreier krav nummer 127 seg om tilgangsstyring og overholdelsen av taushetsplikten i systemet forøvrig. Se første avsnitt i kapittel «5.3. Normens krav nummer 153» for detaljer om lovkrav og begrunnelse for tilgangsstyring.

6.6.1.2 Etterleves kravet i dag?

Som omtalt i kapittelet «5.3. Normens krav nummer 153» ble det i kommunerevisjonens kontroll av tilgangsstyringen i Profdoc Vision avdekket at brukerkontoer ble delt mellom brukere. Dette kan både føre til at brukere får tilgang til opplysninger de ikke har tjenstlig behov for å se, og at journaloppføringer blir vanskelig å spore. Dette gjelder også i dag.[140]

Kommunerevisjonen avdekket også at samtlige ansatte med tilgang til Profdoc Vision, uavhengig av brukergrupper eller tilgangsbehov, hadde full tilgang til en felles meldingsboks. Den ble benyttet til kommunikasjon med spesialisthelsetjenesten og den kommunale pleie- og omsorgstjenesten.[141] Meldingene inneholdt blant annet informasjon om pasientens hjelpebehov, årsak til innleggelse og funksjonsnivå. Meldingsboksen har ikke tilgangsstyring, og således kan alle med tilgang til Profdoc Vision nå alle meldinger, og se innholdet i dem.[142] Det var heller ikke etablert noen form for logging av oppslag i meldingsboksen. Det vil derfor være svært vanskelig å kontrollere hvem som har sett hva. Snoking i helseopplysninger, jf. helsepersonelloven § 21 a, vil vanskelig kunne oppdages. Loggføring kan ha en avskrekkende effekt på potensielle snokere, og kjent mangel på logg kan i verste fall ha motsatt effekt. Dersom en pasient ber om innsyn i sin pasientjournal, skal vedkommende også få kjennskap til hvem som har sett

140 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
141 Kommunerevisjonen (2017) s. 25.
142 Kommunerevisjonen (2017) s. 25.

i journalen.[143] Se «6.8. Normens krav nummer 77» for ytterligere detaljer om dette. At de ansatte vet at pasientene vil få kjennskap til at de har sett i journalen, kan også virke avskrekkende, og således minimere antall snoketilfeller.

Når du i kraft av å være helsepersonell fører inn helseopplysninger i et system hvor personell uten tjenstlig behov enkelt kan få tilgang til det du skriver, bryter du i praksis den lovpålagte taushetsplikten din, jf. helsepersonelloven § 21. Det er lite du som ansatt kan gjøre med dette, fordi du må benytte arbeidsverktøyene du får utdelt, herunder kommunikasjonsverktøyene, for å kunne utføre ditt arbeid. Ved å tilby helsepersonell et verktøy som bidrar til brudd på den lovpålagte taushetsplikten, bryter dataansvarlig med helsepersonelloven § 16, som omhandler virksomhetens plikt til å legge til rette for at helsepersonellet kan overholde sine lovpålagte plikter.

På spørsmål om hvordan tilgangsstyring og logging i meldingsboksen håndteres i dag, svarer systemforvalteren at tilgangsstyring i meldingsboksen og Profdoc Vision for øvrig er en kompleks problemstilling. På den ene siden har pasientene rett på konfidensiell behandling av helse- og personopplysningen. Dette kan innebære en streng tilgangsstyring hvor hver ansatt har begrenset tilgang, og hvor man i særlige tilfeller må søke eller be om utvidede tilganger. På en annen side har man pasientens behov for effektiv og sikker helsehjelp. Dette avhenger blant annet av at helsepersonell har effektiv tilgang til helse- og personopplysninger om pasienten. Videre sier hun at denne tilgangen kanskje må veie tyngre enn konfidensialiteten. Det fremkommer ikke av svaret hvordan tilgangsstyring og logging i meldingsboksen håndteres i dag.

Vi spør konkret om det har vært gjort endringer i tilgangsstyring og logging i meldingsboksen siden kommunerevisjonens konklusjoner i 2017. Systemforvalteren svarer da «ingen kommentar».[144]

Basert på dette datagrunnlaget kan vi ikke si sikkert om tilgangsstyringen og loggingen har blitt strammet inn siden kommunerevisjonen utførte tilsyn. Vi velger derfor å utforme forslag til utbedringer, basert på status slik den ble beskrevet i 2017.

6.6.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 127

6.6.2.1 Tjenestebasert adressering av meldinger.

Bruken av en felles og åpen meldingsboks uten noen form for logging nevnt i kapittel «6.6.1.2. Etterleves kravet i dag?» er årsaken til at vi mener at ikke kun

143 Jf. Pasient- og brukerrettighetsloven § 5-1, pasientjournalloven § 18, samt helsepersonelloven § 45.
144 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

autorisert personell med tjenstlig behov har tilgang til personopplysninger i systemet. Meldinger som mottas i meldingsboksen kan ses av alle med tilgang til Profdoc Vision.

For å sikre at meldinger mottas og leses av konkrete mottakere eller fagavdelinger, mener vi at Helseetaten bør innføre såkalt «tjenestebasert adressering» av meldinger.[145] Dersom tjenestebasert adressering tas i bruk, kan Helseetaten sørge for at ikke alle meldinger ligger ute tilgjengelig for alle med tilgang til Profdoc Vision. Vi ønsker at Helseetaten skal følge samme standard som Direktoratet for e-helse anbefaler.[146] KAD vil da få tildelt et virksomhetsnummer, og alle meldinger som sendes fra eksterne avsendere og er merket med dette virksomhetsnummeret, vil ankomme KAD. I tillegg skal meldingene markeres med en «tjenestetype». Dette kan for eksempel være «Psykologtjeneste» eller «Saksbehandling».[147] De ulike tjenestene vil inneha ulike nummer. På den måten vil de elektroniske meldingene ankomme det spesifikke tjenesteområdet hos KAD spesifikt og uten at den vil være synlig for enhver med tilgang til Profdoc Vision.

6.6.2.2 Logging av tilgang, endring og sletting

Vi anbefaler å innføre logging av tilgang, endring og sletting av de elektroniske meldingene i Profdoc Vision. Dette mener vi bør innføres uavhengig av om Helseetaten innfører tjenestebasert adressering av meldinger. Som tidligere nevnt i kapittel «6.6.1.2. Etterleves kravet i dag?» føres det ingen logg ved bruk av elektroniske meldinger i Profdoc Vision. Det vil være mulig å snoke og endre i meldingsboksen uten at Helseetaten har gode verktøy for å oppdage slike handlinger. Vi anser dette som problematisk. Ved å innføre logging ved tilgang, endring og sletting i elektroniske meldinger kan Helseetaten kontrollere hvem som gjør og ser hva i meldingsboksen. Logging vil ikke begrense tilgang, det vil derimot kunne gjøre det mer risikabelt å «snoke» i meldingene ved at logging kan ha en avskrekkende effekt mot dette. Ansatte med tjenstlig behov for de enkelte meldingene vil da heller ikke bli berørt av dette tiltaket, bortsett fra at det logges at de har vært inne i meldingene. Føring av logger vil ikke i seg selv føre til at uvedkommende ikke får tilgang til helse- og personopplysninger. Loggene må også kontrolleres for å kunne beskytte opplysningene. Logger kan derimot være viktig for å dokumentere hva en bruker ser og gjør i systemet. Slik dokumentasjon vil være gunstig dersom Helseetaten ønsker å gi advarsler til ansatte som bryter taushetsplikten og nødvendig dersom det fører til at Helseetaten vil avslutte arbeidsforholdet på bakgrunn av dette.

145 Direktoratet for e-helse (2020 C).
146 Direktoratet for e-helse (2020 C).
147 Direktoratet for e-helse (2020 C).

Det er verdt å merke seg at føring og arkivering av logg også generer personopplysninger. Loggene må derfor behandles korrekt, og i henhold til helse- og personvernlovgivning.[148] NSM påpeker at det bør vurderes hva og hvor mye som skal oppbevares, og hvor lenge loggene skal oppbevares. Det er også viktig at Helseetaten er bevisste på hvordan loggene skal arkiveres, beskyttes og til sist slettes. En viktig del av beskyttelsen av logger er å sørge for at loggene ikke blir manipulert.[149]

6.6.2.3 Generere opplysninger fra logg automatisk, i lesbart format

For at tiltaket med logging av de ansattes bruk av meldingsboksen skal ha en effekt må det være mulig å gjennomgå loggene, og dette må gjøres rutinemessig. For å gjøre dette effektivt bør opplysninger fra loggen av meldingsboksen kunne genereres automatisk i et lesbart format. Sannsynligheten for å oppdage bruk av meldingsboksen blant ansatte som ikke har tjenstlig behov vil også øke i takt med hyppigheten av kontroller. Det er derfor viktig at kontrollene kan gjennomføres jevnlig, og det vil derfor være sentralt at en slik kontroll ikke er for tidkrevende. Vi mener derfor at loggene må kunne genereres automatisk i menneskelesbart format. Innsynskrav fra pasienter i egen journal og tilgangslogg forekommer også. Det vil være betydelig enklere å imøtekomme slike innsynskrav dersom loggen enkelt kan forstås av mennesker, uten at for mye tolkning må gjennomføres før pasienten forstår innholdet.

