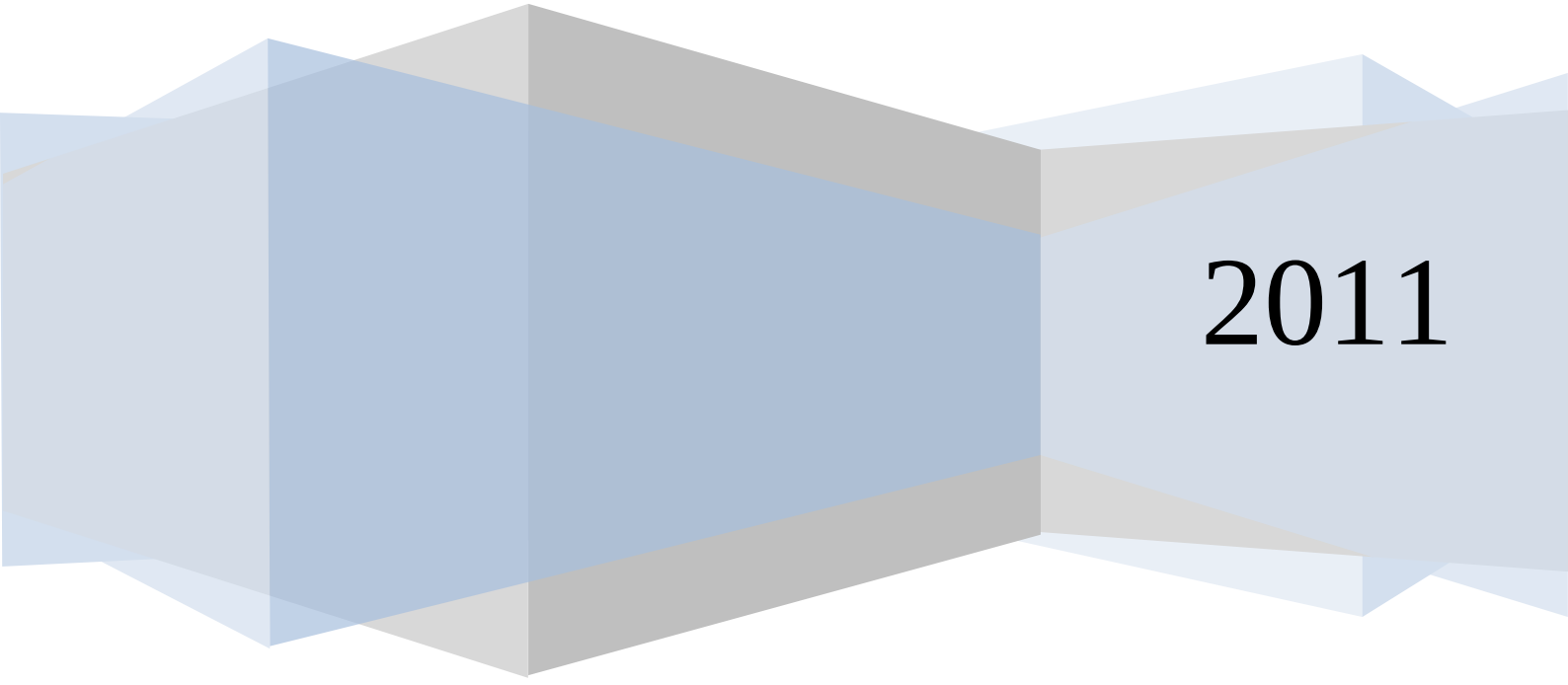
Universitetet i Stavanger

Hva skjer med journalen min?

Hvilke faktorer er det som bidrar til, eller hindrer en sikker behandling av sensitive opplysninger i kommunen?

Jan-Kåre Ruud



2011

FORORD

Denne masteroppgaven betyr slutten på fire års deltidsstudie i samfunnssikkerhet ved Universitet i Stavanger. Studiet har vært både lærerikt og interessant og jeg vil rette en takk til både lærere og medstudenter for en flott tid.

En spesiell takk til alle informantene for at de i en hektisk hverdag tok seg tid til å bli intervjuet. Uten dem hadde grunnlaget for oppgaven falt bort. En spesiell takk også til min veileder førsteamanuensis Ole Andreas Engen for god og grundig veiledning under hele arbeidet med masteroppgaven.

Jeg ønsker også å takke min arbeidsgiver Randaberg kommune som lot meg få mulighet til å gjennomføre studie, ved at jeg fikk permisjon til å delta på forelesninger og økonomisk støtte til studieavgift og litratur.

Stavanger 12. juni 2011

Jan-Kåre Ruud

Innholdsfortegnelse

1 Sammendrag

Få områder har hatt en så hurtig utvikling som elektronisk databehandling (IKT). For 30 år siden var data for de fleste et ukjent begrep og svært få hadde kunnskap om hva det innebar. I dag kan en ikke tenke seg et moderne samfunn uten IKT.
I begynnelsen av 1980 tallet begynte en gradvis å innføre IKT i kommunene. Dette skjedde først og fremst innefor merkantile oppgaver. Senere ble det utviklet programmer for bruk innenfor forskjellige fagområder som økonomi, personal, helse og sosialtjenesten m.m. I dag vil en finne egne program innefor de fleste områdene. Innføringen av IKT skjedde i de fleste kommunene i løpet av noen få år.
Innføring av IKT medførte et helt nytt risikobilde. Det som tidligere lå nedlåst i arkivskap var nå på harddisker som mange ikke forsto hva var. En opplevde at opplysninger ble slettet, at en ikke fant dem igjen, eller at de kom på avveie. Bruken av IKT i kommunene øker kraftig. Dette stiller store krav til sikkerhet, og spørsmålet blir da:
Kan vi som innbygger være sikre på at kommunen forvalter sensitive opplysninger på en sikker måte?
Hvilke rutiner og sikkerhetssystemer har kommunene etablert for at personvernet skal bli ivaretatt?
Hvilke faktorer er det som bidrar til, eller hindrer en sikker behandling av sensitive opplysninger i kommunen?

For å undersøke dette ble det gjennomført en kvalitativ undersøkelse med intervju av åtte personer fordelt på fire kommuner. Alle jobber daglig med sensitive opplysninger i helse- og omsorgstjenesten.

Det som var mest påfallende var mangel på rutiner. Det fantes noen rutiner, men for alle kommunene manglet det et en overordnet beskrivelse av hvordan personvernet skulle ivaretas. Flere påpekte at de hadde mange rutiner, men de var ikke nedskrevet.
Det funnet som var mest alvorig var mangel på kontroll av de opplysninger som legges inn om den enkelte pasient. I dag foregår dokumentasjon elektronisk. Det var ingen av kommunene som hadde rutiner for å kontrollere at opplysningene som lå inne i fagprogrammene var korrekte. Dette til tross for at alle hadde opplevd at opplysinger manglet, eller var lagt inn på feil person.

I tillegg kom det fram at det i liten grad ble meldt fra om avvik når det ble oppdaget feil. De feil som oppsto ble løst der og da. De fleste hadde avvikssystemer, men disse ble lite brukt i forhold til data og personvern.

Det kom også fram mangelfull opplæring av de som skulle benytte programmene. I alle kommunene fikk de ansatte tilgang uten at de hadde gjennomgått noe formell opplæring eller avlagt noe test på at de har nødvendig kunnskap. Alle kommunene hadde en form for opplæringsvakter hvor bruk av fagprogram inngår, men som en sa: ”Hvor god den opplæringen er, avhenger av hvor dyktig den som skal lære bort er”.

Konklusjon:
Svarene var stort sett like i alle kommunene. I de tilsyn som Datatilsynet har foretatt i kommunene kommer det fram mye av det samme. Det mangler mye på at den behandlingen som foretas av personopplysninger i norske kommuner er forsvarlig.

2 Innledning

2.1 Bakgrunn for oppgaven

Få områder har hatt en så hurtig utvikling som elektronisk databehandling (IKT). For 30 år siden var data for de fleste et ukjent begrep, og svært få hadde kunnskap om hva det innebar. I dag kan en ikke tenke seg et moderne samfunn uten IKT. Alle må på en eller annen måte forholde seg til datateknologi, enten ved bruk av PC, internett eller bankkort.
"Den oppvoksne generasjonen er ikke født med ski på beina. De er født med mobiltelefon i lomma og hendene på tastaturet" (Aune, 2007 s. 11)

I begynnelsen av 1980 tallet begynte en gradvis å innføre IKT i kommunene. Dette skjedde først og fremst innefor merkantile oppgaver, og PC'en ble av mange sett på som en avansert skrivemaskin.

Senere ble det utviklet programmer for bruk innenfor forskjellige fagområder som økonomi, personal, helse og sosialtjenesten m.m. I dag vil en finne egne program innefor de fleste områdene. Innføringen av IKT skjedde i de fleste kommunene i løpet av noen få år.

Mange opplevde at innføring av data som meningsløst. Deres jobb var å ta seg av brukerne, ikke sitte foran en datamaskin. Ansatte som både gjennom utdannelse og arbeidserfaring hadde bygget opp en god kompetanse innenfor sitt fagfelt måtte igjen på skolebenken. Flere klarte heller ikke å se noe gevinst i at alt nå skulle legges inn i dataprogram. De gamle systemene med å skrive rapporter og personopplysninger i permer og Kartex fungerte bra nok. Hvorfor endre på det?

Ved innføring av IKT fikk kommunene en ny utgiftspost. IKT utstyr var dyrt i innkjøp å krevde ansatte med kompetanse innefor data. IT-avdelingene i kommunene vokste fort ettersom bruken av data økte. Nye programmer ble kjøpt inn som igjen krevde mer og nye utstyr og kompetanse hos de ansatte. I dag brukes det store beløp på IKT i kommunene.

2.2 Nytt risikobilde

Innføring av IKT medførte et helt nytt risikobilde. Det som tidligere lå nedlåst i arkivskap var nå på harddisker som mange ikke forsto hva var. En opplevde at opplysninger ble slettet, at en

ikke fant dem igjen eller at de kom på avveie. De fleste feilene har ikke store konsekvenser, men det er dessverre også unntak. I 2004 døde en person i Horten kommune. Dødsfallet ble knyttet opp til at kommunens hadde innført nytt pleie og omsorgssystem og derfor ikke fikk hjelp fordi opplysninger var slettet ved en feil. (Denne hendelsen er beskrevet nærmere i kapittel om personvern i Norge.)

I mars 2008 fant en tilfeldig forbipasserende en minnepenn på en parkeringsplass utenfor et kjøpesenter. Da han puttet den inn i sin egen PC oppdaget han 20 filer fra psykologisk pedagogisk-tjeneste (PPT) som i følge www.bt.no inneholdt følgende opplysninger: Dokumenter fra PPT-tjenesten om interne arbeidsforhold. Utredninger av enkeltelever og vurderinger av deres evner og problemer. Et dokument med navn på 107 barn og åtte voksne personer som står i kø for å få hjelp av PPT. Blant de 107 navngitte barna var det detaljerte beskrivelser av hvilke personlige problemer de hadde og hvilke problemer de hadde i hjemmet. Listen ga innblikk i barns lærevansker, foreldre med psykiske problemer og beskrivelser av barnas faglige og sosiale evner. Flere av rapportene visste utredninger av enkeltelever som innehold informasjon om hvordan elevene klarer seg i en test. Konklusjonen for en elev viser at han ligger så langt etter den normale utviklingen at han betegnes som lettere tilbakestående. I en annen rapport, nevnes en persons tidligere alvorlige sykdomshistorie.
(www.bt.no 11.mars 2008)

Personen som fant minnepennen leverte den videre til Bergens Tidende. Saken medførte stort presseoppslag og mye ubehag for den lokale PPT-lederen som hadde mistet pennen da hun var ute og handlet.

Den 6. april 2010 kunne NRK opplyse at det var oppdaget at en ansatt hadde lest ulovelig i pasientjournaler . I løpet av tre år hadde kvinnen over 400 ganger vært inne i 26 journaler som tilhørte kollegaer, venner, naboer og deres familie. (www.nrk.no 06.04.2011) Dette er ikke et enestående tilfelle. Den 11.09.2010 ble en lege ved Molde sykehus tatt for å lest i kollegaers sykejournaler. (www.rbnett.no 11.09.2010) Det finnes flere slike eksempler som har skjedd de siste årene.

2.2.1 Internett en kilde til lekkasje av sensitive opplysninger

Internett er i dag en av samfunnets viktigste informasjonskilder. Bedrifter, kommuner, virksomheter og foreninger opprettet egne hjemmesider hvor de legger ut informasjon om seg selv. Dette krever at en har gode rutiner for å hindre at feil opplysninger kommer ut. Her kan det svikte. Sensitive personopplysninger som diagnose, personnummer og opplysninger om sosiale forhold har noen ganger vært fritt tilgjengelig på nettet. Et eksempel på dette er det som skjedde på Kristiansand sykehus hvor en la ut pasientliser med personnummer og diagnose ut på sykehusets hjemmeside. (www.abcnyheter.no 30.09.2009)

2.2.2 Forstår ikke konsekvenser

I Dagsrevyen mandag 12. april 2010 kom det fram at det var mulig å finne ut hvor mange som arbeider i Forsvarets sikkerhetstjeneste via Brønnøysundregisteret fordi forsvaret hadde levert inn opplysninger som de ikke var klar over ville bli offentlige. I forklaringen fra forsvaret ble det opplyst at en ikke var klar over konsekvensene. Den 29.04.10 kom det videre fram i Dagsrevyen at alle som hadde tilgang til NAV's Aa register (arbeidsgiver- arbeidstaker registeret) også hadde tilgang til navnene på de som arbeidet innefor Forsvarets sikkerhetstjeneste. I følge Dagsrevyen var dette ca. 38 000 personer. Selv om alle i NAV hadde underskrevet taushetserklæring var de ikke klarert for denne type opplysninger.

2.2.3 Fortsetter som før tross avvik

Nesten daglig kommer det fram i massemedia om sikkerhetsbrudd. I NRK 28.september 2010 ble det opplyst at ca. 200 000 nordmenn har vært utsatt for identitetstyveri. Ofte skylders dette at uvedkommende har fått tak i personnummeret til en annen person. Eksemplet det ble vist til i NRK skyldes at et brev fra NAV med personnummer var lagt i feil postkasse.
I www.abcnyheter.no ble det den 19. februar i 2011 opplyst at det i 2010 forsvant 537 pass sporløst i posten, mot 325 året før. Oversikt fra politiet viser at 1.598 pass har forsvunnet i postgangen siden 2006.
Til tross for dette sendes det fortsatt ut skattekort, selvangivelse, bankkort og pass som vanlig post. Det er ikke vanskelig for de som ønsker det å finne ut hva som ligger i konvoluttene.

2.2.4 Hacking blir mer bevisst brukt

Hemmelige opplysninger blir offentliggjort via massemedia. Tidligere var en hacker en ung gutt med spesiell interesse for data. For disse var det å klare og bryte seg inn hos andre det viktigste, ikke nødvendigvis å skaffe opplysninger. Dette er nå endret, og hacking brukes mer bevisst. Den siste tiden har det vært mye fokus rundt Wikileaks og hvordan de har klart å få tak i både militære og sivile opplysninger som regjeringer trodde var sikre. Hensikten her er å lekke hemmelige opplysninger som kan skade de som eier opplysningene. Hendelsene viser at ingen opplysninger er helt sikre selv ikke for en supermakt som USA.

2.3 Holdninger viktigere enn teknikk

Fremtidig databruk handler mye om teknikk, men det handler minst like mye om holdninger og kunnskap. Til syvende og sist er det den personen som bruker systemet som er den største risikoen. Forskning rundt ulykker viser at de fleste feil som gjøres skyldes menneskelig svikt. Det er blitt påstått at datasikkerhet handler om 20 % teknikk og 80 % holdninger. Dette kan sikkert diskuteres, men de fleste vil være enige i at holdninger og kunnskap spiller en stor rolle. Skal holdinger endres forutsetter det ofte mer kunnskap. Sikkerhet tas ikke på alvor før en forstår hvorfor det er viktig.

En vil kunne anta at bevisstheten om personvern vil bli større når de som er oppvokst med data kommer inn i arbeidslivet. En undersøkelse som er gjennomført av TNS Gallup for det statlige Norsk senter for informasjonssikring (NorSIS) viser at bare fire av ti under 30 år er opptatt av datasikkerhet, mens seks av ti over 30 er opptatt av det. (www.siste.no 08.09.10) Selv om dette er en generell undersøkelse så viser den at det er viktig å jobbe med øket datasikkerhet, og det er ikke noe som tilsier at det blir mindre viktig i årene som kommer. Her handler det også om å øke kunnskapsnivået.

2.4 Motivasjon for å skrive oppgaven

Mine motiver for å skrive denne oppgaven er at jeg over flere år har vært opptatt av personvern spesielt til bruk av IKT. I 1998 var jeg med på å innføre dataprogram i helse og omsorgstjenesten i kommunen der jeg er ansatt. Tidlig i prosessen så vi at bruk av IKT medførte mange nye problemstillinger som vi ikke var klar over når vi startet. Det første problemet var å lære og bruke data. De fleste som skulle læres opp hadde liten eller ingen bakgrunn. Opplæringen skjedde heller ikke fordi det var et ønske om å lære data, men fordi

noen ”sjefer” over dem hadde bestemt at en nå skulle begynne å bruke fagprogram. Det sier seg selv at motivasjonen kunne vært bedre. Vi så også at manglende kunnskap medførte at det ble gjort mange feil uten at de som gjorde dem selv var i stand til å oppdage de. Programvarene som ble utviklet hadde også tekniske feil som medførte at opplysninger kom på avveie eller forsvant.
Sener har jeg hatt systemansvar for flere fagsystemer innenfor både helse, sosial og barnevern.