6.6.2.4 Stramme inn tilganger og ta i bruk blålystilgang

Tilgangen til helseopplysninger bør innskrenkes slik at helsepersonellet kun har tilgang til det nødvendige. For å sikre at helsepersonellet har tilgang til opplysninger de behøver i enhver situasjon hvor behovet melder seg, er bruk av blålystilgang med tilhørende kontroll et godt virkemiddel.[150] Selvautorisering lar en bruker få tilgang til opplysninger, journaler eller filområder til tross for begrensninger i hva brukerens rolletilhørighet skal ha tilgang til. En slik funksjon benyttes gjerne i tilfeller hvor vedkommende trenger umiddelbar tilgang til opplysninger, for eksempel i en akuttsituasjon. Dersom blålystilgangen benyttes, må helsepersonellet oppgi en skriftlig begrunnelse for tilgangen, i tillegg til at hendelsen logges, og nærmeste leder varsles.

Blålystilgangen er en enkel og smart måte å ivareta tilgjengeligheten i et system, samtidig som konfidensialiteten bevares. Vi anbefaler å stramme inn tilgangene, samt ta i bruk eksisterende muligheter for blålystilgang.

---

148 Se blant annet pasientjournalloven § 25 og personvernforordningen art. 5(1) bokstav e (lagringsbegrensning).

149 Hoff (2017).

150 Blålystilgang: Se kapittel «4.1.3. Brukeradministrasjon».

6.7 Normens krav nummer 120

6.7.1 Om kravet og status i dag

6.7.1.1 Sperres all tilgang ved opphør i arbeidsforhold?

I et pasientjournalsystem, som i alle andre systemer hvor det foregår behandling av helse- og personopplysninger, plikter behandlingsansvarlig (det samme som dataansvarlig, jf. pasientjournalloven § 2 bokstav e) å ivareta konfidensialiteten i systemet.[151] Dette vil blant annet innebære å sørge for tilstrekkelig tilgangsstyring, slik at kun de med tjenstlig behov får tilgang til helse- og personopplysninger. Tilgang til helseopplysninger skal kun gis i medhold av pasientjournalloven § 6. Tilgangen skal være nødvendig for å yte helsehjelp, administrere, kontrollere eller kvalitetssikre nevnte helsehjelp.[152] Se også kapittel «2.2.1. Hva er konfidensialitet og tilgjengelighet?».

Tilganger skal avsluttes så snart en bruker ikke lenger har tjenstlig behov for tilgangen. Når en bruker slutter i jobben hos KAD, skal tilgangen til helseopplysningene opphøre.[153] Vedkommende har ikke lenger tjenstlig behov for slik tilgang.

6.7.1.2 Etterleves kravet i dag?

I kommunerevisjonens rapport fra 2017 avdekkes det at tilganger til Profdoc Vision ikke sperres ved opphør i arbeidsforhold. Det ser ikke ut til at det er noen form for systemlogikk mellom ansettelsesforhold og tilgang.[154] I stedet kjøres et skript[155] månedlig, som har som oppgave å slette brukere som har vært inaktive i seks måneder. Dette innebærer at sletting av tilganger ved opphør av arbeidsforhold reelt sett ikke gjøres, men at slettingen tar hensyn til siste brukeraktivitet. Hvorvidt en bruker kan omgå denne løsningen ved å simpelthen logge inn minst en gang i halvåret, og på den måten utvide tidsrammen for sin tilgang også etter endt arbeidsforhold, fremgår ikke i klartekst av rapporten, men det fremstår for oss som en reell mulighet. Vi anser det som et brudd på pasientjournalforskriften § 13 første ledd å bevare en slik tilgang i så mye som et halvt år etter endt arbeidsforhold. Dette gjelder uavhengig av om brukere aktivt kan utvide sin tilgang også utover de første seks månedene etter endt arbeidsforhold.

Da vi i april 2020 undersøkte sperring av tilgang ved endt arbeidsforhold, fant vi ut at status i dag i stor grad sammenfaller med slik det var da kommunerevisjonen utførte sin revisjon. Systemforvalteren forklarer at mange ansatte sier at de

151 Personvernforordningen art. 32(1) bokstav b.
152 Pasientjournalloven § 6 annet ledd.
153 Pasientjournalforskriften § 13 første ledd bokstav e.
154 Kommunerevisjonen (2017) s. 25.
155 Rossen (2019).

skal komme tilbake og jobbe som vikarer etter endt arbeidsforhold. Av den grunn beholdes mange brukerkontoer i lang tid etter at de ansatte slutter. Hvorvidt kontoene holdes åpne fordi de ansatte faktisk jobber som vikarer, fremkommer ikke klart av systemforvalterens svar, men svaret hennes tilsier at det er intensjonen om å jobbe som vikar som gjør at kontoen holdes åpen. På samme måte som tidligere, kjøres et skript månedlig, som sletter kontoer som har vært inaktive i seks måneder.

Vi har forståelse for at fullstendig sletting av brukerkontoer umiddelbart etter at ansettelsesforholdet opphører kan være upraktisk når de ansatte svært ofte kommer tilbake og jobber som vikarer kort tid etter. Vi mener likevel at dette ikke forsvarer at tilgangen opprettholdes i hele seks måneder etter at det tjenstlige behovet bortfaller, og at Normens krav nummer 120 brytes. Nedenfor presenterer vi alternativer til dagens praksis.

6.7.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 120

6.7.2.1 Deaktivering av brukere

Vi anbefaler en endring i dagens praksis. I stedet for å slette samtlige brukerkontoer, inkludert brukere som indikerer at de etter ansettelsesforholdets slutt ønsker å ta på seg vakter, for eksempel i ferier eller lignende, kan brukerne deaktiveres. Vi mener med dette at brukerne ikke skal slettes, men at tilgangen deres til Profdoc Vision skal deaktiveres frem til de skal jobbe hos KAD igjen. Da skal det være enkelt å aktivere brukeren igjen. På den måten hindrer Helseetaten at tidligere ansatte har tilgang til Profdoc Vision i en periode etter arbeidsforholdets slutt. Samtidig bør dette minske en del av arbeidsbyrden med å slette og opprette brukere, noe vi antar krever større ressurser enn det å kun aktivere brukerne på nytt. Vi anbefaler også at dette skjer med ansatte som tar ut lengre ferier, permisjoner eller av andre grunner ikke vil behøve tilgang til Profdoc Vision over lengre tidsperioder. Helseetaten og KAD får i samråd avgjøre hvem i virksomheten som skal ha myndighet til å aktivere brukerkontoer igjen.

6.8 Normens krav nummer 77

6.8.1 Om kravet og status i dag

6.8.1.1 Sikrer (pasient-)innsynet også loggen over hvem, og eventuelt fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, på hvilket tidspunkt?

Normens krav nummer 77 er ment som en kontroll av om en pasients innsynskrav i journal og tilhørende bilag også sikrer at pasienten får vite hvem som har

hatt tilgang til helse- og personopplysninger.[156] Helse- og personopplysninger kan deles mellom samarbeidende helsepersonell,[157] og helsepersonell med tjenstlig behov skal ha tilgang til opplysningene. Som nevnt i kapittel «6.6. Normens krav nummer 127» forekommer det dessverre snoking. Loggføring, og tilgjengeliggjøring av loggen til pasient og bruker, kan være et viktig verktøy i kampen mot snoking, på grunn av tiltakets preventive effekt. Bevissthet om at man kan bli oppdaget kan virke avskrekkende. I tillegg til å være et viktig virkemiddel i kampen mot snoking, vil en slik logg kunne hjelpe pasienten med å kontrollere at behandlingen av helseopplysninger gjøres i henhold til vedkommendes uttrykkelige ønsker.[158]

6.8.1.2 Etterleves kravet i dag?

Da kommunerevisjonen kontrollerte Profdoc Vision ved KAD i 2016, fant de at det eksisterte sikkerhetslogger. Loggene inneholdt informasjon om hvilke brukere som logget seg av og på Profdoc Vision, og når dette ble gjort. Det ble også logget når brukerne åpnet en pasientjournal. Det fremgår ikke av rapporten hvorvidt loggen viser hvilke opplysninger i journalen brukerne har sett på, eller hvilken virksomhet brukerne tilhører. Et annet viktig funn gjort av kommunerevisjonen er at tilgang til opplysninger i den mye omtalte meldingsboksen ikke logges i det hele tatt. Det eksisterer med andre ord ingen kontroll med hvem som har sett hva i meldingsboksen. Det fremgår ikke eksplisitt av kommunerevisjonens rapport hvorvidt oversikten over hvem som har sett hva vil vedlegges ved et pasientinnsyn, i henhold til lovkrav og Normens krav nummer 77. Dersom en slik oversikt blir vedlagt journalen ved innsyn, vil den likevel ha store mangler, da Helseetaten ikke har tilgang til påkrevd dokumentasjon.