Jeg er i dag personvernombud i kommunen. Gjennom dette arbeidet ser jeg hvor vanskelig det kan være å få til gode rutiner, og ikke minst en holdning hvor en opplever dette som viktig. I mange kommuner er det få rapporterte brudd på personvernet. Skyldes det at det ikke skjer feil, eller at de ikke blir rapportert? Det er noe av det jeg ønsker å finne ut av gjennom undersøkelsen i denne oppgave.

I oppgaven vil jeg også se på hvordan kommuner håndterer personopplysninger og da spesielt sensitive personopplysninger.
Videre ønsker jeg å se på om det er mulig å få til mer fokus på personvern, og hvilke faktorer som enten er med på å hindre, eller øke muligheten for å få dette til.

Siden dette er et tema som jeg forholder med til daglig vil selvfølgelig mine egne erfaringer og synspunkter påvirke både undersøkelsen, og de konklusjoner jeg trekker. I samråd med min veileder har jeg valgt ikke å bruke min egen arbeidsplass, da det kan bli vanskelig og ha samme holdning til denne som til de andre kommunene jeg undersøker.

3 Problemstilling

Hva skjer med journalen min?

Bruken av IKT i kommunene øker kraftig. Dette stiller store krav til sikkerhet, og er kommunene i stand til å ivareta personvernet med dagens teknolog?
Elektronisk pasientjournal (EPJ- systemet) og røntgeninformasjonssystem (RIS) er på vei inn i helsesektoren. Disse gjør det mulig å sende pasientopplysninger elektronisk. I tillegg er

flere kommuner nå i ferd med å innføre trådløse enheter hvor en kan koble seg inn på kommunens helse og omsorgsprogrammet når en er hjemme hos brukerne. Dette er selvfølgelig til stor hjelp i det daglige, men samtidig setter det også større krav til sikkerhet. Ikke bare til de tekniske løsningene, men enda mer til de som benytter denne type løsninger. Kommunene står i dag ovenfor nye store utfordringer som vil kreve både økt kompetanse og bruk av IKT. Stortingen har nå vedtatt samhandlingsreformen som vil stille krav om økt kompetanse i kommunene, samtidig som kravet til innsparinger og mer rasjonell drift øker. Er kommunene i stand til å møte denne utviklingen, eller medfører innføring av ny teknologi større risiko for at opplysninger kommer på avveie eller ikke er korrekte?

De fleste av oss er opptatt av egen og våre nærmestes helse. I dette ligger det også å få god og riktig hjelp når vi trenger det. En forutsetning er da at de som skal yte hjelpen har riktige opplysninger til riktig tid. Samtidig er det opplysninger vi ønsker skal være private og ikke tilgjengelig for andre. Når alle opplysninger ligger på data krever det sikre systemer og personer som kan ivareta personvern. Spørsmålet blir da:

Kan vi som innbygger være sikre på at kommunen forvalter sensitive opplysninger på en sikker måte?
Hvilke rutiner og sikkerhetssystemer har kommunene etablert for at personvernet skal bli ivaretatt?
Hvilke faktorer er det som bidrar til, eller hindrer en sikker behandling av sensitive opplysninger i kommunen?

For å avgrense oppgave har jeg kun valgt og undersøke kommunens helse- og omsorgstjeneste.

4 Personvern i Norge

I denne delen av oppgaven går jeg igjennom hvordan personvernet er regulert i Norge, og hvilke krav som stilles i både lover og forskrifter. Jeg ønsker å vise hvor detaljert personvernet er regulert, og hvor mange krav som stilles. Kravene vil så danne bakgrunnen i vurderingen om kommunene ivaretar personvernet på en sikker måte. I tillegg vil jeg

redegjøre for hvordan tilsynet med personvernet er organisert. I den siste delen av kapittelet går jeg igjennom resultatene av de tilsyn som Datatilsynet har foretatt. Disse resultatene vil i drøftingenskapitelet ble sammenlignet med de funn som kommer fram i selve undersøkelsen.

4.1 Begreper

Her foretas det en gjennomgang av sentrale begrep som benyttes i både lover, forskrifter og veilere i personvern.

Personopplysning: opplysninger og vurderinger som kan knyttes til en enkeltperson. Dette kan være navn, personnummer, diagnose, familieforhold. I helsesektoren er det de opplysinger som kommunen trenger om pasientene for å utføre behandling og som pasientene må oppgi for å få hjelp

Behandling av personopplysninger: enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter. Innenfor helsesektoren vil en benytte informasjon til å stille diagnose, gjennomføre behandling og oppdatere informasjon.

Personregister: registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen. I kommunene vil registrene både være elektroniske og manuelle. De elektroniske vil innenfor helsesektoren stort sett inngå i fagsystemene. De manuelle oppbevares i arkivskap. Det er ikke uvanlig at en opererer med både elektroniske og manuelle personregister. Helseregister vil være definert som et personregister.

Behandlingsansvarlig: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. I en kommune vil det være den øverste administrative lederen som oftest rådmann, med mindre dette er delegert til andre for eksempel leder for virksomheten.

Databehandler: den som behandler personopplysninger på vegne av den behandlingsansvarlige. Dette er de ansatte som i daglig registrer opplysninger og benytter opplysninger i behandlingen av pasienter.

Registrert: er den personen som opplysingene er knyttet til.

Samtykke: en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv. Samtykket skal gis før det er lov å foreta

registrering av opplysningene. Samtykke bør være skriftlig for å unngå missforståelser i ettertid.

Sensitive personopplysninger: opplysninger om
a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
c) helseforhold,
d) seksuelle forhold,
e) medlemskap i fagforeninger

(Lov om behandling av personopplysninger § 2)

Konfidensialitet

Med "*konfidensialitet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt må være sikret mot at uvedkommende får kjennskap til opplysningene. Utvedkommende i denne sammenheng omfatter også er alle som ikke trenger personopplysningene for å utføre sitt arbeid, selv om de arbeider i samme organisasjon.

Tilgjengelighet

Med "*tilgjengelighet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt som skal behandles av autorisert personell, er tilgjengelig til den tid og på det sted der det er behov for opplysningene. Systemer må ikke bli så sikre at behandlere ikke får nødvendig tilgang. Datasikkerhet handler ofte om å finne en riktig balanse mellom konfidensialitet og tilgjengelighet.

Integritet

Med "*integritet*" menes at personopplysninger og annen informasjon underlagt taushetsplikt må være sikret mot utilsiktet eller uautorisert endring eller sletting. Feil opplysninger kan medføre fare for liv og helse. Det samme kan også mangel på opplysninger som sykdommer eller allergier pasientene har. Opplysinger må være lagret slik at en ikke med vilje eller ved feil kan slette eller legge inn feil opplysninger. Dette vil som oftest kreve at det foretas kontroll med opplysningene i ettertid.

Kvalitet

Med *"kvalitet"* menes at personopplysninger og annen informasjon underlagt taushetsplikt må være korrekt, oppdatert, samt relevant og tilstrekkelige som grunnlag for saksbehandling og tjenesteytelse.

4.2 Regulering av personvern i Norge

Her følger en oversikt over de viktigste lover, forskrifter og offentlige dokumenter som behandler personvernet i Norge.

4.2.1 Lov om behandling av personopplysninger

I 1978 kom Lov om personregistre m.m., denne ble i 2000 erstattet av Lov om behandling av personopplysninger (personopplysningsloven - popplyl) Formålet er definert i :

"§ 1. Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger [….].

Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysning er."

Det er uarbeidet egen forskrift til loven: FOR 2000-12-15 nr 1265:

Forskrift om behandling av personopplysninger (personopplysningsforskriften)

4.2.2 Lov om helseregistre og behandling av helseopplysninger

Innenfor helsesektoren er Lov om helseregistre og behandling av helseopplysninger (helseregisterloven) en av de viktigste. Lovens hensikt er å sikre at informasjon og kunnskap om den enkelte ivaretas slik at det ikke krenker privatlivet, samtidig som helsehjelp gis på en forsvarlig og effektiv måte. (§ 1) Det er i tillegg utarbeidet en rekke forskrifter til loven.

4.2.3 Lov om Schengen informasjonssystem

Norge er også forpliktet gjennom Lov om Schengen informasjonssystem, men da denne faller utfor tema for denne oppgaven går jeg ikke nærmere inn på den.

I tillegg kommer alle særlover innenfor helse, sosial, skole, barnehage, barnevern m.m..

4.2.4 Normen for informasjonssikkerhet

I forbindelse med arbeidet med å innføre elektronisk pasientjournal ble "Normen for informasjonssikkerhet" utarbeidet av representanter for helsesektorene. Disse var Den norske lægeforening, representanter for de regionale helseforetak, Norsk Sykepleierforbund, Norges Apotekerforening og Kommunenes Sentralforbund. I tillegg har Datatilsynet, Helsetilsynet, Rikstrygdeverket og Sosial- og helsedirektoratet deltatt i arbeidet. Formålet med normen er å bidra til tilfredsstillende informasjonssikkerhet i helsesektoren, herunder også kommunene. Normen er også ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet. Normen er juridisk bindene for alle som inngår avtale med Norsk helsenett. [1]

4.2.5 Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger.

Helse- og omsorgsdepartementet sendte i mai 2010 ut Forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.

Departementet skrev i følgebrevet at de har lagt stor vekt på å få fram et regelverk som balanserer mellom hensynet til raskt tilgang til relevante helseopplysninger når dette er nødvendig for å gi behandling, og pasientens rett til å verne om opplysninger. De sier videre at det er avgjørende for tilliten til helsetjenesten at pasienter kan føle seg trygge på at sensitive opplysninger ikke kommer på avveie. Forskriften er foreløpig ikke vedtatt.

---

[1] Virksomheten Norsk Helsenett AS ble stiftet høsten 2004, med grunnlag i nasjonale helsemyndigheters mål om et sikret nettverk for elektronisk samhandling i helse- og omsorgssektoren i Norge, med tilhørende relevante tjenester [……]Norsk Helsenett SF eies av staten, og eierskapet forvaltes av Helse – og omsorgsdepartementet www.nhn.no/om-oss .)

4.3 Tilsyn med personvernet i Norge

I Norge er det nær førti statlige organer som fører tilsyn med private og offentlige aktører for kontrollere at de holder seg innenfor lover og forskrifter. I alt går det med ca 7 000 årsverk til dette arbeidet. Personvernet ivaretas av Datatilsynet. (St.meld. nr. 17 2002-2003 Om statlig tilsyn)

Grovt forenklet er følgende fire grunnvirkemidlene lagt til grunn for de fleste tilsyn i Norge:

1. Tilsyn: Kontroll av de områdene tilsynet har ansvaret for. Hensikten er å påse at de følger de formelle krav som er satt. Datatilsynet har ansvar for tilsyn av de virksomheter som omfattes av lov om personvern.
2. Detaljregulering eller normerende vedtak: Fatte enkeltvedtak om godkjenning eller pålegg. Utarbeide forskrifter innenfor sitt fagområde. For Datatilsynet vil dette være alle virksomheter som behandler personopplysninger.
3. Informasjon: Generell informasjon om reguleringens formål, om regelvekets krav og lignende temaer av betydning. Dette kan både være allmennheten, og de spesielle områdene tilsynet rettes seg mot.
4. Overvåking: Samle inn og systematisere ulike former for kunnskap av betydning for reguleringsområdet. For eksempel prøvetaking for å kartlegge utbredelse av sykdommer, overvåke kredittgivning, vurdere risiko i ulike bransjer. Datatilsynet kan vurdere risiko ved innføring av nye programmer, eller nytt overvåkingssystemer som for eksempel TV overvåking av et offentlig område.

(Statskonsult, Rapport 2002: 12, s. 25,26)

I sin rapport 2002:12 (Be)Grep om tilsyn, Gjennomgang av statelige tilsynsordninger, foretar Statskonsult en inndeling av tilsynene etter tilsynsordningers hovedformal:

1. Sikkerhet for liv, helse, miljø og materielle verdier/ressurser
2. Fungerende samferdsel, kommunikasjon og energiforsyning
3. Fungerende marked
4. Integritetsvern og ideelle verdier

Datatilsynet hører til under den siste kategorien.

4.3.1 Datatilsynet

For å ivareta både samfunnet og enkeltpersoner sine behov for sikkerhet ble Datatilsynet, offentlig kontrollorgan opprettet 1978 i henhold til lov om personregistre m.m., fra 2000 Lov om behandling av personopplysninger (personopplysningsloven)**.** Tilsynet er underlagt Fornyings- og administrasjonsdepartementet, men er faglig uavhengig. Tilsynet er lagt til Oslo og det er ikke opprettet lokale enheter.
Datatilsynet har flere oppgaver, men de viktigste er å være et tilsyn og ombud for personvern i Norge. Gjennom aktivt tilsyn og saksbehandling kontrollerer Datatilsynet at lover og forskrifter for behandling av personopplysninger blir fulgt, og at feil og mangler blir rettet. I tillegg skal Datatilsynet identifisere farer for personvernet og gi råd om hvordan de kan unngås eller begrenses. Datatilsynet har også en viktig ombudsrolle. I den forbindelse gir de rådgivning og informasjon overfor enkeltpersoner som tar kontakt. (www.Datatilsynet.no)

Datatilsynet har flere oppgaver, men de har ingen direkte innvirkning på personvern i kommunene.

Datatilsynet har følgende reaksjonsmulighet når det foreligger brud på lover og forskrifter:

Enkeltvedtak om korrigerende tiltak (pålegg): Datatilsynet kan når de oppdager feil eller mangler fatte vedtak om at manglene skal utbedres innen en gitt tidsfrist.

Enkeltvedtak om tvangsmulkt/gebyr: I de tilfeller ikke pålegg blir fulgt opp eller feilene er så alvorlig at de må rettes fort, kan Datatilsynet gi tvangsmulkt

Enkeltvedtak om forelegg/tvangsgjennomføring: Dersom tilsynsobjekt ikke har fulgt opp tidligere vedtak, eller nekter å gjennomføre det kan Datatilsynet iverksette tvangsgjennomføring. Dette gjennomføres på tilsynsobjektets regning.

Enkeltvedtak om stansing, tilbakekalling av tillatelse: Der feil er så graverende at det kan medføre fare for helse, eller medfører stor fare for personvernet kan Datatilsynet stoppe virksomheten. For de som behandler personopplysninger som ikke er hjemlet i lov må det søkes om konsesjon. Når betingelsen i konsesjonen ikke oppfylles kan datatilsynet trekke denne tilbake.

Politianmeldelse: Der det har forekommet alvorlige lovbrud, eller ikke tidligere pålegg er utført, kan Datatilsynet gå til politianmeldelse.

Alle vedtak er enkeltvedtak etter forvaltningsloven og kan påklages av den som får pålegget.

Datatilsynet har utarbeidet en rekke veileder for hvordan kommune skal håndtere datasikkerhet. Dette er veiledning i oppbygging av internkontrollsystemer i kommunen, gjennomføring av risiko- og sårbarhetsanalyse, oppbygging av sikre nettverk, personvern ombud m.m..

4.3.2 Personvernnemnda

Personvernnemnda er opprettet med hjemmel i lov om behandling av personopplysninger § 43 i Personopplysningsloven. Personvernnemnda skal behandle klager på vedtak som Datatilsynet fatter i medhold av personopplysningsloven og enkelte andre lover. Personvernnemnda har syv medlemmer som oppnevnes for fire år med adgang til gjenoppnevning for ytterligere fire år. Lederen og nestlederen oppnevnes av Stortinget. De øvrige fem medlemmene oppnevnes av Kongen. Hvert medlem har personlig varamedlem. Personvernnemnda møtes en gang i måneden, og behandlet i 2010 ti saker.
(www.personvernnemnda.no)

4.4 Krav for å lagre og behandle personopplysninger

I følge personopplysningsloven stilles det en del krav for å lagre og behandle personopplysninger. Her vil jeg trekke fram følgende forhold:

Lovgrunnlag: Det er fastsatt i lov at det er adgang til å lagre denne type opplysninger. Innenfor kommunen vil registrering av personopplysninger være hjemlet i kommunehelsetjenesteloven, sosialtjenesteloven, barnevernsloven og opplæringsloven. Skal det lagres personopplysninger som ikke er hjemlet i lov, må det søkes datatilsynet om konsesjon. Dette kan for eksempel være register som opprettes i forbindelse med forskning.

Samtykke: Den som blir registrert skal vite hvilke opplysninger som blir lagret og gi sin godkjenning til at det gjøres. Her finnes det unntak, men jeg velger ikke å gå nærmere inn på det, da det ikke er relevant for oppgaven. I tillegg har en krav på å få informasjon om hva opplysningene skal brukes til, og hvem som får tilgang til å lese de. Leveres sensitive opplysninger til andre enn det som det tidligere er gitt beskjed om, skal det innhentes ny tillatelse.