Da vi i april 2020 undersøkte pasientinnsyn og tilgang til informasjon fra loggen, fant vi at det fortsatt var noen mangler. 3. april 2020 ba vi om innsyn i informasjonen om oss, i *Lov om pasient- og brukerrettigheter* (heretter pasient- og brukerrettighetsloven) § 5-1, første ledd og personvernforordningen art. 15. Dagen etter ble journalen postlagt, og mottatt omtrent to dager senere, rundt den 6. april.

Journalen inneholder opplysninger om hvem som har skrevet opplysninger i journal, men ingen opplysninger fra logg er vedlagt eller ført i journalen, på tross av at innsynsbegjæringen også inneholder krav om tilgang på slike opplysninger. Det fremgår ikke av journalen hvem som har sett hva i journalen.

156 Pasient- og brukerrettighetsloven § 5-1, personvernforordningen art. 15.
157 Helsepersonelloven § 25.
158 Pasientjournalloven § 17.

Basert på kontrollen anser vi ikke krav nummer 77 for oppfylt.

Den 27. april 2020 spurte vi systemforvalteren i fagsystemavdelingen hos Helseetaten om hvordan slike pasientinnsyn håndteres, og om pasientene får tilgang til å se hvem som har sett hva, og når, i journalen deres. Hun mente da, etter å ha konferert med sjefen sin, at et journalinnsyn også ville sikre pasienten innsyn i dette. Vi konfronterte ikke systemforvalteren med våre funn fra tidligere samme måned. Vi vet dermed ikke om det har vært endringer i rutiner mellom vårt innsyn og intervjuet, eller om avviket mellom vårt funn og informasjonen vi fikk i intervjuet for eksempel kan skyldes misforståelser eller manglende oversikt over detaljene i innsynsrutinene ved KAD.

Vi velger å utforme tiltak i henhold til funnene fra innsynsbegjæringen vår. Dersom Helseetaten har endret innsynsrutiner siden den gang, vil ikke tiltakene nødvendigvis være like aktuelle.

6.8.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 77

6.8.2.1 Logging av tilgang, endring og sletting

Slik som ved Normens krav nummer 127, er det også her nødvendig å innføre logging av tilgang, endring og sletting av meldingsboksen. Vi vil ikke beskrive hva dette tiltaket innebærer her, men henviser til kapittel «6.6.2.2. Logging av tilgang, endring og sletting». Årsaken til at dette tiltaket er nødvendig er at innsynet i dag ikke vil være komplett uten informasjon tilhørende meldingsboksen. Dette må derfor logges slik at informasjon om hvem som har hatt tilgang, endret eller slettet opplysninger i meldingsboksen vil være mulig å fremskaffe.

6.8.2.2 Generere opplysninger fra logg automatisk, i lesbart format (se 127)

Det andre tiltaket vi mener det er nødvendig å innføre, er generering av opplysninger fra logg automatisk, i et lesbart format. Også dette tiltaket er mer utdypet under kapittel «6.6.2.3. Generere opplysninger fra logg automatisk, i lesbart format». Årsaken til at tiltaket også vil kunne bidra til etterlevelse av krav nummer 77 er at vi anser det som viktig å minske arbeidsbelastningen ved innsynsbegjæringer. Det vil også da være enklere å utforme automatiserte svar på innsynsbegjæringer, noe vi anser som et realistisk fremtidig mål for Helseetaten.

6.9 Normens krav nummer 95

6.9.1 Om kravet og status i dag

6.9.1.1 Dokumenteres det alltid hvem det er gitt opplysninger til, og hvilken virksomhet denne tilhører?

For å sikre pasientens krav på konfidensialitet skal det som tidligere nevnt dokumenteres hvem som har hatt tilgang til vedkommendes helse- og personopplysninger.[159] Dette skal i noen tilfeller gjøres i form av automatisk loggføring,[160] som pasienten kan få innsyn i, eller det skal dokumenteres av helsepersonellet når de deler opplysninger, med hvem, hvor og når.[161]

6.9.1.2 Etterleves kravet i dag?

Det fremgår av kommunerevisjonens rapport at kravet om å alltid dokumentere hvem som har fått tilgang til helseopplysninger ikke følges i alle tilfeller. Som tidligere nevnt var det mangler i både tilgangsstyring og loggføring ved tilgang til meldingsboksen.[162] Oppslag i meldingene ble ikke loggført. Samtlige med tilgang til Profdoc Vision hadde tilgang til meldingene.[163] Hvem som fikk tilgang til helse- og personopplysninger i meldingsboksen ble altså ikke dokumentert.

I tillegg til dette fant kommunerevisjonen at det hendte at brukere benyttet hverandres brukerkontoer for å skaffe tilgang til journaler. Det fremgikk dermed ikke av loggen hvem som i virkeligheten fikk tilgang på opplysningene i slike tilfeller. Det sistnevnte eksemplet anser vi i større grad for å være et brudd på Normens krav nummer 127. Tiltak for å håndtere deling av brukerkontoer finnes i kapittel «6.6. Normens krav nummer 127.»

Da vi undersøkte dette kravet i april 2020 fikk vi vite at det ved utsendelse av meldinger fra meldingsboks manuelt skrives inn hvem som har fått hvilke opplysninger.[164] Slik det også fremgår av kapittelet om Normens krav nummer 127, vil ikke systemforvalteren uttale seg om det har blitt innført logging eller tilgangsstyring i meldingsboksen. Vi kan dermed ikke med sikkerhet si hvordan dette løses i dag. Vi velger derfor å legge siste sikre datagrunnlag til grunn, nemlig kommunerevisjonsrapporten fra 2017, og utformer tiltak deretter. Dersom logging og tilgangsstyring er etablert, vil kun tiltak nummer to, «Tjenestebasert adressering av meldinger» være relevant.

159 Pasientjournalloven § 25, helsepersonelloven § 45, pasientjournalforskriften § 14.
160 Pasientjournalforskriften § 14.
161 Pasientjournalloven § 45.
162 Meldingsboks: Se kapittel «6.6.1.2. Etterleves kravet i dag?».
163 Kommunerevisjonen (2017) s. 25.
164 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

6.9.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 95

6.9.2.1 Tjenestebasert adressering av meldinger (se 127)

Se tiltaket «Tjenestebasert adressering av meldinger» i kapittelet om Normens krav nummer 127.

6.9.2.2 Logging av tilgang, endring og sletting (se 127)

For å etterleve krav nummer 95 må Helseetaten dokumentere hvem som har sett hvilke opplysninger i meldingsboksen. De må også kunne dokumentere hvilken virksomhet personen tilhører. Vi anbefaler logging av tilgang, endring og sletting i meldingsboksen også her. Tiltaket er videre beskrevet under kapittel «6.6.2.2. Logging av tilgang, endring og sletting».

6.10 Normens krav nummer 203

6.10.1 Om kravet og status i dag

6.10.1.1 Kan loggene enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd?

Virksomheten (dataansvarlig) skal automatisk dokumentere enhver tilgjengeliggjøring av helse- og personopplysninger, jf. pasientjournalforskriften § 14 første ledd. I henhold til Normens krav nummer 203 skal tilgjengeliggjøringsloggene enkelt kunne analyseres ved hjelp av analyseverktøy for å kunne avdekke om noen urettmessig har hentet frem journalopplysninger.[165] Det utdypes ikke hva som menes med et «analyseverktøy», og vi legger derfor til grunn at et analyseverktøy som minimum må forstås som et digitalt hjelpemiddel som gjør gjennomgang og kontroll av logg mer effektivt enn manuell gjennomlesning eller kontroll. Verktøyet må utføre deler eller hele kontrollen selv, og er ikke bare en forenkling eller rutinespesifisering av manuell kontroll, slik vi forstår det. Hverken Helsedirektoratet eller Direktoratet for e-helse gir informasjon om, eller konkrete forslag eller eksempler på slike analyseverktøy, utover de generelle kravene fra Normen.

6.10.1.2 Etterleves kravet i dag?

Kommunerevisjonen omtaler ikke metoder eller verktøy for kontroll av logg i sin rapport fra 2017. De skriver at systemforvalter månedlig sjekket systemloggene for bruk av «blålysfunksjonen».[166] De skriver derimot ingenting om hvorvidt kontrollen ble utført manuelt eller ved hjelp av et analyseverktøy.[167]

165 Pasientjournalforskriften § 14 tredje ledd.

166 Blålysfunksjon: Se kapittel «4.1.3. Brukeradministrasjon».

167 Kommunerevisjonen (2017) s. 25.

I april 2020 svarer systemforvalteren i Helseetaten at de dessverre ikke har automatisk gjennomgang av logger, og at de kun har anledning til å gjennomføre manuell loggkontroll.[168]

Basert på dette svaret kan ikke Normens krav nummer 203 sies å være oppfylt.