Innsyn:. En har rett til innsyn i alle opplysninger som blir lagret om en og kan be om å få utskrift av opplysningene. I tillegg har en rett til å kreve at opplysninger som er feil blir rettet eller slettet. Her finnes en del unntak, disse er nærmere definert i § 23.

Unngå at det lagres unødvendige opplysninger: De opplysninger som lagres skal ha en klar hensikt. Det er ikke tillat og lagre opplysninger som ikke benyttes og er nødvendig for behandlingen selv om de er helseopplysninger. Dette kan være opplysninger om økonomisk inntekt, familie, seksuell legning, politisk eller religiøs oppfattelse.

4.4.1 Meldeplikt til Datatilsynet

Ved opprettelse av elektroniske personregister som ikke trenger konsesjon kreves det at følgende opplysninger skal meldes inn til Datatilsynet:
Navn og adresse på den databehandlingsansvarlige. Alle virksomheter som behandler sensitive opplysninger skal ha en person som står ansvarlig. Dette skal være den personen som til daglig har ansvaret for virksomheten. I kommunene vil dette være rådmann. Det skal også redegjøres for når kommunen startet opp med å behandle sensitive opplysninger, og bakgrunnen for at dette ble gjort. I tillegg skal en redegjøre for hvilket lovgrunnlag behandlingen skjer ut fra, og hvem i kommunen som foretar behandlingen.

Kommunen skal ha en total oversikt over hvilke opplysninger som lagres, og hvem de har fått opplysningene fra.

4.4.2 Personvernombud

Isteden for å melde inn databehandling kan virksomheten søke om å få opprette et personvernombud. Det er Datatilsynet som godkjenner denne personen. Personvernombudet skal ha de samme opplysningene som ellers ville bli meldt inn til Datatilsynet. I tillegg skal denne personen påse at organisasjonen følger kravene om personvern, og påpeke når det gjøres feil. Denne funksjonen er bare rådgivende og fritar ikke kommunenes ledelse for ansvaret.

4.5 Erfaringer fra tilsyn i 2003

Datatilsynet gjennomførte i 2003 tilsyn med 31 norske kommuner fordelt i hele Norge. Hensikten med tilsynet var å se om kommunene etterlever kravene bla. til internkontroll, og

kravene etter personopplysningsloven.
Tilsynet konkluderer med at de fleste kommunene kjente godt til prinsippene for personvern, spesielt når det gjelder taushetsplikt. Tilsynet så at det i praksis ble gjort mye riktig. Det som imidlertid manglet var dokumentasjon og systematisering av hvordan personopplysninger skulle håndteres, som medførte at det oppstod feil og misforståelser når det kom andre inn som ikke kjente til de ikke dokumenterte rutinene.

Tilsynet fremhevet spesielt følgende forhold:
Kommunene plikter å ha oversikt over alle personopplysninger som blir behandlet og lovgrunnlaget for behandlingen. Tilsynet fant mange mangler på dette punktet selv om variasjonene var store fra kommune til kommune.
Det var kun et midletall av de som ble undersøkt hvor det var etablert en god struktur for ansvar og myndighet. Det er rådmannen som kommunens øverste administrative leder som er behandlingsansvarlig. Rådmannen vil naturlig nok ha behov for og delegere dette til andre. Det er imidlertid rådmannen som skal fastsette rammene som de øvrige aktørene i kommunen skal forholde seg til. I noen tilfeller var rådmannen svært lite aktiv i forhold til og implementer regelverket. I andre tilfeller var det uklare rammer for ansvar og myndighet. Datatilsynet understreker at orden og en lederstruktur er meget viktig.

Datatilsynet avdekket at det manglet internkontrollsystem hos de fleste av kommunen de besøkte. I Personopplysningsloven kap. 3 stilles det krav om at kommunen skal ha et internkontrollsystem som sikrer at kommunen ivaretar lovkravene for å behandle personopplysninger. I dette ligger også at bestemmelsene skal være kjent ute i organisasjonen. Det var imidlertid stor variasjon mellom kommunene i hvor langt de var kommet i utarbeidelse av interkontroll system. De fleste kommunene hadde utarbeidet noen rutiner, men manglet et helhetlig internkontrollsystem.

De virksomheter som foretar behandling som er hjemlet i lov slipper med enkelte unntak å søke om konsesjon, men de må melde behandlingen inn til Datatilsynet. Til tross for at norske kommuner er stort sett like fant tilsynet ut at det var stor forskjell på hva som var meldt inn til Datatilsynet. For de kommunene som ble undersøkt varierte antall meldinger fra ingen til over tretti. Stort sett er det for få innmeldinger. (Datatilsynets årsmelding 2003)

4.6 Tilsyn i perioden 2004 – 2010

I 2004 var det var et unaturlig dødsfall ved en omsorgsbolig i Horten kommune som følge av omstedighetene rundt manglende tilsyn med en pleiepasient. Datatilsynet gjennomførte tilsyn med Horten kommune på bakgrunn av at de gjennom media og av Helsetilsynet ble kjent med at det hadde skjedd et unaturlig dødsfall. Etter tilsynet kom Datatilsynet med følgende uttalelse:

"*Tilsynet hadde spesielt fokus på omstendighetene rundt innføring av nytt pleie- og omsorgsystem. I dette ligger også et fokus på kommunens internkontroll. Internkontroll danner en viktig basis i behandlingsansvarliges arbeid med å sørge for etterlevelse av gjeldende lover og forskrifter. "*

"*Sammendrag og hovedfunn:*
Datatilsynet konstaterer at det ved gjennomføring av tilsynet ble avdekket vesentlige avvik fra regelverket. Avvikene er spesielt alvorlig sett i lys av ovennevnte hendelse hos kommunen i mai 2004. Datatilsynet danner seg som hovedinntrykk at kommunens toppledelse i all hovedsak har manglende kjennskap til personopplysningslovens bestemmelser.
Avvikene kan oppsummeres i følgende forhold: Kommunen hadde ikke ivaretatt sentrale plikter gitt i personopplysningsloven. Kommunen mangler også et tilfredsstillende system for internkontroll. De kunne ikke legge fram risikovurdering for kommunens informasjonssystem. De ansatte hadde ikke fått nødvendig opplæring i bruk av systemene og det var mangler ved avvikshåndteringen."

"Datatilsynet hadde spesielt trukket frem at kommunens toppledelse ikke i tilstrekkelig grad har ivaretatt sitt ansvar som behandlingsansvarlig. Behandlingsansvarlig skal aktivt sørge for at arbeid med ivaretakelsen av regelverkets krav ivaretas og skal forvisse seg om fremdrift i dette arbeidet".
(RAPPORT FRA TILSYN Saksnummer: 2004/1825, Datatilsynet)

Våren 2009 gjennomført Datatilsynet fem tilsyn i norske kommuner. Av disse fikk samtlige påbud om enten å etablere eller forbedre internkontrollsystemer. I tillegg ble det påpekt at det hos flere manglent risikovurdering, gjennomføring av sikkerhetsrevisjon og gjennomføring og håndtere avvik eller sikkerhetsbrudd.

I 2010 gjennomførte Datatilsynet en ny undersøkelse hvor de sendte ut spørsmål til alle norske kommuner. Undersøkelsen ble foretatt som en tradisjonell spørreundersøkelse. I

henhold til Personopplysningsloven § 42 ble alle kommuner pålagt å svare.
Her svarte bare 52% at de hadde etablert system for interkontroll for behandling av personvern. I gjennomføringen av undersøkelsen ble det fra Datatilsynet stilt en rekke kontrollspørsmål til de som hadde svart ja. Ved å analyse svarene falt andel av de som tilfredsstiller kravene ned til 7 %. (Kommunerapporten 2010-2011, s 9)

4.7 Mulighet for å bli oppdaget

Datatilsynet har som tidligere beskrevet oppgaven med å sikre at norske kommuner ivaretar personvernet. I Norge er det 429 kommuner. Alle disse foretar behandling av sensitive personopplysninger. Fra 2003 til 2009 fikk 36 kommuner tilsyn. Det utgjør 8,4 % av alle norske kommuner som fikk tilsyn i løpet av 5 år. Ut fra antallet tilsier det at sjansen for å få tilsyn er relativ liten, noe som innbærer at feil og mangler kan foregå i lang tid uten at det blir oppdaget. Dette setter både personvernet og sikkerheten i fare. Det viser også den siste undersøkelsen fra Datatilsynet i 2010, da bare 7 % kommunene tilfredsstiller kravene.

4.8 Oppsummering

Som det fremkommer av kapitelet er personvernet i Norge godt regulert både gjennom lover og forskrifter. Det er til dels detaljerte beskrivelser av hva kommuner, og andre virksomheter skal gjøre for å ivareta personvernet. Den første loven kom allerede 1978 så kommunene har hatt god tid til å sette seg inn i lovverket. Når det likevel skjer svikt i personvernet er det derfor lite sannsynlig at dette skyldes mangel på beskrivelser fra overordnede organ. Årsaken til svikt må finnes andre steder. Som det fremkommer fra tilsynene som Datatilsynet har gjennomført kan det virke som kommunene til tross for et regulert lovverk ikke følger det. Spørsmålet blir da hva er årsaken til det? I denne oppgaven ønsker jeg å ta utgangspunkt i det som skjer i selve kommunen og se om noe av årsaken kan ligge der.

5 Teori

5.1 Innledning

I denne delen av oppgaven vil jeg se på teoretiske perspektiver for å belyse problemstillingen med og i vareta personvern i kommunene. Jeg har valgt å benytte teorier som belyser hvordan en kan skape en sikker organisasjon, da mitt utgangspunkt er kommunen som organisasjon. Personvern inngår i mange av de oppgavene som en kommune skal utføre. For å avgrense oppgaven har jeg valgt kun å se på de oppgavene som inngår i helse- og omsorgstjenesten, da spesielt med vekt på den behandling som skjer ved hjelp av elektroniske fagsystemer.

5.2 En sikker organisasjon

En norsk kommune er også en sikkerhetsorganisasjon. For kommuner som for andre organisasjoner er det viktig å unngå at det skjer feil som kan få store konsekvenser. Innenfor personvern vil feil kunne føre til at pasienter ikke får riktig behandling, eller at sensitive opplysninger kommer på avveie. Det blir viktig å finne mekanismer som hindrer at dette skjer. En av teoriene som har sett på dette er High Reliability-teorien (HRT) eller High Reliability-organisasjon (HRO) som ble utviklet av noen forskere ved universitet i California. HRO hevder at det er mulig å utvikle en organisasjon hvor ulykker kan forbygges, selv med komplisert teknologi og stort risikopotensial. (Alven, Boyesen, Njå, Olsen og Sandve, 2004 s.59)

Selv om denne teorien er utviklet innefor høytekniske organisasjoner som romfart og atomindustrien mener jeg at en kan benytte mye av de samme teorier innenfor en kommune, selv om denne har et helt annet risikobilde. Grunnen er at teorien bygger på prinsipper som er generelle for alle organisasjoner hvor sikkerhet er viktig.

Mange av de områdene HRO beskriver vil være viktige forutsetninger for at kommunene skal fremstå som en sikkerhets organisasjon. Jeg vil her trekke fram følgende områder som er relevant for personvern i en kommune:

Sikkerhet og pålitelighet må ha høy prioritering hos alle ledere og hos de ansatte. I dette ligger det at sikkerhet må gjennomsyre hele organisasjonen også i det daglige arbeidet. Personvern må ikke bare overlates til de som er opptatt av tema, eller de som til daglig arbeider med sensitive opplysninger.

Redundans øker sikkerheten. Ved å etablere reservesystemer, duplikasjoner eller sjekkpunkter vil en kunne unngå at det oppstår feil, og samtidig gjøre upålitelige systemer mer sikre. Når det likevel gjøres feil må det være systemer som oppdager disse før de får konsekvenser. Dette kan være tekniske systemer som oppdager at det ikke er tatt backup, eller at opplysinger ikke blir lagret. Det kan også være alarmer som utløses når det oppstår brann eller forsøk på innbrudd i de områdene hvor en oppbevarer datautstyr.
I følge Reason (Reason 1997 s. 223) skyldes 80 – 95 % av alle ulykker og feil menneskelig svikt. Derfor er det like viktig at de operasjoner som utføres av ansatte blir kontrollert. Som oftest vil det være ansatt som kontrollerer en annen ansatt. Dette benyttes for eksempel ved legging og utdeling av medisiner.
Desentralisert styring, sterk organisasjonskultur og kontinuerlig lærling er viktig. Dette krever en desentraliserte organisasjon som er i stand til å få en rask, fleksibel reaksjon på de overraskelsene som kan komme. HRO teorien har i det siste også vært opptatt av at personene i organisasjonen skal ha forskjellig kompetanse. Feil som en person overser kan da lettere oppdages av en annen som har annen utdannelse fordi en er opptatt av andre områder. Kompetanse handler også om forskjellige kulturbakgrunn, opplæring og erfaringer. Kommunene består av ansatte med mange forskjellige utdannelse og erfaring som kan benyttes for å øke sikkerheten. (Alven, Boyesen, Njå, Olsen og Sandve 2004 s.59)

5.3 Kommunen som organisasjon

Det som kjemmetegner en organisasjon fra andre samlinger av mennesker er at det er en planmessig koordinering av menneskers aktivitet for og nå et felles mål, hvor arbeidet er fordelt etter oppgaver (Schein, 1983 s. 25) Schein trekker også fram at en organisasjon er bygget opp hierarkisk. Det er også vanlig å skille mellom formelle og uformelle organisasjoner. I følge Nils Brusoson og John P. Olsen (Brusoson, Olsen 1990, kapittel 1) skiller den formelle organisasjonen seg ut med at den er opprettet for å ivareta bestemte oppgaver og fremme at forholdsvis presist mål. En norsk kommune er en formell organisasjon fordi den skal vareta befolknings behov innenfor helse, NAV, skole, barnehage, kultur, tekniske tjenester m.m. Målet for arbeidet er vedtatt av Stortinget og regjering.

5.4 Kommunens organisasjonskultur

Der mennesker er sammen over lengre tid vil det oppstå kulturer. Mens kommunen organisasjon er lett å beskrive gjennom organisasjonskart og instrukser kan organisasjonskulturen være vanskeligere å definere.

Flere forfattere har definert begrepet organisasjonskultur. Den enkleste og samtidig en av dem som også er lettest å forstå er *"Kultur er måten vi gjør ting på her hos oss"* (Deal & Kennedy, 1982;4, hentet fra Bang 1988 s. 22). Den sier noe om hvordan kulturen preger medlemmene i måten de utfører arbeidet sitt, men den sier ingen ting om årsaken til at det skjer. Den blir derfor for enkel til å bruke for å analysere hvilke faktorer som danner en organisasjon og opprettholder den. Andre forfattere går lengre i sine tolkninger, og trekker også fram medlemmenes vikelighetsoppfattelse og de verdier og normer som råder innenfor organisasjonen. (Carlsson, 1984;4, hentet fra Bang 1988 s. 22). Her trekker en også inn at organisasjonskultur handler ikke bare om hvordan en gjør ting, men også om de verdier og normer som ligger bak det som utføres. Schein trekker også inn at organisasjonskultur bygger på antagelser som er oppfunnet, oppdaget eller utviklet av gruppa i det den lærer og hanskes med sine eksterne tilpasninger og interne integrasjonsproblemer som har fungert bra nok til å bli betraktet som gyldig, og som derfor læres bort til nye medlemmer som den rette måten å oppfatte, tenke og føle på i relasjon til disse problemer*"* (Schein, 1985;9, hentet fra Bang 1988 s. 22)

Schein understreker noen faktorer som må ligge til rette for at en organisasjonskultur skal oppstå og utvikles.. Medlemmene i gruppa har gjennom erfaring tilegnet seg kunnskap som den mener er viktig å ta med videre, og videreføre til nye medlemmer i gruppa. Han legger vekt på at gruppen må ha vært lenge nok sammen til å ha opplevd og delt betydningsfulle problemer og at en må ha hatt muligheter til å løse disse problemene og observere effekten av løsningene.

Organisasjonskultur er med andre ord ikke noe som vedtas, men noe medlemmene skaper sammen over tid gjennom erfaringer, og som opprettholdes ved at den overføres til nye medlemmer i organisasjonen som bringer kulturen videre. På den måten kan en organisasjonskultur overleve selv om medlemmene skiftes.

Det kan være krevende å finne ut av en kommunes organisasjonskultur. De fleste kommuner ønsker å fremstå med en offisiell kultur som skal gjennomsyre det arbeidet som gjøres. Dette gjøres blant annet ved at kommunene har utarbeidet verdiord som en finner på brevark og

hjemmesider, og som en ønsker skal gjenspeile det kommunen stå for. Det er ikke helt sikkert at disse verdiene alltid gjenspeiler verdiene i hele organisasjonen.

5.5 Typer organisasjoner

Reason beskriver tre forskjellige typer kultur og hva som beskriver disse. Dette er et skjematisk oppsett, og i de fleste kulturene vil en kunne finne elementer av alle typer selv om en er mer dominerende.

Patologiske kulturer	Byråkratiske kulturer	Generative kulturer (skapende)
Vil ikke vite	Finner ikke feil	Søker aktivt for å finne feil
Budbringere blir ”skutt”	Budbringere blir lyttet til hvis de ankommer	Budbringere blir trent opp og belønnet
Man skyr ansvarlighet	Ansvar blir divisjonalisert	Ansvar er delt
Feil blir straffet eller skjult Nye ideer blir motarbeidet	Feil fører til lokale reparasjoner Nye ideer skaper problemer	Feil fører til omfattende reformer Nye ideer blir ønsket velkommen

(Reason 1997 s. 38)

5.5.1 Patologiske kulturer

I en patologisk organisasjon ønsker en ikke å forholde seg til feil eller mangler, eller en fornekter at det finnes noen. I denne type organisasjon vil en sannsynlig ikke legge vekt på forsvarsmekanismer, enkelt og greit fordi en mener at en ikke trenger dem. Ansatte som kommer fram med kritikk vil fort og effektivt bli frosset ut. Skulle det oppstå feil blir det viktig å finne syndebukken som så blir straffet. Ansvar og skyld blir individualisert ved at en kun er opptatt av menneskene og ikke hvordan organisasjonen fungerer. En ser ikke, eller er ikke villig til å se om årsaken til feil også kan ligge i hvordan en organiserer arbeidet. De kommuner som har en patologisk kultur vil fort få store problemer med å ivareta personvernet. Først og fremst fordi en ikke ser behov for å gjøre noe.

5.5.2 Byråkratiske kulturer

I en byråkratisk organisasjon vil en satse på de fysiske løsningene. Øvelser og opplæring vil det være lite fokus på. Denne type organisasjon vil kunne ha utarbeidet rutiner for personvern, men en regner med at jobben er gjort når rutiner er på plass. En har lite fokus på at det kan oppstå feil, eller at rutiner må evalueres.

Det som eventuelt skjer vil skje innefor egen avdeling, og i liten grad involvere hele organisasjonen. Her vil det kunne oppstå egen subkultur innenfor enkelte avdelinger som ordner opp selv, uten å trekke med resten av organisasjonen. Feil blir løst der de skjer og erfaringer bringes ikke videre til resten av avdelingen slik at andre kan få de samme erfaringene. Organisasjonen fortsetter som får.

5.5.3 Generative kulturer

I den generative kulturen vil en ha et ønske om å oppdage feil og utbedre dem. Opplæring og øvelser vil være en naturlig del av organisasjonens daglige liv. Innenfor personvern innebærer det at en ikke bare etablerer nødvendige hard defence (fysiske sikringstiltak) og soft defence (rutiner, øvelser m.m.), men også har et bevisst forhold til det i det daglige arbeidet. I dette ligger det også en bevissthet i alle ledd i organisasjonen om at dette er viktig. Sikkerhet vil dermed handle om mer enn bare forsvarsmekanismer, men like nye om holdninger og kognitive prosesser hos de som forholder seg til det i det daglige. I denne type organisasjon vil det aldri bli en diskusjon om det er viktig med personvern. Her er diskusjonen hvordan det best kan ivaretas og stadig bli bedre. Personvern vil heller ikke bli et eget tema som bare tas opp ved jevne mellomrom. Personvern vil inngå som en naturlig del av det daglige arbeidet som utføres.

Flere av de samme elementene finnes innenfor HRO teorien. Her påpekes det at for å forstå HRO må en også se på hvordan kognitive prosesser virker inn på det å oppdage og rette feil. Rosness, Guttormsen, Steiro, Tinmannsvik og Herrera henviser til Weick og Sutcliffe som benytter begrepet ”*Mindfulness”*. De hevder at kognitive prosesser er et fremtredende karakteristikum for HRO. Det spesifikke er at HRO aksepterer at feil kan skje. Dersom feil kan oppstå må organisasjonen utvikle ferdighet hvor man oppdager feil, og fjerner disse på et tidlig stadium før det medfører stor skade. Forfatterne har utarbeidet en oversikt hvor de

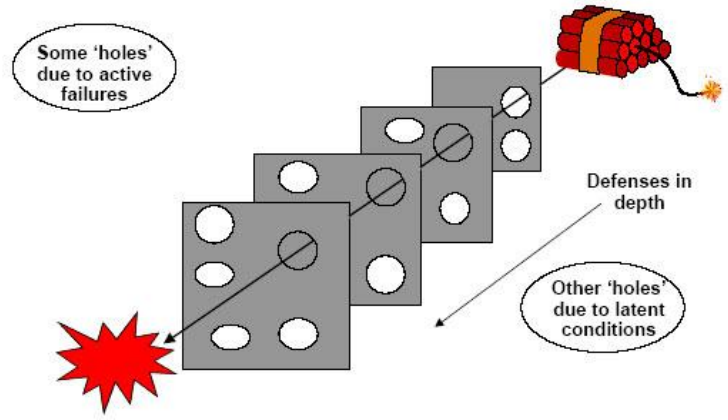
setter opp de forskjellige elementene innenfor Mindfulness. De trekker fram følgende elementer som er viktig:
Personene eller de ansatte må hele tiden være opptatt av at det kan oppstå svikt som en tidligere ikke har oppdaget.
Det må være en motvilje mot å forenkle arbeidsprosesser. Forenkling kan medføre at en overser potensielle farer. HRO teorien trekker også fram viktigheten av å ha personer tilstede med forskjellig bakgrunn og kompetanse for på den måten lettere se hvilke svakheter det er i organisasjonen, for på den måte å lære av hverandre.
Ansatte må ha en kontinuerlig overplikt over det som skjer for å oppdage om det i arbeidsprosessene, eller i det arbeidet som utføres er svakheter som om det ikke blir tatt tak i kan medfører svikt over tid.
Ingen organisasjon er feilfri. Feil vil oppstå, men de må ikke hemme driften. Ved å trekke på den kompetansen som er i organisasjon kan en lettere løse de problemer som oppstår.
Når det oppstår problemer i virksomheten flyttes beslutningene til den eller de som har best kunnskap og evne til å løse problemet. En bruker kompetansen der den finnes uavhengig av hierarki og avdeling. På den måten vil den enkeltes kompetanse også bli en del av organisasjonens totale kompetanse, ikke bare i den avdelingen en arbeider. (Sintef report STF38 A 04403, 2004)

5.6 Hvorfor oppstår feil?

Til tross for både rutine og gode holdninger vil en aldri helt kunne sikre seg mot at det oppstår tekniske svikt eller at mennesker gjør feil. I denne delen av kapittelet trekker jeg fram noen momenter som kan være årsak til at det gjøres feil, og hvordan en kan redusere de.

Reason beskriver hvorfor det skjer feil. Han benytter metaforen swiss-cheese (Reason 1997 s. 12). Med denne viser han at det i alle sikkerhetssystemer vil kunne forekomme hull som kan medføre at det likevel oppstår feil. Selv der en etablerer flere sikkerhetssystemer som overlapper hverandre kan alle svikte samtidig.
Årsaken til dette kan være mange. Reason (Reason 1997 s. 223) hevder at mellom 80 – 95 % av alle feil skyldes menneskelig svikt på en eller annen måte. Innenfor helsesektoren er mennesket den viktigste resurs, og viktigste faktor for å hindre at det oppstår feil.
I Arbeidsmiljøloven er det satt begrensninger på hvor lenge en ansatt kan jobbe

sammenhengende. Dette er ikke bare ut i fra den ansattes ønske om fritid, men også for å hindre at en mister konsentrasjonen fordi en blir trøtt eller sliten. Ukonsentrerte ansatte gjør lettere feil. Dette gjelder også den som skal kontrollere at det ikke oppstår feil.
Manglende kompetanse kan medføre at det skjer feil. Ansatte som ikke har fått nødvendig opplæring vil fort kunne forårsake uhell fordi de ikke hadde nok kjennskap til det som skulle gjøres.
I noen tilfeller kan også sabotasje forekomme, men dette vil forhåpentligvis være lite aktuelt i en kommune.



I en organisasjon kan det oppstå uenighet. Denne uenigheten kan også handle om at de ansatte har forskjellig oppfating av sikkerheten, og derfor ikke er oppmerksomme nok slik at det oppstår feil.

5.7 Subkulturer som jobber med eller i mot

I de fleste organisasjoner vil det ikke bare oppstå en kultur, men flere. Disse kalles subkultur, delkultur eller underkultur. Det som ofte er særtrekket for en subkultur er at den gjelder bare for deler av organisasjonen.
Henning Bang henviser i sin bok Organisasjonskultur (Bang 1988 s. 30) til Van Naanen og Berly definisjon på subkultur:
"en undergruppe av organisasjonens medlemmer som samhandler jevnlig med hverandre, som identifiserer seg selv som en distinkt gruppe i organisasjonen, som deler et sett av problemer som de fleste i gruppa er enige om er problematiske, og som rutinemessig handler

på grunnlag av gruppens unike kollektive virkelighetsoppfattelse"

Som det fremkommer av denne definisjonen har en subkultur mange av de samme egenskaper som en organisasjonskultur, men skiller seg ved at de oppstår som tydelig gruppesammensatt på bakgrunn av en felles virkelighetsforståelse og hva som er problematisk. I organisasjoner kan en subkulturene være avdelinger i organisasjonen. Det kan også være bestemte yrkesgrupper som leger eller sykepleiere, som på tvers av avdelinger har etablert seg som en felles gruppe.

Subkultur kan ha stor innvirkning på kommunens kultur ved at den klarer å påvirke de beslutninger som tas. Dette kan for eksempel skje der subkulturene består av personer som har en kompetanse kommunen er avhengig av, og ved trusler om å slutte kan de presse igjennom avgjørelser. Der det er mange sterke kulturer og disse har forsjellige interesser kan dette medføre at kommunen får problemer med å nå sine overordnede mål. Konfliktene kan når de får lov til å utvikle seg medføre at sikkerhetsarbeidet ikke varetas, fordi en er mer oppatt av og argumentere mot hverandre.

Bang nevner flere type konflikter som kan oppstå mellom kulturer. Jeg tar for meg tre typer konflikter som kan få innvirkning på det å utvikle gode rutiner for personvern.

5.7.1 Konflikt mellom vertikale sjikt

Tradisjonelt i norsk arbeidsliv har det i perioder vært konflikt mellom ledelse og ansatte. Den vanligste konflikten handler ofte om lønn og arbeidstid, men det kan også være en opplevelse av at lederne ikke forstår hvordan de som jobber med brukerne, pasientene eller elevene har det. Lederne bare pålegger de mer og mer oppgaver uten at den medfører flere resurser. Innføring av dataprogrammer kan være en slik oppgave mange ansatte føler de ble pålagt uten at det medførte flere resurser. Bruken av data oppleves kun som en merbelastning som tar arbeidet vekk fra det de egentlig skulle ha gjort. Irritasjon over å bli pålagt noe en egentlig ikke ønsker, og som i tillegg medfører mer arbeid kan bidra til at en ikke har nok fokus på sikkerhet. (Bang 1988 s. 34)

5.7.2 Konflikt mellom yrkes- eller profesjonsgrupper

Kommunene består av ansatte med forskjellige utdannelsesbakgrunn og arbeidsoppgaver. En vil finne ansatte med bare grunnskole til de med hovedfag/master eller embetseksamen.

Innefor helse og omsorg har det i lang tid vært diskusjon om forholdet mellom de forskjellige yrkesgruppene. Tradisjonelt er helsesektoren hierarkisk bygget opp. De forskjellige gruppene vil ha forskjellige oppgaver og myndighet. Det kan oppstå uenighet om hva dette skal innebære, og ikke minst hvem som skal definere det. Innenfor personvern kan dette handle om hvem som skal kunne legge inn og lese opplysninger i fagprogram. De fleste yrkesgrupper har en stolthet for eget fag, og vil ikke uten videre gå med på at andre kan det bedre, eller skal fortelle dem hvordan ting skal gjøres. (Bang 1988 s. 35)

5.7.3 Konflikt mellom avdelinger

En kommune består av mange avdelinger med forskjellige oppgaver. De forskjellige avdelingene vil naturlig nok være mest opptatt av sin egen funksjon. Når andre begynner å stille spørsmål eller krav i forhold til hvordan oppgavene utføres kan dette føre til motsetninger, eller i verste fall konflikter. Det kan også her oppstå uenighet om hvem som skal ha tilgang til hvilke pasienter i fagsystemet og hvem som skal få lese hvilke opplysinger. En avdeling kan vurdere at noen pasientopplysninger kun skal være tilgjengelig hos dem. Mangel på opplysninger kan medføre at en annen avdeling ikke får nok opplysninger til å ivareta forsvarlig behandling. Dette kan være opplysninger om spesielle sykdommer eller allergier, som om det ikke gir videre kan medføre fare for den enkelte pasient. Det kan også være opplysninger om livssyn, familie og andre sosiale forhold som det er viktig for den enkelte pasient blir ivaretatt på en riktig måte. (Bang 1988 s. 33)

5.7.4 Motsetninger ikke bare negativt

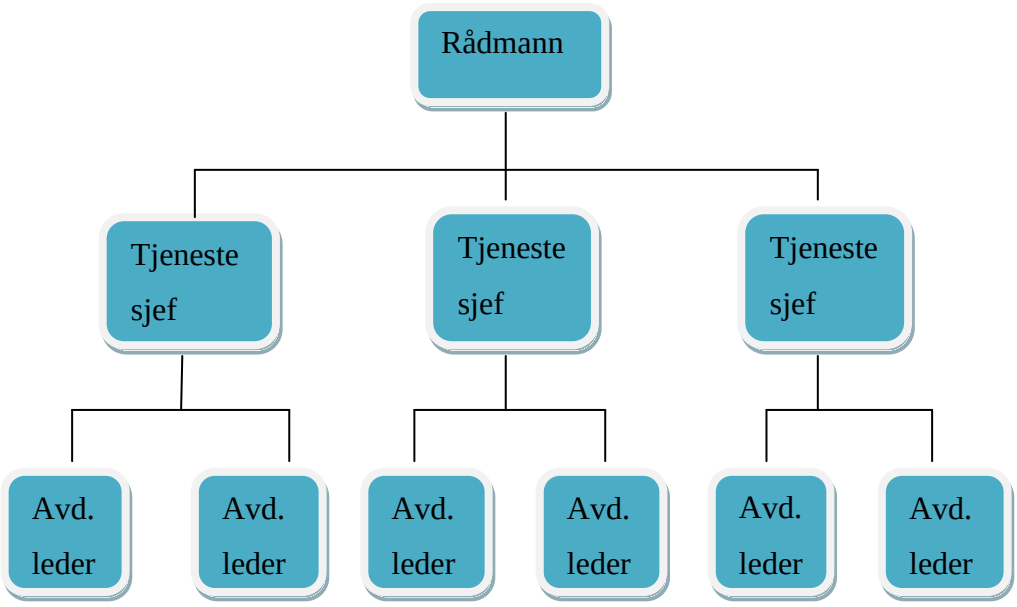
I utgangspunket vil en kunne anta at kulturkonflikter kun er negativt. Flere har påpekt at en organisasjon uten motsetninger er en død organisasjon. Det å se på konflikter bare som negativt er et for enkelt bilde. Alle organisasjoner er avhengig av motsetninger og konflikter for å utvikle seg. Det er graden av konflikten som avgjør om den er positiv eller negativ, og organisasjonens evne til å takle konflikter. Dette handler igjen om hvilken kultur en har i organisasjonen.

5.8 Hierarki et hinder for sikkerhet?

En norsk kommune er organisert etter et tradisjonelt hierarkisk system. Den daglige driften styres av en rådmann som er ansatt av kommunestyret. (Med unntak av bykommuner som har

parlamentarisk styre.)
Under rådmannen er det oftest minimum to ledernivåer. Hvordan dette er organisert vil variere fra kommune til kommune.

Under vises et forenklet organisasjonskart for en kommune.



I følge personopplysningsforskriften § 2-3 er det den daglige ledelsen i virksomheten som har ansvaret for at bestemmelsene i personopplysningsforskriftene overholdes. Denne personen vil i kommunen være rådmann.

Kommunene er inndelt i forskjellige avdelinger ut fra hvilke tjenester de skal yte. I hovedtrekk kan de deles inn i to hovedgrupper:

1. De som yter tjenester ut til befolkningen som: barnehager, barnevern, skoler, omsorg, helse, NAV, kultur m.m. Det er i disse avdelingene med unntak av kultur og tekniske tjenester det meste av lagring og behandling av sensitive opplysninger skjer. Det er også her en benytter de forskjellige fagsystemene hvor sensitive opplysninger lagres.
2. Intern støtte. Yter bistand til de andre avdelingene. Dette vil være: personal, arkiv, økonomi og IT-avdelingen. I disse avdelingene skjer det lite eller ingen form for behandling av sensitive opplysninger. Der det kan forkomme er i personalavdelingen i

forbindelse med sykdom hos ansatte. I arkiv og dataavdelingen vil de ha ansvar for at opplysninger lagres på en sikker måte, men ikke foreta noen behandling av dem.