6.10.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 203

6.10.2.1 Innføring av analyseverktøy som rutinemessig gjennomgår loggene

Slik det fremkommer ovenfor har ikke Helseetaten innført et automatisk analyseverktøy for å gjennomgå logg. Gjennomgang av logger er som tidligere nevnt viktig. Uten dette vil logging tilføre lite for å styrke informasjonssikkerheten. Sikkerhetslogger dokumenterer gjerne svært mye, og kontinuerlig. En manuell kontroll av så omfattende data vil være tidkrevende og lite treffsikkert. Manuelle kontroller av logger kan ha god effekt dersom man leter etter en konkret hendelse, eller dersom man vet at noe foregikk innenfor et gitt tidsrom. Manuelle kontroller vil derimot ikke være like effektive dersom man undersøker logger etter uspesifiserte trusler eller hendelser. Datamaskiner kan analysere store datamengder, kontinuerlig, og kan lete etter mønster og uregelmessigheter døgnet rundt.[169]

Bruken av analyseverktøy bør gjøres rutinemessig, for eksempel ved faste tidsintervaller, og det bør også gjøres ved mistanke om brudd på informasjonssikkerheten. Vi anbefaler Helseetaten å innføre et automatisk analyseverktøy for å forenkle gjennomgangen av logger.

NSM anbefaler at loggene føres i et standardisert format. På den måten kan det enkelt benyttes et tredjeparts analyseverktøy til å gjennomgå loggene.[170] Det finnes en rekke aktører som leverer analyseverktøy for gjennomgang av logg, og vi anbefaler at Helseetaten selv vurderer hvilke verktøy som vil passe deres behov best.

168 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.
169 Encyclopædia Britannica (Udatert).
170 Nasjonal sikkerhetsmyndighet (2020).

6.11 Normens krav nummer 204

6.11.1 Om kravet og status i dag

6.11.1.1 Er det etablert rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser?

Grunnlaget for Normens krav nummer 204 er det samme som for krav nummer 203, nemlig å avdekke urettmessige tilganger til helse- og personopplysninger. Krav nummer 203 omhandlet hvorvidt loggene i praksis enkelt kan analyseres, og om det er etablert verktøy for å dette. Krav nummer 204 kontrollerer om det er etablert rutiner for slik gjennomgang. Kravets ordlyd «[…] før de får alvorlige konsekvenser» skal forstås som at rutiner skal være på plass for jevnlig og hensiktsmessig gjennomgang av logg, og at slik gjennomgang ikke skal gjennomføres bare ved mistanke om brudd eller etter et brudd.

6.11.1.2 Etterleves kravet i dag?

Det fremkommer ikke av kommunerevisjonens rapport hvorvidt det konkret var etablert rutiner for analyse av logg for å oppdage hendelser før de fikk alvorlige konsekvenser. Kommunerevisjonen skriver at det ikke eksisterte rutiner for kontroll av sikkerhetsloggen, utover kontroll med bruken av blålysfunksjonen. Dette tyder på at rutiner i henhold til Normens krav nummer 204 ikke var etablert.

Da vi undersøkte dette i april 2020 svarte systemforvalteren ved Helseetaten at slike rutiner ikke var etablert.

Vi anser derfor ikke Normens krav nummer 204 for å være oppfylt.

6.11.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 204

6.11.2.1 Innføring av analyseverktøy som rutinemessig gjennomgår loggene (se 203)

Muligheten for å være i forkant og oppdage brudd før de får alvorlige konsekvenser er et viktig argument for å analysere loggene jevnlig. For å dekke dette kravet mener vi også her det bør innføres analyseverktøy som rutinemessig gjennomgår loggene. Se kapittel «6.10.2.1. Innføring av analyseverktøy som rutinemessig gjennomgår loggene» for en mer dyptgående beskrivelse av dette.

6.12 Normens krav nummer 206

6.12.1 Om kravet og status i dag

6.12.1.1 Et det etablert rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister?

Normens krav nummer 206 deler formål med både krav nummer 203 og 204. Formålet med kravene er å sørge for at virksomhetene har rutiner og verktøy på plass for å kunne avdekke urettmessig tilgang til helse- og personopplysninger, og dermed brudd på konfidensialiteten.

Den dataansvarlige skal holde oversikt over hvem som skal ha tilgang til hvilke opplysninger, altså et såkalt autorisasjonsregister.[171] Den dataansvarlige skal også i ettertid kunne kontrollere hvem som benyttet seg av tilgangen. En metode for slik kontroll er å sammenholde autorisasjonsregisteret (hvem som skal ha tilgang til hva), med loggene (hvem som faktisk har fått tilgang til hva).

Normens krav nummer 206 krever at det skal etableres rutiner for slik kontroll.

6.12.1.2 Etterleves kravet i dag?

Det fremkommer ikke av kommunerevisjonens rapport om autorisasjonsregisteret kan sammenholdes med loggene. Kommunerevisjonen fastslår at det ikke er etablert rutiner for kontroll av logg, utover kontroll av blålystilgangen. Kravet ble med andre ord ikke oppfylt på kontrolltidspunktet.

I april 2020 undersøkte vi det samme. Vi får beskjed om at det er praktisk mulig å sammenholde logger med autorisasjonsregister, men at det ikke er etablert rutiner for å gjøre dette.[172]

Normens krav nummer 206 er dermed ikke oppfylt.

6.12.2 Tiltak for å styrke etterlevelsen av Normens krav nummer 206

6.12.2.1 Sammenholde den automatiske kontrollen av loggen med autorisasjonsregisteret for å avdekke uautorisert tilgang

Vi anbefaler at Helseetaten får på plass rutiner for å sammenholde loggene med autorisasjonsregisteret, slik at Normens krav nummer 206 blir overholdt. En slik rutine vil gjøre at Helseetaten ved behov kan forsikre seg om at det bare er autoriserte brukere som har hatt tilgang til Profdoc Vision. Dersom brukere utover de som er registrert i autorisasjonsregisteret fremkommer av systemloggene, er

171 Jf. Pasientjournalforskriften § 13 tredje ledd.

172 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

dette et tegn på at det enten foreligger en feil i systemene, eller at noen som ikke skulle hatt tilgang allikevel har tilgang.

6.12.2.2 Innføring av analyseverktøy som rutinemessig gjennomgår loggene (se 203)

Vi anbefaler at kontrollen effektiviseres ved at tilgangsregisteret og systemloggene automatisk sammenholdes av et analyseverktøy. En slik automatisk kontroll vil kunne gjennomføres betydelig hyppigere enn hva en manuell kontroll av det samme kan. En manuell kontroll vil sannsynligvis være betydelig mer tidkrevende enn en automatisk kontroll, særlig fordi en automatisk kontroll ikke nødvendigvis binder opp menneskelige ressurser i selve kontrollprosessen.

7 Anbefaling og konklusjon

7.1 Avhandlingens fokus og funn

7.1.1 Fokus

I denne avhandlingen har vi undersøkt hvordan konfidensialiteten i pasientjournalsystemet Profdoc Vision ivaretas gjennom tilgangsstyring. Vi har kontrollert tilgangsstyringen etter kravene fastsatt i Normen, og vurdert hvorvidt Helseetatens pasientjournalsystem oppfylte kravene i 2016, og igjen i 2020.

Kommunerevisjonens rapport fra 2017 undersøkte ikke Profdoc Visions etterlevelse av Normens krav, men kontrollerte generell tilgangsstyring i løsningen. Vi har gjennom analyse av rapporten vurdert etterlevelsen av kravene slik den var i 2016, og avdekket manglene. Vi har videre kontrollert de samme kravene i 2020, og funnet ut at det fire år senere fortsatt er betydelige mangler i etterlevelsen. Videre vil vi presentere funnene og komme med forslag til endringer for å utbedre de gjenværende manglene, samt anbefalinger til hva Oslo kommune nå bør foreta seg.

7.1.2 Funn

I 2016 kontrollerte kommunerevisjonen tilgangsstyringen i Profdoc Vision. Den ble ikke vurdert etter Normens krav, på tross av at Normen er et rammeverk for informasjonssikkerhet i helsesektoren som har detaljerte krav til tilgangsstyring og konfidensialitet, og at Helseetaten gjennom sin tilknytning til Norsk helsenett forplikter seg å etterleve kravene her. Våren 2020 har vi gjennomgått kommunerevisjonsrapporten, og tilført den ny verdi i form av å holde deres funn opp mot avtalefestede krav i Normen.[173] Gjennom vår analyse av kommunerevisjonens rapport fra 2016 og Profdoc Visions daværende etterlevelse av Normen, vet vi at det i 2016 var minst 19 brudd på krav til konfidensialitet og tilgjengelighet. I tillegg var det 23 normkrav som ikke ble avdekket i rapporten, og hvor det dermed ikke foreligger tilstrekkelig data til å kunne konkludere med etterlevelse eller mislighold av kravene. Vi har utelukkende fokusert på tilgangsstyring og konfidensialitet i avhandlingen vår, og vi har derfor sortert vekk krav fra Normen som ikke direkte omhandler dette. Det er hele 294 krav, og vi har kontrollert 44 av dem. Vi kan ikke si noe om etterlevelsen av de resterende 250 kravene.