En norsk kommune kan betegnes som en top – down organisasjon. Beslutninger blir fattet øverst i organisasjonen og gjennomført nedover, dette kan føre til at de som arbeider med pasienter har liten påvirkning på de beslutninger som blir tatt innenfor personvern.
HRO teorien understreker viktigheten av desentralisert styring og en organisasjon som er i stand til å handle raskt. I tillegg er HRO teorien oppatt av at personer innefor organisasjonen skal ha forskjellig kompetanse. I kommunene består ofte avdelingene av personer med samme fagbakgrunn. Skolen består av pedagoger, helse av helsepersonell o.s.v. Ut fra HRO teorien kan det stilles spørsmål ved om kommunene med sin hierarkiske og klare sektorinndeling klarer å etablere gode rutiner for personvern bl.a. fordi avdelingene er for like i sin sammensetning av personell, og det er lang avstand fra der avgjørelsene blir tatt til de som utfører tjenestene.

5.9 Forventninger til kommunene

I høringsforslag til ny forskrift om informasjonssikkerhet, m.m understreker departementet i kap. 4.1.3 at helsetjenesten er helt avhengig av at pasienten har tillit til at helsetjenesten behandler sensitive pasientopplysninger, slik at de ikke kommer i hendene på uvedkommende. Samtidig skal opplysningene være tilgjengelig for helsepersonell som skal gi helsetjeneste i kommunen.
I 2009 kom St.meld. nr. 47 (2008-2009) Samhandlingsreformen Rett behandling – på rett sted – til rett tid. Her står det blant annet:

"Ny framtidig kommunerolle
Kommunenes rolle i den samlede helse- og omsorgspolitikken vurderes endret slik at de i større grad enn i dag kan oppfylle ambisjonene om forebygging og innsats i sykdomsforløpenes tidlige faser. Kommuner med større kompetanse for helse- og omsorgstjenesten gis også bedre forutsetninger for å svare på kravene fra pasienter med kroniske sykdommer."

Videre i St.meld. nr. 47 (2008-2009) kap. 14 tas fremtidig bruk av IT opp. Her understrekes det at IT vil bli et viktig middel for å bedre pasientenes tilbud. Ikke bare i selve behandlingen,

men også som et virkemiddel i å informere bade pasientene og pårørende.
Er kommunene i stand til å møte den utviklingen som vil komme?

I Norge er det 429 kommuner. Den største er Oslo med over 599 230 innbyggere 01.01.2011 (www.Oslo.kommune.no) og den minste er Utsira som hadde 211 innbyggere 01.01.2011(www.Utsira.Kommune.no). Til tross for store forskjeller i både antall innbyggere og areal skal norske kommuner ivareta de samme lovpålagte tjenestene ovenfor sine innbyggere. Det stilles også de samme krav til kvalitet og sikkerhet uansett hvor stor eller liten en kommune er. Innbyggerne i kommunene er avhengig av at kommunen er i stand til å ivareta deres behov.
Helse- og omsorgstjenesten i kommunen preges av mange små stillinger. Det er ikke uvanlig at ansatte kan ha stillinger ned i 10 %. Disse jobber ofte i helger og på kvelds- og nattestid, som gjør at de har liten kontakt med lederne og det som skjer i avdelingene på dagtid. Samtidig skal de ha nok kunnskap til å benytte elektronisk fagsystem. I tillegg har det innenfor helse- og omsorgstjenesten vært stor gjennomtrekk av ansatte. Jeg har selv arbeidet i virksomheter hvor det i løpet av ett år har vært en utskifting på opptill 50 %. Når det er mange små stillinger samtidig med en stor gjennomtrekk vil dette sette organisasjonen på store oppgaver når det gjelder opplæring og oppfølging av den enkelte ansatte. Kvalitet på tilbudet kan bli dårligere på grunn av manglende kontinuitet. Dette kan ramme både det rent faglige, men også sikkerhet rundt personvern.
Norsk kommuner rammes av innstramninger som medfører at en må spare og redusere tilbudet til befolkningen. Dette vil også kunne berøre sikkerhetsarbeidet. For en kommune vil det alltid være en avveining om hvilke tilbud en skal prioritere. Dette kan medføre at en velger bort sikkerhet og personvern fordi en ikke har nok resurser.

5.10 Tiltak for å ivareta sikkerhet

HRO beskriver hvilke prinsipper som må ligge til grunn for å få en sikker organisasjon og hvordan disse må prege organisasjonen, men prinsippene må fylles med innhold.

Reason beskriver to typer forsvarssystemer for å hindre feil og ulykker. Den første kaller han Soft defences som defineres som rutiner, øvelser, opplæring, holdninger, tilsyn m.m. Det andre er Hard defences. I dette ligger de fysiske forsvarsmekanismene som er låsing av dører,

alarmer, TV-overvåking, backupsystemer m.m.. Jeg har i oppgaven valgt å ha mest oppmerksomhet rundt soft defence da det er disse forsvarmekanismene de ansatte i avdelingene har mest innflytelse over.

Som tidligere beskrevet bruker Reason metaforen swiss-cheese. Her viser han at ingen sikkerhetsrutiner er helt sikre. De vil kunne svikte. For å hindre at dette skjer må det i kommunene etableres flere sikkerhetsbarrierer som overlapper hverandre. Selv om dette heller ikke kan bli 100 % sikkert, men jo flere bedre sikkerhetsbarrierer det er jo, større er muligheten for at det ikke skjer feil.

Jeg har utarbeidet en oversikt over de Hard og Soft defences som kommunen må etablere for å sikre personvernet. Oversikten er ført inn i en tabell hvor Soft defences er satt opp på den ene siden og Hard defences på den andre.

I beskrivelsene er det tatt utgangspunkt i lover og forskrifter pluss retningslinjer fra Datatilsynet som er beskrevet i kapittelet om Personvern i Norge.

Soft defences	**Hard defences**
Rutiner for datasikkerhet i organisasjonen	Rutiner for backup og sikring av data
Kontroll av opplysninger	Sikring av områder hvor det behandles og oppbevares sensitive opplysninger
Rutiner for avvikshåndtering	Eget nettverk for sensitive opplysninger
Ledelsens godkjenning av rutiner og årlig gjennomgang av sikkerheten	Oppgradering av dataprogram
Klart definert ansvarsdeling i organisasjonen	Viruskontroll, brannmurer
De ansattes og ledernes holdninger	
Risikoanalyse	
Definert akseptabelt risikonivå	
Opplæring av de som bruker systemene	
Tilgangsstyring til programmer	
Logging	
Innrapportering til Datatilsynet	
De ansattes håndtering av personvern	

5.11 Soft defences

5.11.1 Rutiner for datasikkerhet i organisasjonen

I følge Personopplysningsforskriften § 2-16 skal det foreligge dokumentasjon for hvilke rutiner som er utarbeidet og som har betydning for informasjonssikkerheten. I disse rutinene skal det foreligge dokumentasjon over at kommunen følger de lover og forskrifter som regulerer personvernet. Rutinene skal være skriftelige og godt kjent i hele kommunen. Ved endringer skal det være utarbeidet rutiner som gjør at alle endringer blir oppdatert så fort som mulig. For å unngå at det oppstår flere utgaver av samme rutine må gamle rutiner makuleres. Alle rutinene må dateres. Der rutiner er lagres elektronisk må alle gamle rutiner fjernes, eller avpubliseres når det kommer endringer.

5.11.2 Kontroll av opplysninger

Alt helsepersonell er pålagt å dokumentere (Helsepersonelloven § 39). Dokumentasjonen skal sikre at nødvendige opplysninger om pasienten er nedtegnet. Dokumentasjonen skal også foregå fortløpende. Alle dokumentasjon skal dateres og signeres av den som har registrert opplyningene. Nærmere beskrivelse av hva en journal skal inneholde er definert i Forskrift om pasientjournal § 8. Dokumentasjonen vil i kommunene i hovedsak foregå i fagsystemer. Oppstår det feil vil dette kunne få store konsekvenser som kan gå på liv og helse. Det må utarbeides rutiner som sikrer at opplysninger er riktig.
Det stilles også krav om at det skal være en som har det overordnede ansvaret for journalen (Forskrift om pasientjournal § 6) Denne personen må også ha ansvar for at de opplysningene som legges inn er korrekte og tilstrekkelige. Det skal fremkomme i journalen hvem som er ansvarlig.

5.11.3 Rutiner for avvikshåndtering

Avvikshåndteringen skal ha som hensikt og fjerne årsaken og hindre gjentagelse. (Personopplysningsforskriften § 2-6) Avvikshåndteringen skal dokumenteres i rapporter som inneholder opplysninger om selve avviket, hva som ble gjort av strakstiltak, hva som ble gjort for å rette opp avviket og evaluering av de tiltak som ble iverksatt. I tillegg skal det dokumenteres hvem som er involvert i avviket. Et godt utarbeidet avvikssystem er en forutsetning for å kunne avdekke feil og rette de opp.

(En veiledning om internkontroll og informasjonssikkerhet, Datatilsynet, 6.1)

5.11.4 Ledelsens godkjenning av rutiner

Personopplysningsforskriften § 2-3 påbeker at virksomheten ledelse har ansvar for at bestemmelsene i forskriften følges. Videre stilles det krav om at informasjonssystemene skal gjennomgås en gang i året for å kartlegge om det er hensiktsmessig i forhold til virksomhetens behov. Etter gjennomgangen skal det skrives en rapport hvor eventuelle avvik kommenteres, og det settes en dato for når avviket skal være lukket.

5.11.5 Klart definert ansvarsdeling i organisasjonen

Det er den som har det daglige ansvaret for virksomheten som har ansvaret for at bestemmelsen om informasjonssikkerhet etter Kapittel 2 i personopplysningsloven følges. Dette skal være definert og nedskrevet i rutinene. I en kommune vil det være rådmannen som har det overordnede ansvaret. I de tilfeller oppfølgingen av denne oppgaven er delegert til andre skal det være nedskrevet og gjort kjent i organisasjonen.

5.11.6 De ansatte og ledernes holdninger

Holdninger kan ikke vedtas, de er heller ikke definert i lovverk. Holdninger må skapes. Som det fremkommer i HRO teorien er de ansattes evne og vilje til sikkerhet viktig. Selv om kommunene har nedskrevne rutiner, og følger de krav som settes vil det alltid være de ansattes holdninger som avgjør om dette fungerer og er levende i organisasjonen. Holdninger skapes ikke av seg selv. Det må jobbes aktivt for at disse skal oppstå og videreutvikles. Noen må ta ansvar for at dette skjer.

5.11.7 Risiko analyse

Det skal gjennomføres risikovurderinger for å kartlegge hvor sannsynlig det at det oppstår feil, og hvilke konsekvenser feilen vil få både for driften og pasientene.
En risiko og sårbarhetsanalyse defineres som en systematisk identifisering og kategorisering av risiko, som skal være til hjelp for å kartlegge behov for tiltak, og hvordan forskjellige virkemidler og løsninger kan føre til at en når ønsket målsetning.
(Alven, Boyesen, Njå, Olsen og Sandve 2004 s.31)
Resultatet skal dokumenteres. Ved endringer av driften som kan få påvirkning på sikkerhet

skal det foretas en ny vurdering. (Personopplysningsforskriften § 2-4)
Endinger i en kommune vil være når en innfører nye dataprogrammer eller foretar en omorganisering hvor ansvarsfoldene endres enten ved at en slår sammen avdelinger, eller deler den opp.

5.11.8 Definert akseptabelt risikonivå

I HRO blir det hevdet at det er mulig å utvikle en organisasjon hvor en kan forebygge ulykker. De fleste vil hevde at dette er svært krevende, om ikke umulig. I en kommune med begrensede midler vil en ikke kunne klare å forhindre alle feil eller ulykker. Samtidig er det viktig at en definer hvilke feil som ikke kan aksepteres, fordi det kan medføre for store konsekvenser. For en kommune vil dette først og fremst være feil som får konsekvenser for liv og helse.
Det å fastsette nivået på risikoen er et ledelsesansvar. (§ 2-4 personopplysningsforskriften.) Ledelsen i en organisasjon står ikke fritt til selv å bestemme nivået for risiko. De er forpliktet til å følge gjeldende lover og forskrifter.
For å sikre at en har et akseptabelt risikonivå må det foretas en risiko- og sårbarhetsanalyse.

5.11.9 Opplæring av de som bruker systemene

Det stilles krav om at de som skal få tilgang til personopplysninger skal ha fått nødvendig opplæring før tilgang gis. Opplæringen skal sikre at de ansatte har nok kunnskap slik at de kan bruke dataprogrammene på riktig og sikker måte. I tillegg må det gis opplæring i hva som skal legges inn av opplysninger. Ved endringer av programmer som følge av oppgardering, eller endringer av hvilke opplysninger som skal lagres, må det gis ny opplæring.
I høringsforslag til ny forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre blir kravet til opplæring understreket i § 12.

5.11.10 Tilgangsstyring til programmer

Hvordan gis tilgangen til datasystemene? Kan den enkelte ansatte selv be om å få tilganger, eller er det utarbeidet rutiner for godkjenning før det gis tilganger og hvem er det i tilfelle som gir dette?
"Helsepersonell som yter helsehjelp til pasient, har bare tilgang til helseopplysninger som er

nødvendig og relevant for å kunne yte helsehjelp til pasienten," (Høringsforslag til ny forskrift om informasjonssikkerhet, tilgangsstyring m.m. § 19, 1. ledd)
Tilgangsstyring handler ikke bare om hvilke programmer den enkelte ansatte skal kunne logge seg inn på, men like mye hva en skal kunne utføre og hvilke opplysninger en skal kunne lese.
Det er den enkelte leder som skal definer hvilken tilgang som skal gis, men det bør være like rutiner for hele kommunen. Det må også være en rutine som sikrer at ansatte som slutter ikke lenger har tilgang.

5.11.11 Logging

All bruk av fagsystemer skal logges. I følge Datatilsynets veileder om internkontroll og informasjonssikkerhet (5.8.3) er virksomheten pålagt å logge all bruk. Hensikten er å sikre at ikke uvedkommende kommer seg inn på sensitive opplysninger de ikke har tilgang til, eller foretar noe ulovlig.

I høringsforslag til ny forskrift om informasjonssikkerhet, tilgangsstyring m.m.(§ 32) kommer departementet med forslag om at følgende opplysninger skal logges:

a) entydig identifikasjon av den som har fått tilgang. Dette forutsetter at det kun gis personlige tilganger med egen id og passord

b) stedet hvor vedkommende har vært pålogget fra. Har må ip-adressen til den maskinen som benyttes registreres

c) referanse til de opplysninger det er gitt tilgang til. Hensikten er å se at den enkelte ikke har større tilganger enn det en trenge for å utføre jobben

d) hvilke systemer vedkommende har benyttet mens han eller hun var pålogget

e) det tidspunkete vedkommende har hatt tilgang til opplysninger

f) Bruk av informasjonssystemer som er i strid med fastsatte rutiner skal behandles som avvik.

Skal logging ha en hensikt må den brukes. Det vil være vanskelig kun å benytte den ved mistanke da det er vanskelig og definere hva mistanke er. Velger en å gå igjennom alle ved

faste tidspunkt er det lettere å avdekke missbruk og alle stiller likt. Dette er også i tråd med Datatilsynet syn.
Det er en forutsetning at dette er kjent blant de ansatte, og at alle nyansette får informasjon før de får tilgang.

5.11.12 Innrapportering til Datatilsynet

Som tidligere nevnt skal kommunen i følge Personopplysningsloven § 31 sende inn opplysninger til Datatilsynet om hvilke opplysninger de lagrer og behandler i kommunen. Bakgrunnen er at en skal dokumentere at kommunen ikke behandler andre en de opplysningene en trenger for å ivareta de oppgavene en er pålagt. Det skal også være mulig for befolkningen å få kunnskap om hvilke opplysninger en kommune behandler.

I følge § 7 – 12 i Personopplysningsforskriften kan kommunene søke Datatilsynet om å få opprette personvernombud. En slipper da og melde inn til Datatilsynet, men personvernombudet skal ha oversikten over hvilke opplysninger som blir behandlet i kommunen og kunne legge de fram om de blir etterspurt.

5.12 Hard defences

5.12.1 Rutiner for backup og sikring av data

Datatilsynet stiller krav om at det daglig skal tas backup av alle data, og at disse skal oppbevares på et sikkert sted. Dette er spesifisert i Norm for informasjonssikkerhet pk. 5.5.3 Tilgjengelighet s.22 ***:*** *”Virksomhetens ledelse skal for øvrig sørge for sikkerhetskopiering av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk. Sikkerhetskopier skal oppbevares avlåst og brannsikret, og adskilt fra driftsutstyret. Det skal jevnlig foretas test av at sikkerhetskopiene er korrekte og kan tilbakeføres”.*
Opplysninger kan forsvinne eller bli slettet. Skulle opplysninger forsvinne vil det kunne medføre uante konsekvenser. Gode backupsystemer er en forutsetning for at kommuner skal kunne ivareta sikkerheten og opprettholde forsvarlig drift. Backup må tas med faste intervaller og det er vanlig at en i kommuner tar det minst en gang i døgnet for ikke å miste mer enn en

dags arbeid.

5.12.2 Sikring av områder hvor det behandles og oppbevares sensitive opplysninger

"*Adgang til lokaler og utstyr hvor personopplysninger behandles skal kontrolleres. Det gjelder spesielle sikringstiltak der hvor det behandles sensitive personopplysninger eller der man har informasjon om sikring av slike opplysninger*." (Veiledning i informasjonssikkerhet for kommuner og fylker s. 24)

Serverrommet vil være hjerte for datasystemene. Det er her data behandles og opplysninger lagres. Kommer det uvedkommende inn og denne personen har uhedelige hensikter, eller er veldig klåfingret vil det kunne medføre store skader. I alle kommuner skal tilgangen til serverrommet begrenset slik at bare autorisert personell har tilgang. Det er kun ansatte i IT-avdelingen som skal ha tilgang og kjenne til rutinene.

Til tross for at en har backup vil ødeleggelse av servere enten det skyldes sabotasje, brann, overoppheting eller vannskade medføre store konsekvenser. I en undersøkelse som ble gjort i en kommune, ikke en av de som det ble foretatt intervju i, ville en ødeleggelse av hele serverrommet føre til at en ville trenge ca. 4 uker på å få lagt inn all data igjen. Største problemet ville være å skaffe tilveie nye maskiner og servere fordi det meste ikke er på lager i Norge og måtte bestilles fra utlandet. En vil også bruke lang tid på å få lagt tilbake alle data. Det å drive en kommune uten å ha tilgang til elektroniske data sier seg selv vil være svært krevende.

En måte å løse dette på er å ha to like serverrom som speiler hverandre. Det vil si at data lagres samtidig i begge serverrom. Skulle det ene falle ut vil en fortsatt ha full tilgang. Dette forutsetter selvfølgelig at det er god avstand mellom rommene. Det finnes i dag også andre type løsninger hvor en kan leie seg ekstra maskinvare. Problemet her som så ofte ellers innenfor kommunal virksomhet er økonomi. Det blir en vurdering av kost og nytte.

De fleste kommuner velger derfor å beskytte serverrommet best mulig med alarmer og brannslokningsutstyr.

Så langt er ingen kommuner meg bekjent vært utsatt for brann eller vannlekkasje som har fått store konsekvenser. Det er derfor lett å velge den enkleste løsningen.

I tillegg kan lengre strømstans medføre at livsviktige opplysinger ikke er tilgjengelig. Eneste måte å løse dette på er ved å ha aggregater.

Siden dette punktet berører tekniske løsninger som de ansatte i helse- og omsorgstjenesten i utgangspunktet ikke skal ha inngående kjennskap til er det ikke tatt med i undersøkelsen.

5.12.3 Eget nettverk for sensitive opplysninger

Datatilsynet stiller krav om at sensitive opplysninger skal lagres og behandles i et lokket nettverk (sikker sone), og som ikke har tilgang til kommunens øvrige nett eller internett. (Veiledning i informasjonssikkerhet for kommuner og fylker s. 25.) Dette for å hindre at sensitive opplysninger ved feil blir lagt ut på nettet, eller at noen kan hacke seg inn.
Det skal kun være autorisert personell som har tilgang til sikkert nettverket, og alle som logger seg inn skal gjøre det med personlig brukernavn og passord. Det skal ikke være mulig å kopiere opplysninger fra sikkert nettverk til internet eller kommunes ordinære nettverk.
Alle skrivere skal være koblet opp mot sikkert nettverk og det skal ikke være mulig å skrive ut på skrivere som ikke er sikret.

5.12.4 Oppgradering av dataprogram

Alle dataprogrammer trenger oppdateringer. Ingen dataprogram er ferdige når de slippes ut på markede. Enten det er operativsystemer eller fagprogrammer. Grunnen er at en etter en tids drift oppdages feil som en ikke oppdaget under utvikling. Programmer blir også utsatt for virus. Oppdatering er en forutsetning for å beskytte seg mot nye former for virus.
Kommunene må ha rutiner som sikrer at dette skjer og at det gjøres av personer som både kjenner programmet og har gode datakunnskaper. Feil oppgradering kan medføre at programmer slutter å virke, opplysninger forsvinner eller det ikke er mulig å legge inn nye opplysninger. Det må også være rutiner for å kontrollere at programmene fungerer før de settes i drift.

5.12.5 Viruskontroll

Problemet med virus øker. Stadig kommer det nye virus som om de får operere fritt kan gjøre stor skade. Det stilles krav om at kommunen har gode rutiner for å beskytte seg mot virus. (Veiledning i informasjonssikkerhet for kommuner og fylker s. 29.) Eneste måten å gjøre det på er og ha gode virusprogram som oppdateres kontinuerlig i tillegg til oppgradering av andre program. De fleste programmer gjør dette nå automatisk, men det må være kontroll med at det

fungere slik det skal. I tillegg må det være brannmurer som hindrer at noen uvedkommende kan komme seg inn på nettverket.

5.13 Oppsummering

Norske kommuner har i de siste årene opplevd store endringer. Selv om kravene til både dokumentasjon og bruken av elektroniske informasjon har endret seg drastisk, er det lite som har endret seg i hvordan en kommune er organisert.
Spørsmålet blir om kommunene slik de er organisert i dag er i stand til å ivareta dagens behov. Eller like viktig, hvordan klarer en å møte de utfordringer som en vet vil komme innenfor bruken av elektroniske hjelpemidler. Blir de ansatte satt i stand til å bruke de nye hjelpemidler og kommunikasjonsmidler slik at tjenestene blir bedre, eller er innføring av ny teknologi med på å øke risikoen for at det oppstår feil.
Reasom viser til to typer forsvarsmekanismer hard soft og defences. For å ivareta personvern i kommunene er det nødvendig med begge deler. Den ene handler om å bygge opp fysiske forsvarsmekanismer, mens den andre handler om rutiner, øvelser og holdninger. I de fleste kommuner vil det stort sett være enklere å etablere hard defences enn soft defences. Grunnen er at det kan være lettere og skape forståelse for hvorfor en trenger backupsystemer, enn at det er behov for rutiner og øvelser. Hard defences er også lettere og administrere da det ofte handler om tekniske løsninger, mens soft defences handler mer om de ansattes holdninger og kunnskap. Kommunenes viktigste resurs er mennesker. Det er mennesker som utfører tjenestene ut til befolkningen enten det er i skole, barnehage eller helse og omsorg. Der det er mennesker sammen over tid oppstår det kulturer som kan ha innvirkning på hvordan arbeidet utføres. Er disse kulturene med på fremme sikkerheten? I HRO understrekes det at det ikke bare må være systemer som fanger opp når det skjer feil, men like viktig er de ansattes holding til sikkerhet, og evne til å oppdage svakheter i systemet før feil oppstår og evne til å lære av de erfaringer en gjør.
Kommuner har som målsetning å unngå at det oppstår feil, men det holder ikke bare å ønske. Det krever at en gjør noe bevisst for å unngå at det skjer feil. I denne undersøkelsen ønsker jeg å se hva kommunene gjør og hvilken holdning, og kunnskap de ansatte har til problemstillingen.

6 Metode

I denne undersøkelsen har hensikten vært å finne ut hvor godt kommuner ivaretar personvernet. Bakgrunnen for undersøkelsen var de opplysninger som har kommet fram både i media, og gjennom Datatilsynets tilsyn med kommunene, som viste at de ikke hadde gode nok rutiner for å ivareta personvernet. Min hypotese er at kommunene ikke er i stand til å ivareta personvernet på en sikker måte. Gjennom undersøkelsen har det vært et ønske å finne ut om dette stemmer, og hva som må gjøres for at dette kan gjøres bedre.

6.1 Case studie

Min undersøkelse er en Case- studie *"Case kommer av det latinske ordet casus som understreker betydningen av det enkelte tilfelle. [….]Termologien vektlegger derfor at det dreier seg om ett eller noen få tilfeller som gjøres til gjenstand for inngående studier."* (Andersen s. 8-9, hentet fra Jacobsen 2005 s.90)
Her er det sentralt og definere hva undersøkelsesenheten er. Dette er den enheten en ønsker å undersøke. I denne undersøkelsen er undersøkelsesenheten åtte ansatte i fire kommuner som alle arbeider innenfor helse og omsorgstjenestenes. Det som er undersøkt er hvordan informantene forholder seg til personvernet i sitt daglige arbeid.

6.2 Datakilder

Oppgaven består av både primære og sekundære datakilder. Primærdata er de data som forskeren selv henter inn og hvor en går direkte til kilden. Informasjon hentes inn enten ved intervjuer, observasjon eller spørreskjema og er skreddersydd for undersøkelsen. Sekundærdata er informasjon som er samlet av andre. Her kan informasjonen være samlet inn til et annet formål eller en annen problemstilling enn den forskeren selv undersøker. (Jacobsen 2005 s.137)
I denne undersøkelsen er primærdata intervjuer med informanter som daglig arbeider innenfor den kommunehelsetjeneste, og som behandler sensitive opplysninger.

Sekundærdata er opplysninger som er hentet fra massemedia og Datatilsynet. Disse dannet grunnlaget for hypotesen.

6.3 Gjennomføringen av undersøkelsen

Den empiriske delen av oppgaven ble gjennomført som en kvalitativ undersøkelse ved intervju med personer som daglig jobber med sensitive opplysninger.
Det ble foretatt individuelle intervjuer. Denne type intervjuer er preget av at innhenting av data foregår i en dialog og informasjonen kommer som ord, setninger og fortellinger. Som oftest foregår intervjuene ansikt til ansikt, men det kan også skje via telefon. (Jacobsen s.137)
Grunnen til at jeg valgte ansikt til ansikt er først og fremst at det er lettere å få til en god "tone" i intervjuet når en ser hverandre og har foretatt noe småprating på forhånd. Telefonintervjuet kan oppleves mer stivt og formelt.
Selve undersøkelsen ble gjennomført som et pre-strukturert intervju. Pre-strukturert intervju blir definert som intervjuer hvor en på forhånd har definert noen områder som en konsentrer seg om. Graden av struktur kan variere fra helt lukket hvor det er faste svaralternativer til helt åpne hvor det ikke er utarbeidet noen intervjuguid. (Jacobsen 2005 s.144)
I denne undersøkelsen var det utarbeidet en intervjuguid, men guiden ble ikke fulgt slavisk, og fungerte mest som en huskeliste for hvilke teama som skulle tas opp. Det var ikke utarbeidet noen svaralternativ på forhånd. Spørsmålene var stort sett de samme, men lederne fikk i tillegg spørsmål om selve organiseringen av tjenestene.
Under de to første intervjuene kom en inn på temaer som ikke var med i den opprinelige guiden. Disse ble så senere innarbeidet. Intervjuene ble tatt opp på bånd slik at det var lettere og konsentrere seg om selve intervjuet.
Etter at intervjuene var gjennomført ble hvert intervju skrevet ut. Det ble så utarbeidet en matrise hvor alle svarene fra de forskjellige ble satt opp mot hverandre. Dette ga en god oversikt over likheter og forskjeller på svarene.

6.4 Utvelgelse av intervjuobjektene

I utvelgelsen av intervjuobjekter ble det lagt vekt på å intervjue ansatte som til daglig arbeidet med pasienter. Grunnen var et ønske om å se hvor kjent de var med personvern og hvordan det ble praktiser i det daglige arbeidet. Ved å velge både en avdelingsleder og en ansatt uten lederoppgaver ønsket jeg å se om det var forskjell mellom den som ledet avdelingen og de som var ansatt i avdelingene.
Alle var ansatt i den kommunale helsetjenesten. Der ble foretatt intervju med åtte personer

fordelt på fire kommuner. I hver kommune er det intervjuet en avdelingsleder og en ansatt som arbeidet med pasienter. Alle som ble intervjuet var utdannet sykepleiere. I noen kommuner arbeider de som ble intervjuet i samme avdeling. Det er intervjuet både personer fra sykehjem og hjemmetjeneste.
Intervjuene var avtalt på forhånd og ble foretatt på den enkeltes arbeidsplass i et eget rom uten andre til stede. Intervjuene ble foretatt på den enkeltes arbeidsplass fordi dette var enklere for de som ble intervjuet.
Alle svarene ble behandlet anonymt både navn og hvilken kommune den enkelte er ansatt i. Grunnen er at en kan forvente mer ærlige svar enn om det ikke hadde vært anonyme. Kommunene er i Rogaland, men størrelsen varierte fra en av de minste til en av de største. Ved at det er så stor forskjell på størrelsen på kommunene ønsket jeg å se om det var forskjell på svarene fra en liten kommune til en stor. Alle kommunene har innført dataprogram for helse- og omsorgstjenesten. Flere av kommunene har over ti års erfaring med programmene, og de ansatte bør være vant til å benytte elektronisk dokumentasjon.

I kapitelet omtales avdelingslederne som leder og de ansatte i avdelingene som ansatt.

Betegnelsen pasient er benyttet da denne er mest benyttet innenfor helsetjenesten.

6.5 Validitet og reliabilitet

Sentralt i all forskning står begrepene validitet (gyldighet og relevans) og reliabilitet (pålitelighet og troverdighet)

Med validitet menes at en faktisk måler det en ønsker å måle, at det som måles er relevant og at det som er målt hos noen også gjelder for andre. I denne sammenheng vil det innebære at den undersøkelsen som er foretatt i fire kommuner også kan sies og gjelde for andre, eller sier undersøkelsen bare hvordan de som ble intervjuet opplevde situasjonen? (Jacobsen s.19)
I denne undersøkelsen er validiteten ivaretatt ved at det er valgt fire forskjellige kommuner. Alle de som ble intervjuet jobbet daglig med personvern og alle hadde vært ansatte i flere år og kjente fagområdet godt. Alle var også utdannet sykepleiere og har ut fra sin utdannelse en faglig bakgrunn til å vurdere problemstillingen.

Med reliabilitet menes at undersøkelsen er å stole på og er gjennomført på en troverdig måte. Dette ble forsøkt ivaretatt ved at alle intervjuene ble foretatt anonymt i eget rom uten andre tilstede. Det kan selvfølgelig stilles spørsmål ved om informantene hadde svart det samme ved en ny undersøkelse. Dette kan en ikke være helt sikker på uten å foreta en ny undersøkelse. (Jacobsen 2005 s.20)

7 Empiri og drøfting

7.1 Innledning

I dette kapittelet vil jeg gå igjennom funnene i undersøkelsen og drøfte det som er kommet fram ved og sette det opp mot de krav som stilles i lovverket. I drøftingen tar jeg utgangspunkt i de hard og soft defences områdene som er beskrevet i teorikapittelet. Jeg vil også se på om funnene i denne undersøkelsen stemmer overens med funnene som er gjort av Datatilsynet.

Ut fra de teoriene som er beskrevet i teorikapittelet vil jeg prøve å analysere hvorfor situasjonen er som den er, og hvilke tiltak som må iverksettes for å få til bedre sikkerhet.

Det er fra Regjering og Datatilsynet utarbeidet til dels detaljerte bestemmelse på hvordan en skal sikre personopplysninger. Lov om personregister m.m. kom allerede i 1978. Loven ble senere erstattet av personopplysningsloven. Det er i tillegg kommet forskrifter, veiledere m.m. (Det er nærmere beskrevet i kapittelet Personvern i Norge.) Kravene om personvern burte derfor være godt kjent blant de som arbeider med personopplysninger.

I gjennomgang av funnene har jeg prøvd å foreta rangering av hvilke funn som får størst konsekvenser for personvernet i kommunen. Da undersøkelsen har hatt mest fokus på soft defences er dette beskrevet først. Selv om hard deences også er like viktig for å sikre personvernet, tror jeg at den største utfordringen ligger i å endre de ansattes og dermed kommunens holdninger.

7.2 Rutiner for datasikkerhet

Det som var mest karakteristisk ved undersøkelsen var mangel på skriftelige rutiner.
Noen ledere visste at kommunen ikke hadde egen rutine for datasikkerhet, mens andre ikke hadde kjennskap til om det var utarbeidet. Svarene var de samme for de ansatte. Flere var sikre på at rutiner fantes et sted, men de hadde ikke sett dem. En kommune hadde rutine for at alle måtte logge seg ut av datamaskinen når de var ferdig eller forlot rommet, men ikke noe utover det. I en kommune henviste de til en perm med manualer for fagprogrammet. De var temmelig sikre på at det lå noen rutiner om personvern i permen, men de hadde ikke selv sett dem. En av kommunene var i ferd med å utarbeide rutiner.

De fleste henvist til at alle ansatte måtte underskrive taushetserklæring når de begynte og at mye av personvernet var ivaretatt med det. Flere henviste også til at som sykepleiere hadde de taushetsplikt som var knyttet opp til den offentlige godkjenningen.
Det stemmer at alle som arbeider innefor helsevernet er pålagt taushetsplikt. Denne skal underskrives før en begynner i arbeidet. I tillegg har alle som har en offentlig godkjent helseutdannelse taushetsplikt gjennom sin profesjon jf. Lov om helsepersonell m.v. kapittel 5. Denne loven beskriver kun hva taushetsplikten innbærer og hvilke unntak som finnes. Den sier ingen ting om hvilke rutiner som skal ivaretas, eller hvordan en skal sikre seg mot at opplysninger kommer på avveie eller er feil.