173 Norsk helsenett (Udatert B).

Våren 2020 gjennomførte vi en ny kontroll av de samme 44 kravene fra Normen, for å avdekke dagens etterlevelse. Gjennom våre undersøkelser har vi funnet at det per april 2020 er 16 underkjente normkrav i Profdoc Vision. Det er viktig å understreke at det ikke er slik at det kun er tre normkrav som har blitt utbedret siden 2016. Faktisk er det hele 8 krav som i 2016 var underkjent og som i 2020 har blitt godkjente.[174] Rapporten fra 2016 har naturligvis ikke kontrollert samtlige krav fra Normen, fordi dette ikke var rapportens opprinnelige hensikt. Det kan derfor tyde på at en del av kravene som i 2016 ikke ble kontrollert, ved kontroll viser seg å være underkjente nå i 2020.

Til tross for flere utbedringer siden 2016, er det våren 2020 fortsatt en rekke mangler i Profdoc Vision og Helseetatens etterlevelse av Normens krav. Se kapittel 5 og 6. Undersøkelsen avdekket også at Profdoc Vision ligger i kommunens driftsmiljø AKS (Arbeidsflater, Kontorstøtte og system), og at pålogging til Profdoc Vision i dette driftsmiljøet medfører tregheter. Dette var en av årsakene til at ansatte ved KAD benyttet hverandres brukerkontoer. Fordi AKS ikke er en del av Profdoc Vision, men snarere en driftsplattform som benyttes av hele kommunen, anså vi ikke utbedringer av dette for å være innenfor avhandlingens mandat. Likevel ønsker vi å nevne at kommunen bør se på muligheter for å øke hastigheten ved pålogging til Profdoc Vision på AKS-plattformen.

Manglende etterlevelse av Normens krav innebærer i de fleste av tilfellene også manglende etterlevelse av lovkrav.[175]

7.2 Konsekvenser

7.2.1 Konsekvenser for Helseetaten og Profdoc Vision

For Helseetaten og Profdoc Vision betyr manglende etterlevelse av Normens krav, og herunder også lovkrav, at de først og fremst ikke etterlever flere sentrale helserettslige bestemmelser, herunder blant annet helsepersonelloven § 16. Bestemmelsen sier at virksomheten er pålagt å legge til rette for at helsepersonellet som jobber der er i stand til å overholde sine plikter. Rett i overkant av 35 % av de kontrollerte tiltakene etterleves i 2020.[176] Følgelig er ikke Norsk helsenetts krav om etterlevelse av Normen oppfylt. Brudd på lovkrav kan blant annet føre til bøter fra Datatilsynet, straff etter *Lov om straff* (straffeloven) for brudd på

174 Se kapittel «5.5. Statistikk til tabell».

175 Direktoratet for e-helse. (2020 C).

176 16 godkjente krav i 2020, av totalt 45 kontrollerte krav. Se kapittel 5.

taushetsplikt,[177] samt erstatningsansvar for lovstridig behandling av helseopplysninger.[178]

7.2.2 Konsekvenser for pasienten

Konsekvensene av å ikke ha tilstrekkelig informasjonssikkerhet kan direkte ramme pasienten eller brukeren[179] som opplysningene omhandler,[180] og avsløring av helseforhold kan få store konsekvenser for pasienten det gjelder. For enkelte pasienter kan tilgjengeliggjøring av slike opplysninger avsløre hemmeligheter de for all del ikke ønsker å dele med andre enn den tiltenkte legen. For andre kan opplysninger på avveie medføre potensiell livsfare. De fleste av oss kan kjenne seg igjen i at vi på et punkt har delt noe med legen vår vi helst ikke vil at andre skal vite om. I noen tilfeller kan slike opplysninger være direkte skadelige i feil hender. Helserettsadvokat, jurist, og Førsteamanuensis ved UiO, Anne Kjersti Befring, fortalte i en forelesning høsten 2019 om et skremmende eksempel på sensitive pasientopplysninger på avveie. Hun fortalte en historie om en sak hun arbeidet med en gang, hvor en ung muslimsk kvinne hadde oppsøkte et sykehus. Skjult fra sin kontrollerende ektemann og familie fikk hun utført en abort. En stund etter aborten ble hun konfrontert av familiemedlemmer som hadde fått kjennskap til aborten, på tross av at jenta aldri hadde delt dette med noen andre enn helsepersonellet ved sykehuset. Spørsmålet om hvordan noen hadde fått vite om dette ble reist. Mye tyder på at årsaken var journalsnoking fra helsepersonell som kjente jentas familie.[181] Hvordan det gikk med jenta kjenner vi ikke til i dag. En mer effektiv tilgangsstyring og overholdelse av kravene til konfidensialitet kunne muligens forhindret dette. Vi understreker at dette *ikke* forekom ved KAD, Oslo legevakt eller i Profdoc Vision.

7.2.3 Konsekvenser for tilliten

Befolkningens tillit til helsevesenet er i fokus for helsevesenet, og er også innlemmet i formålsparagrafen i helsepersonelloven.[182] Tilliten bygger på en oppfatning av å motta trygge og riktige helsetjenester fra dyktig helsepersonell. Den bygger også på en oppfatning av at taushetsplikten, og i videre forstand konfidensialiteten, etterleves. Dersom en pasient opplever at svært private opplysninger havner på avveie, blir snoket i eller blir delt med uvedkommende, kan dette gå hardt utover pasientens tillit til helsevesenet. Dette kan føre til at vedkommende vegrer seg for å oppsøke helsehjelp senere. Et slikt tap av tillit kan også

177 Straffeloven § 209.

178 Pasientjournalloven kap. 5.

179 Med «bruker» mener vi brukere i henhold til definisjonen i pasient- og brukerrettighetsloven § 1-3 bokstav f.

180 Også omtalt som «de registrerte», jf. personvernforordningen art. 4(1).

181 Befring (2019).

182 Helsepersonelloven § 1.

spre seg i befolkningen. Tapt tillit til helsevesen og helsemyndigheter kan over tid kulminere i dårligere folkehelse. Våren 2020 har bevist hvor avgjørende tillit er for at befolkningen tar helsevesenets og helsemyndighetenes anbefalinger på alvor. Denne tilliten må helsevesenet kjempe for å opprettholde.

7.3 Plan for utbedring av underkjente krav

7.3.1 Vårt bidrag

I avhandlingen har vi kartlagt Profdoc Visions etterlevelse av 44 av Normens krav. Resultatet viser at det er mangler i etterlevelsen også i dag, fire år etter at flere av funnene først ble oppdaget. Vi har i denne avhandlingen presentert de viktigste manglene vi har avdekket, og hvilke tiltak vi mener Helseetaten bør vurdere for å etterleve Normen. Vi har gjennomført rent faglige vurderinger av mangler i etterlevelsen, men vi har ikke kartlagt Helseetatens muligheter til å bøte på manglene. Helseetaten må selv, eller i samråd med andre, avklare hvilke av våre tiltak som kan gjennomføres, innenfor de teknologiske og økonomiske rammene de befinner seg i.

7.3.2 Neste steg

Gjennom vår kartlegging av manglene i tilgangsstyring og konfidensialitet i Profdoc Vision, har vi lagt grunnlaget for videre utredninger. Først og fremst bør Helseetaten gjennomføre en verdivurdering, slik at de får en fullstendig oversikt over hvilke informasjonsverdier de sitter på. Deretter bør de gjennomføre en risikovurdering av Profdoc Vision, hvor de tar høyde for manglene vi her har avdekket, og eventuelle andre avvik vi ikke har kontrollert. De bør også avklare akseptabel risiko i systemet.[183] Et system som behandler store mengder svært sensitive personopplysninger bør etter vår mening ha lav akseptabel risiko. Vurderingene som fremkommer av verdi- og risikovurderingene skal danne grunnlag for en prioriteringsliste for implementering og utbedring av manglene. Helseetaten bør også undersøke hvilke av manglene som direkte eller indirekte medfører brudd på helse- og personvernlovgivning, og innlemme resultatet av vurderingen i prioriteringen av tiltak.

Oslo kommune planlegger bygging av en ny storbylegevakt på tomta til nåværende Aker sykehus, hvor blant annet KAD befinner seg i dag.[184] Vi mener at dette er en god anledning til å vurdere Profdoc Visions fremtid, i lys av funnene i denne avhandlingen. Er Profdoc Vision også fremtidens pasientjournalsystem?

183 Se kapittel «3.3.2. Risikoappetitt».

184 Oslo kommune (Udatert A).

Kan hende er omorganisering og flytting av legevakt en god anledning til å fornye pasientjournalsystemet som har eksistert siden 1995.[185]

En potensiell utskiftning av pasientjournalsystemet er en kostbar affære, og systemforvalteren forteller at de har fått prisanslag på nye pasientjournalsystemer, hvor kostnaden for systemet og overgangen til dette er ca. 20 millioner kroner.[186] Vi har ikke gjennomført vurderinger av kostnader kontra manglende etterlevelse av kravene i Normen, men vi har forståelse for at kostnader alltid vil spille en rolle når tiltak vurderes innført. Vi mener likevel at Oslo kommune bør prioritere å utbedre manglene vi har avdekket her. Flere av manglene er i våre øyne medvirkende til lovbrudd, og vil uansett bidra til unødig risiko for pasientens personvern og integritet. Et ønske om fortsatt tilkobling til Norsk helsenett bør også trekkes inn som vurderingsgrunnlag.

Oslo kommune og Helseetaten bør minst gjøre følgende:

A. Gjennomføre verdivurdering av helsedata og Profdoc Vision.
B. Gjennomføre risikovurdering av Profdoc Vision, hvor det tas høyde for funnene i denne avhandlingen. Andre kjente mangler eller svakheter må naturligvis også vurderes.
C. Vurdere lovmessigheten av systemet i lys av funnene i avhandlingen og andre kjente mangler.
D. Fastsette risikoappetitt.
E. Kartlegge muligheter for utbedring av funn i dagens system (Profdoc Vision).
F. Kartlegge kostnader ved utbedring av dagens system.
G. Kartlegge mulighetene for etterlevelse av Normens krav ved bruk av andre systemer.
H. Kartlegge kostnader og gevinster ved overgang til nytt system.

Oslo kommune og Helseetaten bør samlet sett vurdere om man ønsker å utbedre og beholde dagens system, eller om man heller skal satse på et nytt pasientjournalsystem. Vurderingen bør minst ta høyde for kostnader, lovkrav, risikoer og akseptabel risiko. Fordi Profdoc Visions grunnarkitektur allerede er 25 år gammel, bør kommunen vurdere om systemet som helhet er modent for utskiftning, eller om fortsatt bruk er et godt alternativ.

Ønskede gevinster av arbeidet må planlegges nøye, og det må jobbes kontinuerlig og målrettet med å oppnå dem. Kommunen bør også lage planer for å måle

185 Kommunerevisjonen (2017) s. 20.
186 Intervju med systemforvalter i Fagsystemavdelingen i Helseetaten, Oslo kommune. 27. april 2020.

gevinstoppnåelsen etter at prosjektet fullføres, slik at det kan avdekkes om ønskede mål har blitt nådd, og at gevinstene i prosjektet har blitt hentet ut. Uavhengig av om kommunen kommer frem til at utskiftning av systemet er rett valg, eller at dagens system kan utbedres såpass at det vil fungere en stund til, må fremdriften planlegges.

Vi håper at denne avhandlingen bidrar til at kommunen sørger for at konfidensialiteten til pasientene styrkes, og at de avdekke manglene ikke finnes om fire nye år.

Kildeliste

Litteratur:

Befring, Anne Kjersti og Bente Ohnstad. *Helsepersonelloven Kommentarutgave.* 1. utg., Bergen: Fagbokforlaget, 2019.

Duvaland, Lars. «Taushetsplikt» i *Sentrale helserettslige emner.* Aslak Syse red., 1. utg., Oslo: Gyldendal Juridisk. 2016, s.135-166.

Engelshiøn, Sverre og Elisabeth Vigerust. *Pasientjournalloven og helseregisterloven kommentarutgave*. Oslo. Universitetsforlaget. 2015

Jacobsen, Dag Ingvar: Hvordan gjennomføre undersøkelser? 3. utg, Oslo. Cappelen Damm Akademisk 2015

Nettsider:

Altinn «Sikkerhetsnivå» Udatert [hentet 23.05.2020].

Aven, Terje. «Risikoappetitt» 2019 https://snl.no/risikoappetitt [Hentet 24.03.2020].

Bratbergsengen, Kjell. «Database» 2019 https://snl.no/database [Hentet 14.05.2020].

Braut, Geir Sverre. «e-helse» 2019 https://sml.snl.no/e-helse [Hentet 09.05.2020]

Braut, Geir Sverre. «Epikrise» 2020 https://sml.snl.no/epikrise [Hentet 10.03.2020].

CGM. «Our History: Pioneer of intelligent IT in the healthcare sector" Udatert https://www.cgm.com/corp/ueber_uns_1/auf_einen_blick/historie/historie.en.jsp [Hentet 09.05.2020]

Datatilsynet «Risikovurdering» (2019) https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/ [13.05.2020].

Datatilsynet. «Innebygget personvern» 2018 https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/ [Hentet 23.05.2020].

Datatilsynet. «Når er det krav om sterkere autentisering (for eksempel to-faktor) enn bare brukernavn og passord?» Udatert https://www.datatilsynet.no/regelverk-og-verktoy/sporsmal-svar/Informasjonssikkerhet-hos-virksomheter/nar-er-det-krav-om-sterkere-autentisering/ [Hentet 08.05.2020].

Digitaliseringsdirektoratet. «Begrepsliste: Informasjonssikkerhet» Udatert https://internkontroll-infosikkerhet.difi.no/begrepsliste-informasjonssikkerhet [Hentet 10.03.2020].

Digitaliseringsdirektoratet. «Styringsdokument» 2019 https://www.prosjektveiviseren.no/dokumentasjon/ledelsesprodukter/styringsdokument [Hentet 18.03.2020].

Direktoratet for e-helse (2020 C) https://ehelse.no/standarder/om-standardisering-i-e-helse/tjenestebasert-adressering [13.05.2020].

Direktoratet for e-helse. «Normen - Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren» 2020 B https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren [Hentet 18.03.2020].

Direktoratet for e-helse. «Om Normen» 2020 A https://ehelse.no/normen/om-normen#Versjonshistorikk%20Normen [Hentet 18.03.2020].

Direktoratet for e-helse. «Tilleggsdokumenter (Oversikt over Normens krav, CCM og ISO27001-mapping)» 2020 C https://ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#Tilleggsdokumenter%20(Oversikt%20over%20Normens%20krav%2C%20CCM%20og%20ISO27001-mapping) [hentet 09.05.2020].

Encyclopædia Britannica. «Information system infrastructure and architecture» 2017 https://www.britannica.com/topic/information-system/Information-system-infrastructure-and-architecture [Hentet 23.05.2020].

Encyclopædia Britannica. «Pattern recognition» Udatert https://www.britannica.com/technology/pattern-recognition-computer-science [Hentet 16.05.2020].

Helse- og omsorgsdepartementet «elektronisk pasientjournal» 2016 https://www.regjeringen.no/no/tema/helse-og-omsorg/e-helse/innsikt/elektronisk-pasientjournal/id2480061/ [Hentet 01.04.2020].

Helsedirektoratet. «Legevakt» 2019 https://helsenorge.no/hjelpetilbud-i-kommunen/legevakt [Hentet 13.03.2020].

Hoff, Bente. «Logging - Du må vite hva som skjer og hva som har skjedd» 2017 https://www.nsm.stat.no/blogg/logging---du-ma-vite-hva-som-skjer/ [Hentet 15.05.2020].

Holck, Per. «Hippokratiske ed» 2020 https://sml.snl.no/hippokratiske_ed [Hentet 22.05.2020].

Information and Privacy Commissioner/Ontario Canada. «Privacy-Enhancing Technologies: The Path to Anonymity Volume 1» 1995 http://www.ontla.on.ca/library/repository/mon/10000/184530.pdf [Hentet 03.05.2020].

Johansen, Lars T, June Beathe Høgsve Iversen og Lise Broen. «Planlagt hjemmefødsel og forsvarlig helsehjelp» 2017 https://tidsskriftet.no/2017/05/helse-og-jus/planlagt-hjemmefodsel-og-forsvarlig-helsehjelp [Hentet 22.05.2020].

Kanestrøm, Jorunn. «Ikke god nok pasientkontroll» 2010 https://forskning.no/helsepolitikk-universitetet-i-oslo-partner/ikke-god-nok-pasientkontroll/814435 [Hentet 09.05.2020].

Knudsen, Egil. «Tjeneste lar deg sjekke om passordet ditt har lekket på nettet» 2017 https://www.tek.no/nyheter/nyhet/i/RRE3or/tjeneste-lar-deg-sjekke-om-passordet-ditt-har-lekket-pa-nettet [Hentet 08.05.2020].

Kommunerevisjonen «Informasjonssikkerhet personopplysninger» 2017 https://www.oslo.kommune.no/getfile.php/13205600-1490092019/Tjenester%20og%20tilbud/Politikk%20og%20administrasjon/Budsjett%2C%20regnskap%20og%20rapportering/Rapporter%20fra%20Kommunerevisjonen/Rapporter%20fra%20Kommunerevisjonen%202017/04-2017%20Informasjonssikkerhet%20personopplysninger.pdf [Hentet 31.03.2020]

Monsrud, Marius. «69 600 per innbygger til helse» 2020. https://www.ssb.no/nasjonalregnskap-og-konjunkturer/artikler-og-publikasjoner/69-600-per-innbygger-til-helse [Hentet 22.05.2020].