Som beskrevet under kapittelet om soft defence stilles det krav om at det skal utarbeides rutiner for datasikkerhet kommunene. Disse rutinene skal ikke bare beskrive hvordan en skal sikre at personvernet ivaretas, men i tillegg skal en dokumentere at kommunen holder seg innenfor de krav som stilles i lover og forskrifter. Som tidligere beskrevet er det ikke opp til hver enkelt kommune og starte opp med å registrere personopplysninger. Det må være forankret i lov før dette kan gjøres. Samtidig skal de som blir registrert bli informert om hvilke opplysninger som lagres og gi sitt samtykke til at dette gjøres. Alle har rett til å nekte at opplysninger blir lagret, men de må da bli orientert om hvilke konsekvenser dette kan medføre. I tillegg har alle fullt innsyn i de opplysninger som er lagret om den. Hvordan dette skal ivaretas skal være nedskrevet og kjent for både de som søker hjelp og for de ansatte som legger inn opplysninger.
Det stilles også krav om at det ikke skal registreres opplysninger som ikke er nødvendig eller som ikke har noen hensikt for den behandling som skal foretas. For å sikre at dette skjer må det være rutine som forteller hvilke opplysninger som skal inn i systemet og hvem som har

ansvar for at de legges inn. I tillegg må rutinene hindre at sensitive opplysinger blir lagret i usikre medier. I dag finnes det utallige former for lagringsmeier som cd, minnepenner, mobiltelefoner, laptop m.m. Alle disse gjør det enkelt å ta med seg til dels store datamengder uten problemer. I de tilfeller sensitive opplysninger skal oppbevares eller behandles i bærbare lagringsenheter må date krypteres. Dette understrekes flere ganger i Veiledning i informasjonssikkerhet for kommuner og fylker, at data som skal transporteres utenom sikker sone må krypteres.
Kommunene må ha rutiner som forplikter de ansatte til ikke å lagre personopplysinger slik at de kan komme på avveie.

I de tilsyn som Datatilsynet gjennomførte i kommunene kom det fram mange av de samme manglene. Flere kommunene manglet et helhetlig system for internkontroll. I den siste undersøkelsen som ble foretatt av Datatilsynet i 2010 og som ble publisert 15. januar 2011 svarte bare 52 % at de hadde utarbeidet internkontroll for personvern. Når Datatilsynet foretok kontrollspørsmål hos de som hadde svart ja, var det bare 7 % som fylte kravene for sikring av sensitive opplysninger. Dette er ekstremt lavt når en tar utgangspunkt i at resultatet burte vært 100 %. Det er også skremmende når en vet at alle kommunene har hatt langt tid på seg til å innføre internkontroll. Det blir viktig å spørre seg om hvordan dette kan være mulig. Svaret er sikkert ikke entydig, men mangel på kontroll av kommunene fra Datatilsynet er helt sikkert en av årsakene. Det blir viktig for Datatilsynet å se på dette og hva en kan gjøre for å få mer fokus på dette i kommunene. Diskusjonen rundt dette vil også bli tatt opp under konklusjon.

For å sikre personvernet må det være utarbeidet skriftelige rutiner som er godt kjent i hele organisasjoner. I HRO teorien understrekes det at alle i organisasjonen må være opptatt av sikkerhet. For å få dette til må rutiner være skriftelige. Rutinene skal inneholde et helhetlig internkontrollsystem som beskriver hvordan kommunen ivaretar personvernet til daglig. De må være lett tilgjengelig og skriftelige. Ved nyansettelse må de viktigste punktene deles ut og den ansatte kvittere for at en har lest de. Dette handler om å skape holdninger om at personvern er viktig.

7.3 Mangel på kontroll av opplysninger

Ingen av kommunene hadde rutiner som sikret at de opplysningene som den enkelte ansatte la inn var korrekte, med unntak av medisinkort som skal underskrives av lege. Alle som ble intervjuet, med ett unntak hadde opplevd at rapporter var skrevet på feil person. En leder som i tillegg til å være avdelingsleder også var systemansvarlig hadde flere ganger opplevd at ansatte tok kontakt for å få rettet opp feil som var skrevet i journalen da de selv ikke hadde rettigheter til å gjøre det. Flere fortalte at feilene ble oppdaget fordi en kjente personer det var skrevet om og når de leste rapporten så de at det var skrevet på feil person. Det ble også fremhevet at for ett av fagprogrammene var det en svakhet som gjorde at en lett kunne registrere opplysninger på feil person. Dette hadde de opplevd flere ganger. I følge HRO er redundans viktig for å sikre at det ikke skjer feil. Dette ser ut til å mangle totalt.

7.3.1 Kvalitet på det som registreres

Alle som ble intervjuet var opptatt av at det som ble registrert i fagprogrammene ikke bare var korrekt, men også hadde høy kvalitet. Flere ønsket å sette ekstra fokus på at de ansatte lærte seg til å skrive gode rapporter. Det kom fram at språket ofte var dårlig og en ikke fikk fram det som var viktig. Noen skrev alt for mye og tok med opplysninger om andre pasienter eller familieforhold som ikke har noe med den enkeltes situasjon å gjøre. En leder var overrasket over hvor dårlig språk mange unge hadde. ”Må lærer de å skrive norsk og ikke SMS- språk, eller bruke for fargerikt språk. Skal være et nøkternt språk, ikke bruke mange utropstegn, smilefjes og lignende”.

En nevnte også at fordi flere ansatte ikke kommer fra Norge behersker de språket dårlig og klarer ikke å oppfatte alt som sies og er ikke i stand til og dokumenter.

Det ble også fremhevet at opplysningene ikke bare skal inneholde medisinske opplysninger men også sosiale forhold. Når det begynner en nyansatt er det viktig å få opplysninger om vaner og interesser til den enkelte for lettere kunne møte deres behov. Spesielt de som arbeidet på sykehjem var opptatt av dette, da det her var mange som ikke selv kunne gi uttrykk for egne behov og ønsker.

Det skjedde også at opplysningene var mangelfulle, eller det var ikke registret noe i det hele tatt. Noen av de som ble intervjuet nevnte at de hadde fått telefon fra pårørende med spørsmål om hva som hadde hend i den og den situasjonen. Når de så gikk inn i rapporten stod det ingen ting.

I Datatilsynet sine krav for å lagre og behandle personopplysninger fremheves det at en ikke skal lagre opplysninger som ikke har en klar hensikt. Dette kan være opplysninger om økonomi, familie med mer, men det trekkes også fram at opplysningene skal vær korrekte og ha tilstekkelig grunnlag for behandlingen.
HRO teorien legger vekt redundans, at det er systemer som fanger opp feil som blir gjort. Reason mener at fra 80 – 95 % av alle feil skylles menneskelig svikt. I en sektor som helsesektoren hvor nesten all produksjon foretas av mennesker, vil kontroll for å hindre menneskelig svikt være spesielt viltig. Når en så ser at det nesten ikke finnes noen form for kontroll er det innlysende at det lett kan oppstå feil, som også kan få store konsekvenser.
Det eneste området hvor det var nedskrevne rutiner for kontroll var medisinutdeling. Medisinkort er ikke gyldige før de er underskrevet av lege og det skal også signeres når de deles ut. Det gjennomføres også tilsyn ved faste tidspunkt.

7.3.2 Konsekvenser av feil

Ingen av de som ble intervjuete hadde opplevd at det hadde oppstått situasjoner hvor det hadde vært fare for liv og helse på grunn av det var skrevet inn feil opplysninger. Fra noen ble det hevdet at grunnen var at det forkom lite feil. En annen mente at grunnen var: ”vi kjenner jo pasientene så godt at vi ser når det står noe feil, eller mangler opplysninger”. Det er selvfølgelig en god sikkerhet at en kjenner pasientene godt, ikke minst for pasientene som opplever trygghet ved å ha kjente personer rundt seg, men samtidig øker dette risikoen for at det kan oppstå farlige situasjoner når de som har kunnskapen ikke er tilstede. Da må det finnes riktige og oppdaterte opplysninger som er lett tilgjengelig.
Fra de som jobbet i hjemmetjenesten ble det understreket viktigheten av gode rapporter da de skiftet pasienter oftere og ikke fikk så god tid til bli kjent med dem. Det viser at riktige rapporter med nødvendig informasjon er en forutsetning for riktig behandling.

7.3.3 Hvordan sikre kontroll

Det må være en kontroll med at de opplysningene som legges inn er riktige. Ikke fordi en ikke stoler på hverandre, men for å forsikre seg at det som står der er riktig. I en travel hverdag som det er for de fleste som arbeider innenfor den kommunale helsetjenesten er det lett å gjøre feil. Dette understrekes også av Reason, som fremhever at i alle systemer kan det oppstå svikt.
I følge Forskrift om pasientjournal § 6 skal det i alle helseinstitusjoner være en

journalansvarlig. Denne personen skal i følge forskriften ha det overordnede ansvaret for journal og bestemme hva som skal stå i den. I de fleste kommunene var dette definert, og hos de fleste var det avdelingsleder som hadde denne funksjonen. De ga imidlertid uttrykk for at de ikke hadde kapasitet til å gå igjennom alle journaler noe alle var frustrert over.
Det står ingen ting i loven eller forskriften at denne personen skal være en leder. Det kan nesten være umulig for en leder på en stor avdeling med mange pasienter og ha full oversikt over alle journaler. Det vil være behov for delegere. Innenfor HRO legges det vekt på at en skal trekke på den kompetansen som er i organisasjonen for å unngå at det oppstår feil. I de fleste avdelinger vil det være flere enn avdelingslederen som har kompetanse til å kontrollere journaler, da dette ikke er en administrativ jobb, men en faglig. Oppgaven kan med fordel delegeres til andre. Det er viktig at dette blir formalisert og at det er avklart hvem som har ansvar for hva. Det må være en form for kvittering på at journaler er lest igjennom og godkjent. Det holder ikke bare å ta stikkprøver. Alvorlige feil kan da ikke bli oppdaget.
Ved innføring av elektronisk pasientjournal vil dette bli enda viktig. Her vil pasientopplysninger bli hentet fra fagsystemet og videresendt til for eksempel sykehus eller fastlege. Disse har ikke samme kjennskapet til pasientene som de vil ha på et sykehjem, og er avhengig av at alle opplysninger er korrekte. Det vil her ikke holde at en bare kontrollerer opplysninger når de sendes over. Det må være rutiner for kontroll tidligere. Opplysninger som er feil eller mangelfulle vil være vanskeligere å oppdage jo lengre tid det går fra de ble skrevet.

7.4 Avvikshåndtering en forutseting for sikker behandling

Kontroll må også innebære at feil blir rapportert. HRO teorien legger vekt på at en organisasjon lærer gjennom prøving og feiling. Det er igjennom erfaring fra tidligere hendelser en kan få ny lærdom som hindrer at en gjør de samme tingene om igjen. I Reason sin beskrivelse av den Generative kulturen det å søke etter feil, og oppmuntre de som kommer fram med feil, noe som gjør at organisasjonen er i stand til å utvikle seg å bli bedre.
Det samme understrekes også i HRO teorien hvor det legges vekt på hvordan de ansatte må være opptatt av å oppdage situasjoner hvor det kan oppstå svikt, og ikke prøver og forenkle arbeidsprosessene eller ta snarveier. HRO legger også vekt på at en gjennom erfaring lærer noe nytt som en tar med seg når en møter nye utfordringer.
I undersøkelsen hadde alle med ett unntak et system for avvikshåndtering. For de som hadde

det var de varierende hvordan det ble brukt. Ingen brukte det bevisst i forhold til data. De som ikke hadde avvikssystem mente det kunne være bra å ha det, men var redd for at det skulle ta for mye tid og resurser. I en hektisk hverdag vil alt en skal gjøre som ikke er direkte rettet inn mot pasientene oppleves som noe som tar tid fra det en egentlig skal gjøre. Uansett er det viktig at de ansatte ser på avvikshåndtering som et virkemiddel for å bedre tilbudet for pasientene. Det er kun gjennom systematisk registrering av avvik at en får synliggjort feil og får mulighet for å gjøre noe med dem. Det kom fram i undersøkelsen at det var varierende hva som skjedde når feil ble oppdaget. De fleste feil ble bare tatt opp med den som hadde forårsaket feilen og rettet der og da. Denne form for håndtering kan minne om Reason sin Byråkratiske kulturer hvor den som oppdager feil blir lyttet til når de kommer og at en løser det som oppstår der og da uten å bringe det videre eller gjøre noe mer ned det. På den måten blir det ikke noe ”mer” problem rundt det. Erfaringene en får igjennom å løse feilene vil ikke andre i avdelingen lære noe av, eller andre i kommunen som har mange av de samme utfordringene.

7.4.1 Gode sikkerhetssystemer krever avvikshåndtering

Til tross for at en klarer å etablere gode rutiner og flere sikkerhetssystemer for å fange opp feil vet en at feil likevel skjer. Dette viser Reason med sin swiss-cheesemetafor hvor han påpeker at det i alle sikkerhetssystemer finnes svakheter som gjør at feil oppstår. Selv der det er flere sikkerhetsrutiner som overlapper hverandre vil det kunne oppstå feil. Spesielt der sikkerhetsrutinene håndheves av mennesker kan det svikte i flere ledd fordi den som kontrollerer også kan overse feil. Derfor er det ikke noe motsetningsforhold mellom det å ha gode sikkerhetssystemer og et godt system for avviksrapportering. Egentlig er det en forutsetning. For å avdekke feil og i tillegg få rettet dem opp må feil dokumenters. Sikkerhetsarbeid er ikke et prosjekt en gjennomfører, for så å være ferdig med det. I mindfulness teorien legges det vekt på at de ansatte skal ha en kontinuerlig overplikt for å se om det i arbeidet er svakheter som over tid kan medføre svikt. Kun gjennom å ha systemer som fanger opp feil og mangler, som så blir fulgt opp, vil en kunne gjøre organisasjonen stadig sikrere. Her vil avviksmeldinger være en viktig forutsetning.

7.4.2 Definere hva avvik er

Når en skal definere hva et avvik er, må en først definere hva det skal være et avvik fra. For noen avvik er dette enkelt å definere da det vil være brudd på lover og forskrifter. I andre tilfeller må det være nedskrevne hva som er avvik. Muntlige rutiner er det vanskelig å dokumentere avvik fra, da en ikke har noe skriftlig å vise til. Derfor må alle rutiner som det er viktig bli overholdt være nedskrevet og godkjent av lederne.

7.4.3 Kultur for avvikshåndtering

I undersøkelsen kom det fram litt forskjellige synspunkter på om en hadde en kultur hvor det var lov og melde fra om feil eller komme med forslag til forbedringer. De fleste mente det var greit å melde fra om avvik også når andre hadde gjort feil, men de var opptatt av det måtte tas opp med den personen som hadde gjort det først. Det var også rom for å komme fram med kritikk og forslag til endringer på deres arbeidsplass og at de ansatte ble oppmuntret til både og melde fra om avvik, og komme med forslag.
En leder var mer skeptisk og mente det var vanskelig å komme fram med kritikk da det kunne tas personlig. ”Dette er noe som må tas opp til stadighet at vi må kunne kritisere hverandre uten at det er negativt. Det er ved å ta lærdom av det som er feil at en kan bli bedre, ellers så fortsetter vi bare å gjøre de samme feilene om igjen.”
En ansatt opplyste at hos dem var det dårlig kultur på det å melde fra om avvik. ”Det blir gjort alt for lite. Vi tok det opp for ikke så lenge siden om at dette er noe vi må bli bedre på og at en må hjelpe hverandre. Vi mangler også en leder som er tydelig på at vi må gjøre det”. Her ser en hvor viktig ledernes holdninger er for å få til endring av kulturen. Dersom ikke lederen går foran og aktivt påvirker til endring skjer det ofte lite. Passive ledere kan ofte skape passive ansatte. Alle mente at de skrev for lite avvik og at de trengte å bli bedre på det.

I alle organisasjoner vil det oppstå en kultur som utvikler seg over tid. Schein fremhever flere faktorer som må være tilstede for at det skal oppstå en kultur. Han nevner at gruppene må ha vært sammen over tid og delt problemer sammen. I tillegg har en funnet fram måter å løse problemer på. Skal kulturen endres må også gruppens erfaringer endres. Ønsker en å få til en kultur hvor sikkerhet er viktig må en også ha en kultur hvor det både er lov og riktig å melde fra om feil. Carlsson understreker viktigheten av at en i organisasjonen har felles verdier og normer som danner grunnlaget for det en utfører. Det å kunne melde fra om avvik uten å bli straffet er en viktig verdi i en organisasjon. Klarer en ikke det vil en kunne ende opp med

elementer fra patologisk kultur, hvor det blir viktigere å ta den som melder fra om feilene enn og gjøre noe med feilene.
Det lett å forstå at det å melde fra om feil som blir foretatt av en kollega kan være vanskelig. En ønsker ikke å kritisere kollegaer eller sladre. Spesielt gjelder dette når feilen skyldes slurv, eller i verste fall bevisste feil som om det blir oppdaget kan få konsekvenser for den ansatte. Dette ble også understreket i intervjuene. En ansatt hadde funnet liste over pasienter som hjemmetjenesten skulle besøkes, med navn og telefonnummer i en tjenestebil mandag morgen. De hadde ligget der over natta. Vedkommende innrømmet at det ikke ble skrevet avviksmelding, men det ble tatt opp med den som hadde glemt igjen listen. Det er forståelig at det kan være vanskelig å melde fra videre i slike tilfeller.