Nasjonal sikkerhetsmyndighet «Ny versjon av NSMs Grunnprinsipper for IKT-sikkerhet klar» 2020 https://www.nsm.stat.no/aktuelt/grunnprinsipper-for-ikt-sikkerhet-2.0/ [Hentet 15.05.2020].

Nasjonal sikkerhetsmyndighet. «Passordanbefalinger fra Nasjonal sikkerhetsmyndighet» 2018 https://www.nsm.stat.no/aktuelt/passordanbefalinger-fra-nasjonal-sikkerhetsmyndighet/ [Hentet 27.05.2020].

Norsk helsenett. «Helsenettet» Udatert A https://www.nhn.no/helsenettet/ [Hentet 14.05.2020].

Norsk helsenett. «Må vi følge Normen?» Udatert B https://www.nhn.no/maa-vi-foelge-normen/ [Hentet 14.05.2020].

NRK. «Helse Sør-Øst: Innrømmer at utenlandske IT-arbeidere fikk tilgang til sensitive pasientdata» 2017 https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443 [Hentet 18.03.2020].

NRK. «Pasientsystem fremdeles stengt etter datainnbrudd på sykehus» 2018 https://www.nrk.no/osloogviken/pasientsystem-fremdeles-stengt-etter-datainnbrudd-pa-sykehus-1.13879494 [Hentet 18.03.2020].

Nätt, Tom Heine. «Autentisering» 2019 B https://snl.no/autentisering [Hentet 11.03.2020].

Nätt, Tom Heine. «Tilgangskontroll – informasjonssikkerhet» 2019 A https://snl.no/tilgangskontroll_-_informasjonssikkerhet [Hentet 10.03.2020].

Oslo kommune. «Kommunal akutt døgnvakt» 2020 https://www.oslo.kommune.no/helse-og-omsorg/helsehjelp/kommunal-akutt-dognenhet-kad/ [Hentet 18.03.2020].

Oslo kommune. «Legg inn på AKER KAD på 1-2-3» 2018 https://www.oslo.kommune.no/getfile.php/13313306-1549545685/Tjenester%20og%20tilbud/Helse%20og%20omsorg/Helsehjelp/R%C3%A5dgivning%2C%20sentre%2C%20ombud/Kommunal%20akutt%20d%C3%B8gnenhet%20%28KAD%29/Legg%20inn%20i%20KAD%20p%C3%A5%201-2-3%20oppdatert%2028.11.18.pdf [Hentet 18.03.2020].

Oslo kommune. «Ny storbylegevakt» Udatert A https://www.oslo.kommune.no/slik-bygger-vi-oslo/ny-storbylegevakt/ [Hentet 20.05.2020].

Oslo kommune. «Kommunerevisjonen» Udatert B https://www.oslo.kommune.no/etater-foretak-og-ombud/kommunerevisjonen/ [Hentet 29.05.2020].

Rossen, Eirik. «Skript – IT» 2019 https://snl.no/skript_-_IT [Hentet 27.05.2020].

Statistisk sentralbyrå. «Allmennlegetjenesten.» 2020 A https://www.ssb.no/statbank/sq/10033326 [Hentet 17.03.2020].

Statistisk sentralbyrå. «Allmennlegetjenesten» 2019 https://www.ssb.no/helse/statistikker/fastlegetj/aar [Hentet 11.03.2020].

Statistisk sentralbyrå. «Befolkning.» 2020 B https://www.ssb.no/statbank/sq/10033327 [Hentet 17.03.2020].

Statistisk sentralbyrå. «Befolkningen» 2020 C https://www.ssb.no/befolkning/faktaside/befolkningen [Hentet 11.03.2020].

Annet:

Befring, Anne Kjersti. Forelesning i Helserett (JUS5550). Oslo, 16. september 2019.

Direktoratet for ehelse. «Veileder for tilgangsstyring» 2017 https://ehelse.no/normen/veiledere/veileder-tilgangsstyring/_/attachment/download/9dd715c4-f26f-4cc7-9921-0e404546b3b0:de2f3d16084ba2b9cfffd2b04acc54e74ce58776/Veileder%20for%20tilgangsstyring.pdf [Hentet 16.03.2019].

Nasjonal sikkerhetsmyndighet. «Podcast - Når skal vi egentlig bytte passord?» [Podcast], (2019) https://www.nsm.stat.no/blogg/podcast---nar-skal-vi-egentlig-bytte-passord/ [Hentet 08.05.2020].

Lov- og forarbeidsregister:

2019 Lov 10. april 2019 nr. 11 Lov om helsepersonell m.v. (helsepersonelloven) [hpl].

2019 For 3. mars 2019 nr. 168 Forskrift om pasientjournal (pasientjournalforskriften).

2014 Lov 20. juni 2014 nr. 43 Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) [hregl].

2014 Lov 20. juni 2014 nr. 42 Lov om behandling av helseopplysninger ved ytelse av helsehjelp (pasientjournalloven).

2013 Forskrift 20. mars 2013 nr. 231 Forskrift om krav til og organisering av kommunal legevaktordning, ambulansetjeneste, medisinsk nødmeldetjeneste mv. (akuttmedisinforskriften)

2011 Lov 24. juni 2011 nr. 30 Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven).

2005 Lov 20. mai 2005 nr. 28 Lov om straff (straffeloven) [strl.].

1999 Lov 2. juli 1999 nr. 63 Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven).

For (EU) 2016/679) EUROPAPARLAMENTS- OG RÅDSFORORDNING (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [PVF, GDPR].

1967 Lov 10. februar 1967 Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven) [fvl].

Domsregister

HR-2013-2333-A (Narkotikapose-dommen).

Vedlegg

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
1.	69	Sørger virksomheten for at alt personell som gis tilgang til helse- og personopplysninger og annen informasjon underlagt taushetsplikt, er kjent med taushetsplikten?	Dette fremkommer ikke av rapporten. Det nevnes kun at CGM-ansatte (3 stykker) har signert taushetserklæring.
2.	127	Sikres det at bare autorisert personell med tjenstlige behov får tilgang til helse- og personopplysninger?	Informasjon i elektroniske meldinger var tilgjengelig for alle, uavhengig av brukergruppe. Oppslag i disse ble ikke logget.
3.	71	Behandles brudd på taushetsplikten som avvik?	Dette fremkommer ikke av rapporten.
4.	77	Sikrer innsynet også loggen over hvem, og eventuelt fra hvilken virksomhet, som har tilegnet seg hvilke opplysninger, på hvilket tidspunkt?	Nei. Det fremkommer ikke av rapporten om dette vil inngå i innsynet. Det kan ikke genereres automatiske rapporter. Loggen viser bare hvem som logget på systemet, og hvilken journal de tittet i, når. Avdeling/virksomhet fremkommer ikke.
5.	95	Dokumenteres det alltid hvem det er gitt opplysninger til, og hvilken virksomhet denne tilhører?	Nei. Logg viser ikke tilgang til meldinger. Det fremkommer ikke at dette dokumenteres andre steder.
6.	103	Oppbevares opplysninger om hvem som har hatt tilgang til eller fått utlevert helseopplysninger som er knyttet til pasientens eller brukerens navn eller fødselsnummer (logger) til det av hensyn til helsehjelpens karakter ikke lenger antas å bli bruk for dem?	Dette fremkommer ikke av rapporten.
7.	96	Gir helsepersonell tilgang til nødvendige og relevante helseopplysninger til samarbeidende personell i den grad dette er nødvendig for å kunne gi helsehjelp til pasienten på forsvarlig måte, med mindre pasienten eller brukeren motsetter seg det?	Dette fremkommer ikke av rapporten.
8.	113	Innhenter virksomheten taushetserklæring for den enkelte medarbeider?	Dette fremkommer ikke av rapporten.

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
9.	115	Har virksomheten etablert tiltak som ivaretar at alle som gis tilgang til informasjonssystemer og tilhørende informasjon, har tilstrekkelig kompetanse til å benytte systemene og til å ivareta informasjonssikkerheten og personvernet til den registrerte?	Dette fremkommer ikke av rapporten.
10.	118	Leveres alle medier (herunder digitalt, papir, osv.) som kan inneholde helse- og personopplysninger når et arbeidsforhold opphører?	Dette fremkommer ikke av rapporten.
11.	119	Leveres adgangskort tilbake og deaktiveres ved opphør i arbeidsforhold?	Dette fremkommer ikke av rapporten.
12.	120	Sperres all tilgang ved opphør i arbeidsforhold?	Tilbaketrekking av tilganger (herunder sletting av brukere) er ikke knyttet til arbeidsforhold. Det kjøres et skript hver måned som deaktiverer brukere som har vært inaktive i 6 måneder. Det tar med andre ord 6 hele måneder å fjerne brukere som ikke lenger skal ha tilgang.
13.	125	Er tilgangsstyring etablert for alle informasjonssystemer?	Nei. Det er ikke god nok tilgangsstyring i Profdoc Vision
14.	150	Bekrefter den autoriserte sin identitet på en sikker måte?	Tilgang til Profdoc Vision ble oppnådd ved pålogging til kommunens driftsplattform AKS for dem som var autoriserte brukere av Profdoc Vision («singel sign on») I tillegg var det mulig å logge inn med en tofaktorautentisering med ID-kort med passord og innlogging på kommunens driftsplattform. Når medarbeiderne var innlogget på kommunens driftsplattform, var det i tillegg en mulighet for å logge seg inn på Profdoc Vision med eget brukernavn og passord.

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
15.	128	Gis tilgang til behandlingsrettede helseregistre etter en konkret beslutning basert på at det er iverksatt eller skal iverksettes tiltak for medisinsk behandling av pasienten?	Nye brukere skal godkjennes av vaktkoordinator. Hvilke vurderinger de gjør seg fremkommer ikke.
16.	132	Vurderes autorisasjonen på nytt når det oppstår endringer i ansvarsområder eller ansettelsesforhold eller langvarig fravær?	Ingenting i rapporten tilsier at dette gjøres. Skript kjøres for å finne inaktive brukere.
17.	134	Er autorisasjonen for tilgang til behandlingsrettede helseregister tidsbegrenset?	Nei. Det er knyttet til aktivitet (mangel på inaktivitet), ikke tid, så vidt vi kan se fra rapporten.
18.	135	Angir autorisasjonen for tilgang til behandlingsrettede helseregister hvilke virksomheter autorisasjonen omfatter?	Nei. Alle har tilgang til alle avdelinger, med unntak av overgrepsmottaket.
19.	136	Er det etablert tiltak slik at mulig misbruk av autorisert teknisk personell, med særskilt behov for tilgang til større mengder helse- og personopplysninger, skal kunne avdekkes?	Nei. Logging følges ikke opp, med unntak av blålystilgang.
20.	137	Grunngis og registreres bruk av selvautorisering?	Ja.
21.	160	Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang? Eksempler på sikkerhetskrav: Behandlingsrettet helseregister må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	Nei. Det skulle bli gjennomført kontroller, men dette har ikke fungert på en god måte. Mer fremkommer ikke av rapporten.
22.	138	Er det etablert tekniske tiltak slik at personer i eller utenfor virksomheten ikke skal kunne endre opplysninger uten at det registreres i informasjonssystemene hvem som har endret og hva som er endret? Eksempler på sikkerhetskrav der det ikke benyttes PKI: Passordfil skal krypteres	Dette fremkommer ikke av rapporten.

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
23.	139	Registreres all tildeling av autorisasjon i et autorisasjonsregister?	Det arkiveres hos vaktkoordinator, sier etaten i rapporten. Tilsynet så ikke disse skjemaene.
24.	122	Har virksomheten rutiner for autorisering, endring og avslutning av tilganger?	Vaktkoordinator oppretter tilgangene. Rapporten sier ingenting om hvem som senere kan endre tilgangene. Blant annet skal et autorisasjonsskjema utfylles, og tilgang gis av vaktkoordinatorene ved avdeling Aker. Brukere må også først være registrert i PRK. Rutiner for skjemaet blir ikke fulgt. Andre rutiner fremkommer ikke i rapporten.
25.	141	Benytter bruker med administratortilganger personlig separat brukerkonto for administratoroppgaver?	Dette fremgår ikke av rapporten.
26.	145	Har virksomheten sørget for at det opprettes et autorisasjonsregister som minimum inneholde: 1. informasjon om hvem som er tildelt autorisasjon 2. til hvilken rolle autorisasjonen er tildelt (om rolle benyttes i virksomheten) 3. formålet med autorisasjonen 4. tidspunkt for når autorisasjonen ble gitt og eventuelt tilbakekalt 5. informasjon om hvilken virksomhet den autoriserte er knyttet til 6. helsepersonells autorisasjon for tilgang til helseopplysninger i annen virksomhet (kun om tilgang til helseopplysninger i annen virksomhet er tatt i bruk)	Nei. Vaktkoordinator ved avdeling Aker oppbevarer et autorisasjonsskjema for hver bruker. Skjemaet inneholder informasjon om hvem som har fått tildelt autorisasjon, men ingenting om rollen eller formålet med autorisasjonen. Det fremkommer ikke av revisjonsrapporten om tidspunkt for tilbaketrekking av autorisasjon fremkommer i autorisasjonsskjemaet, og heller ingenting om hvilke virksomheter de skal få tilgang til.
27.	147	Har virksomheten oversikt over tilgjengeliggjøring av opplysninger til andre virksomheter?	Ja, hvilke virksomheter som har tilgang. Ikke hvem i virksomhetene som har tilgang

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
28.	149	Har dataansvarlig og virksomhetene som gis tilgang til opplysninger hos dataansvarlig avklart gjennom avtale eller på annen måte: 1. hvordan autentisering skal foregå på en sikker måte 2. hvordan autorisering til helseopplysninger hos dataansvarlig skal foregå 3. hvordan logging og oppfølging av logger skal foregå	Dette fremkommer ikke av rapporten.
29.	151	Besluttes sikker måte på grunnlag av en risikovurdering?	Nei. Ikke gjennomført risikovurdering for det enkelte informasjonssystem, og ikke gjennomført overordnede risikovurderinger av Profdoc Vision i det hele tatt.
30.	153	Sikres det at flere personer ikke benytter samme autentiseringskriteria?	Nei, kolleger benytter hverandres brukerkontoer og datamaskiner til registrering av opplysninger. Årsaken er at det tar for lang tid å logge ut og inn igjen på egen konto. Det fremkommer ikke at slike rutiner er på plass.
31.	154	Tildeles autentiseringskriteria (som brukernavn og passord) på en betryggende måte?	Dette fremkommer ikke av rapporten.
32.	155	Sikres tilgang fra hjemmekontor og/eller mobilt utstyr (og mobilnettverk) ved sikker autentiseringsløsning?	Dette fremkommer ikke av rapporten.
33.	159	Gis det ved behov ny autentisering ved bytte av rolle (om roller benyttes)?	Dette fremkommer ikke av rapporten.
34.	160	Påser virksomhetens ledelse at det jevnlig gjennomføres kontroll av hvem som har hatt elektronisk tilgang? Eksempler på sikkerhetskrav: Behandlingsrettet helseregister må ha funksjonalitet slik at kontrollen kan gjennomføres effektivt.	Nei, brukere må autentiseres for å få tilgang til systemet, det er elektroniske logger på plass, men det er ingen rutiner på plass for kontroll av disse.

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
35.	161	Foretar den enkelte leder gjennomgang og kontroll av tilgangsstyring, herunder tildelte autorisasjoner: 1. Ved organisasjonsendringer, overflytting av personell til annen enhet/avdeling eller endring av arbeidsområde? 2. Minimum årlig (gjerne i forbindelse med sikkerhetsrevisjon)? 3. Ved sikkerhetsbrudd for det informasjonsområdet som blir berørt av bruddet?	Dette fremkommer ikke av rapporten.
36.	162	Varles virksomhetens ledelse dersom kontrollen fører til mistanke om at det har skjedd en urettmessig tilgang?	Nei, Helseetaten hadde ikke etablert skriftlige rutiner for å melde hendelser eller avvik. Avvik i Profdoc Vision ble ikke meldt.
37.	163	Dersom kontrollen viser at det har skjedd en urettmessig tilgang, behandles det som et avvik?	Nei. Manglende rutiner for avvik.
38.	164	Følges misbruk av selvautorisering opp som avvik?	Dette fremkommer ikke av rapporten.
39.	170	Er det etablert rutine for administrasjon av nøkler/adgangskort i adgangskontrollsystemet?	Dette fremkommer ikke av rapporten.
40.	201	Registreres som minimum følgende i loggene ved autorisert bruk av behandlingsrettet helseregister: 1. Identitet til den som har lest, rettet, registrert, endret og/eller slettet helse- og personopplysninger 2. Organisatorisk tilhørighet 3. Grunnlaget for tilgjengeliggjøringen 4. Tidsperioden for tilgjengeliggjøringen	I loggene føres det kun oversikt over hvem som logger seg inn og ut av Profdoc Vision, tidspunktet for dette, samt hvilke pasientjournaler de ser på. I tillegg logges bruk av blålystilgang. Grunnlag for tilgjengeliggjøring samt hva som er endret eller slettet logges ikke.
41.	203	Kan loggene enkelt kunne analyseres ved hjelp av analyseverktøy med henblikk på å oppdage brudd?	Dette fremkommer ikke av rapporten.
42.	204	Er det etablert rutiner for å analysere loggene slik at hendelser oppdages før de får alvorlige konsekvenser?	Nei.

Nr.	Normens nr.	Krav fra Normen	Kommunerevisjonens etterlevelse
43.	206	Et det etablert rutiner for ved behov å kunne sammenholde loggene med autorisasjonsregister?	Det fremkommer ikke av revisjons-rapporten hvorvidt disse loggene kan sammenholdes med autorisasjons-registeret.
44.	209	Lagres logger, som genereres ved ytelse av helsehjelp, til det ikke antas å være bruk for dem?	Det fremkommer ikke av rapporten.