I en annen kommune var det en ansatt som hadde glemt igjen arbeidsliste med opplysninger om andre pasienter hjemme hos en pasient. Disse ble så lest av en pårørende. Her ble hendelsen tatt opp som et avvik og diskuter blant de ansatte.

Alle de som ble intervjuet understreket viktigheten av at en tok hendelen opp med den som hadde forårsaket avviket før en melde det videre. Det er selvfølgelig at dette gjøres, der det er mulig.

7.4.4 Hensikten med avviksmeldinger

Det har liten hensikt å etablere et godt utviklet avvikssystem dersom de som skal benytte det ikke ser hensikten. I sin definisjon av organisasjonskultur understreker Schein at skal en organisasjonskultur etableres og utvikles må gruppen være lenge nok sammen til at en har opplevd og delt betydelige problemer sammen. I tillegg må en ha opplevd mulighet av å løse disse og se effekten av løsningen.
Som tidligere nevnt kom det i undersøkelsen fram at ingen hadde opplevd at mangel på rapporter eller feil hadde medført konsekvenser som fikk følge for liv og helse. De feil som oppstod løste en greit selv. Hva er da hensikten med å etablere et godt system for avvikshåndtering? Erfaring er viktig for å få til en felles forståelse av hva farene er. Ut fra Scheins teori kan det nesten virke som det ikke er mulig å utvikle en organisasjonskultur for avviksmeldinger før en ha opplevd konsekvensen av og ikke har det, da han legger stor vekt på medlemmenes erfaring.

7.4.5 Lærdom uten erfaringer

Erfaringer er viktig, men en kan ikke alltid vente til en har egne erfaringer. Da kan det være for seint. Det kan være krevende å få til endringer før en opplever at det er nødvendig. Spesielt i en travel hverdag er det å konsentrere seg om feil som en ikke ser konsekvensene av vanskelig. Her må en finne en måte å klare dette på. Det å diskutere hvorfor det oppstår feil, og hvilke konsekvenser det kan få for pasientene er et godt utgangspunkt. Videre kan en foreta øvelser hvor en ser hva som kan skje når det oppstår feil, og disse får utvikle seg uten at det gjøres noe med. Her kan det selvfølgelig innvendes at dette er tidkrevende, og at det ikke er mulig å få til i en stram hverdag. Nå behøver ikke alltid øvelser være tidkrevende. De kan gjennomføres som papirøvelser hvor en diskutere seg gjennom forskjellige senarioer. Det å trekke inn erfaringer fra andre arbeidsområde kan være en riktig måte å forstå konsekvenser på. Dette er noe en gjør bl.a. innefor brannvern hvor en viser til hendelser som har fått store konsekvenser.

Innenfor "mindfulness" teorien trekkes det fram en del momenter som er viktig for å hindre at det oppstår feil. Det legges vekt på at de ansatte er opptatt av at feil kan oppstå og at det er viktig at en oppdager svakheter tidlig for å unngå at det skjer feil. Dette handler om å ha sikkerhet i ryggmargen. Dette får en kun til dersom tema tas opp ved faste intervaller og at de ansatte minner hverandre på det i det daglige arbeidet. Også her er det noen som må gå foran og trekke de andre med seg. I noen sammenheng benytter en betegnelsen endringsagenter. Dette er ansatte som har som oppgave å påvirke organisasjonen i en bestemt retning. De er vanlige ansatte og alle vet hvem de er, men de skal ha et spesielt fokus på å påvirke de andre.

7.4.6 Tilbakemeldinger

For at avviksmeldinger skal ha noe effekt må det også gis tilbakemelding til melder på hva som videre skjer. Meldinger som ikke fører til noe virker passiviserende på melderne. De vil fort slutte å skrive siden det ikke har noen hensikt. Det må settes en frist for når det skal gis tilbakemelding og hvilke tiltak som skal iverksettes. Følges dette ikke opp må det etableres systemer som gjør at det meldes videre opp i organisasjonen.
Ved innlevering av avviksmeldinger skal disse sendes videre til lederen for virksomheten. For de mest alvorlige sendes de videre til AMU (arbeid og miljøutvalg) eller rådmann. En av kommunene hadde et kvalitetsutvalg hvor alle avviksmeldinger ble tatt opp. For de andre ble meldingene sendt opp til nærmeste leder som hadde ansvar for å behandle avviket.

Siden det så å si ikke ble skrevet avvik på datasikkerhet kom det heller ikke fram hvordan disse ble behandlet.

7.5 Ledelsens godkjenning av rutiner

Siden ingen av de som ble intervjuet hadde sett at det var utarbeidet rutiner må en kunne anta at de ikke fantes. Av naturlige årsaker vil det da heller ikke vært foretatt noen godkjenning av rutinene fra lederne. I undersøkelsen som ble foretatt av Datatilsynet i 2010 var det to av de kommunene jeg undersøkte som opplyste at de ikke hadde utarbeidet rutiner, og to som opplyste at de hadde. Dersom rutiner skulle finnes har de liten effekt, når de som til daglig skal ivareta personvernet ikke kjenner til de.
Personopplysningsforskriften § 2-3 påpeker at virksomhetens ledelse har ansvar for at bestemmelsene i forskriften følges.
I en tradisjonell hierarkisk organisasjon vil beslutninger bli fattet av lederne. Jo, mer omfattende bestemmelsene er jo, høyere opp i hierarkiet fattes beslutningene. Dette vil i hovedsak være saker som handler om økonomi og beslutninger som berører hele eller deler av organisasjonen.
Skal det være fokus på personvern i hierarkisk organisasjonen må lederne på rådmannsnivå gå foran og vise vei. Det er de som må bestemme hvilke rutiner kommunen skal ha og har ansvar for at de blir gjennomført. I følge personopplysningsloven er det den som til daglig har ansvar for virksomheten som også har ansvar for at bestemmelsene i personopplysningsloven oppfylles. Dette er i kommunene rådmann. Det ble i denne undersøkelsen ikke foretatt noen vurdering av hvor aktive rådmennene var i forhold til å sikre personvernet, men uansett må dette måles ut fra hvordan det fungerer i det daglige.
I en kommune med flere ledernivå kan det være en utfordring å sikre at de beslutninger som fattes på rådmannsnivå kommer ut til alle i organisasjonen. Ansvaret er det lederne på de forskjellige nivåene som har, men det må være en kontroll på at det skjer.

Det vil kunne oppstå uenighet i organisasjonen om viktigheten av sikkerhet og hvilke krav en som skal ligge til grunn. Her må de som har ansvar for virksomheten gå inn å definere. I kommune er det rådmann som har fullmakt til å definere hvilke rutiner som skal gjelde i kommunen. Dette står ikke i motsetningsforhold til at de ansatte er med i prosessen. Som oftest er de ansattes deltakelse en forutsetning for å få nok grunnlag til å fatte beslutninger.

7.6 Årlig gjennomgang av sikkerheten

Hvert år skal det være en gjennomgang av datasikkerheten. En leder visste at det ikke hadde skjedd, siden de innførte fagprogrammet, mens de øvrige ikke visste om det forekom, men en regnet med at det skjedde. De regnet med at det ble gjort på et høyere nivå. En avdelingsleder uttrykte det slik: ”Slikt skjer ikke på mitt nivå” En forventer at ting blir løst oppover i systemet uten at en selv får kjennskap til det. En kommune hadde planer om å starte opp, men var ikke kommet i gang.

Rutiner blir ofte statiske. Sikkerhetsarbeid er en kontinuerlig prosess som krever at en stadig blir bedre. Det vil nok være naturlig i de fleste kommuner at det er andre enn avdelingslederen som har ansvar for at dette gjøres, men en slik gjennomgang vil ha liten hensikt dersom de som til daglig jobber ute i avdelingene ikke blir tatt med, eller enda verre, ikke blir informert om funnene.
Innenfor HRO teorien legges det vekt på at sikkerhet og pålitelighet har høy prioritering i alle ledd i organisasjonen. Uten at lederne går foran med et godt eksempel er det vanskelig å kreve at de ansatte skal ha et spesielt fokus på sikkerhet. HRO legger også stor vekt på at desentralisert styring. Skal en få til et levende sikkerhetsarbeid i hver avdeling må avdelingslederne og de ansatte trekkes med i gjennomgang og utformingen av sikkerheten. Det vil som oftest være på dette nivået en har best kjennskap til svakheter ved sikkerheten.

I en travel hverdag er tid ofte en mangelvare. Skal en i tillegg begynne med årlige gjennomganger av datasikkerhet vil dette kreve mer tid. En måte å løse dette på er å legge gjennomgangen samtidig med for eksempel vernerunden. Dette vil også lett kunne slås sammen da metoden for gjennomføringen er like.

7.7 Definert ansvarsdeling i organisasjonen

Det ble i undersøkelsen ikke fortatt intervju med ledere over avdelingsledernivå. Det kommer derfor ikke fram hvordan rådmann i kommunen har avklart ansvarsfordelingen seg i mellom i forhold til personvern, men rådmannen har ansvaret for at dette gjøres.
Det sier seg selv at rådmannen ikke er i stand til å ha oversikt over alt som skjer i kommunen. En vil være avhengig av å delegere oppgavene til andre. Det vil være naturlig at de som til daglig har ansvar for tjenestene også har ansvar for at personvernet ivaretas i sin avdeling,

men uansatt er det være rådmann som står ansvaret for at lovverket følges. Velger rådmannen å delegere den daglige oppfølgingen av datasikkerhet til andre må dette være definert i kommunens rutiner for personvern som ingen av de, som ble intervjuet kjente til.

Datatilsynet har åpnet for at organisasjoner kan søke om å få opprette personvernombud. Denne personen skal påse at personvernet ivaretas, og påpeke mangler. Personvernombudet er kun rådgiver og står ikke ansvarlig for de tiltak som iverksettes, det er lederen for virksomheten sitt ansvar. En av kommunene i undersøkelsen hadde etablert ordningen med personvern.

7.8 Ledelsens holdninger til sikkerhet

Alle avdelingslederne mente at lederne i kommunen var opptatt av sikkerhet til tross for at det ikke var utarbeidet skriftelige rutiner. Det var litt varierende hva de var oppatt av. Noen var opptatt av tilgangsstyring, mens andre presiserte viktigheten av at ansatte logget seg ut når de var ferdig med å legge inn opplysninger.
De ansatte hadde med ett unntak en opplevelse av at deres avdelingsleder var opptatt av personvern. Som en sa: ”Lederen vår er det i alle fall.” Det er et godt utgangspunkt å være oppatt av personvern, men som ledere er en også forpliktet til å gjøre noe med det. Uten det skjer det ingen forbedring.
En mente at lederen ikke var god på personvern. ”Har for lite rutiner. Slik som nøkler. Folk kan få tilgang til ting de ikke skal”. ”Vår leder er alt for lite opptatt av sikkerhet”. Dette var eneste gangen det i undersøkelsen kom fram missnøye med ledernes holdning til sikkerhet.

7.9 De ansattes holdninger til personvern

Alle lederne mente at personvern var noe de ansatte var opptatt av, men i den travle hverdagen blir en del ting glemt. Døra til vaktrommet står åpen når rommet er tomt, medisinpermen blir liggende åpen på medisintralla uten at personer er til stede og epikriser ligger og flyter på skrivebord.
Lederne opplyste at de diskuterte personvern en del i avdelingene. De var oppatt av hvordan en skriver journaler og hva som skal være med. ”Vi prøver å fortelle de ansatte hvilke plikter og ansvar de har”. Understreke at de ikke skriver om andre pasienter eller pårørende i journalen, men kun forholder seg til den det rapporteres om. ”En trenger ikke å ta med hele

slekta" Dette er noe lederne sa de var veldig bevisst på under opplæring. Har en pasient slått en annen skriver en ikke navnet på den andre. Være bevisst på at brukeren selv skal kunne lese journalen. De ansatte bekreftet mye av det sammen. De fleste mener det er viktig med personvern for å beskytte brukernes privatliv, men at i en travel hverdag var det lett å glemme ting. I en kommune understreket de at dette var et tema de stadig diskuterte og minnet hverandre om. Det kunne for eksempel være at en ikke skulle snakke om pasienter når andre var tilstede, eller passe på at dører var låst . "Vi har mange rutiner, men de er ikke nedskrevne."

En mente at en snakket for lite om personvern. "Hjemmetjenesten er utrolig sårbar. Vi går hjem til folk og observerer mye. Mange ansatte bor i samme området som pasientene. Viktig ikke å fortelle mer enn det som er nødvendig. Vi må holde fokus på det hele tiden ellers så kan det skje feil".

For å få til endringer i personvernet er holdninger viktig. De fleste som ble intervjuet mente de var opptatt av personvern og at det var noe en stadig minnet hverandre om. Schein fremhever at organisasjonskultur bygger på antagelser som grupper har utviklet, og som har fungert så bra at de er blitt gyldige, disse vil så overføres til nye medlemmer. Selv om gruppene har utviklet gode rutiner for å ivareta personvern må de være skriftelige. Når det mangler skriftelige rutiner vil nyansatte, som ikke kjenner kulturen lettere kunne gjøre feil.

7.10 Risikoanalyse

Bare en av lederne i undersøkelsen visste at det var foretatt er ros-analyse. Da den var akkurat var gjennomført og vedkommende hadde selv vært med på å gjennomføre den. Vedkommende understreket at det i analysen var kommet fram mange ting som de ikke var klar over, slik som at papirer ble liggende å flyte uten at de ble makulert. Dette understreker viktigheten av ros-analyse. Selv om en tror at de fleste ting er i orden er det kun ved en systematisk gjennomgang en kan avdekke svakheter i organisasjonen. De andre lederne som ble spurt visste ikke om det var gjennomført ros-analyse, eller om at det var planer for å gjennomføre det. Det kan selvfølgelig tenkes at ros-amalyse ble gjennomført før de ble ansatt i de stillingen de har i dag,

Det stilles krav om at det skal foretas en risikoanalyse ved endring av driften. (Personopplysningsforskriften § 2-4)

Endringer ved driften vil for eksempel være når en innfører nye dataprogrammer som har innvirking på pasientbehandlingen, eller når tjenestene omorganisering. I kommunene blir det innimellom fortatt omorganiseringer. Tjenester slås sammen, eller splittes opp. Alle disse vil kunne ha innvirkning på den tjenesten som ytes, og det skal derfor foretas en ros-analyse for å sikre at personvernet ivaretas.
Når nå flere kommune innfører håndholdte enheter og elektronisk pasientjournal, hvor pasientopplysninger sendes elektronisk må det gjennomføres en ros-analyse i hver kommune før iverksetting.

7.11 Definert akseptabelt risikonivå

Ingen av de spurte visste om det var definert et akseptabelt risikonivå i kommunen. I følge personopplysningsforskriften §§ 2-10 til 2-14 skal virksomheter fastsette et akseptabelt risikonivå. En kan ikke fritt velge hva dette skal være. Det skal i utarbeidelsen legge vekt på hvilke sikkerhetstiltak som trengs for å ivareta det som er virksomhetens formål. For en kommune vil det være områdene som dekkes innenfor områdene konfidensialitet, tilgjengelighet, integritet og kvalitet.

Der det er mennesker vil det også oppstå feil. I alle organisasjoner må en leve med at det kan oppstå feil. Det er også en del av tankegangen i HRO at ingen organisasjon er feilfri. For en organisasjon er det viktig å avklare hvilke feil som ikke kan aksepteres. Hvilke feil dette er avhenger av hvilke konsekvenser de vil ha for driften.
I kommuner kan forskjellige områder komme i konflikt, som for eksempel konfidensialitet og tilgjengelighet. For streng sikkerhet kan medføre at opplysninger ikke er tilgjengelig når det er behov for dem. Her må kommunen si noe om hvordan disse forholdene skal veies opp mot hverandre, slik at begge kan ivaretas på en sikker måte.
For å få en fullstendig oversikt må en foreta en ros-analyse. Når dette ikke blir gjort er det vankelig å definere risikonivået. Igjen handler det om at lederne i organisasjonen går foran og sikrer at dette blir gjennomført. Akseptabelt sikkerhetsnivå skal inngå som en del av kommunens sikkerhetsmål.

7.12 Opplæring en forutsetning for å gjøre ting riktig

Ingen kan forlange at ansatte skal kunne håndtere et ukjent dataprogram uten opplæring. Det finnes i dag et uttall dataprogram og selv om en er vant til å bruke data vil det alltid være behov for opplæring.

På spørsmålet om hvilken opplæring de som be intervjuet hadde fått før de begynte å bruke fagsystem, varierte svarene fra kommune til kommune. En hadde ikke fått noe opplæring før en fikk tilgang til fagprogrammet. Det ble derfor mye prøving og feiling i begynnelsen. En annen fikk en halv dag opplæring, men denne ble også gitt etter at vedkommende hadde fått tilgang. En hadde fått god opplæring, men på grunn av tekniske problemer tok det lang tid før en fikk bruke systemet. Vedkommende hadde da glemt det meste av det de hadde lært. I en kommune hadde de hatt kurs som alle måtte igjennom før de fikk tilganger. De andre trodde de fikk noe opplæring omtrent samtid som de fikk tilgang.

I en kommune hadde de hatt en test som alle måtte igjennom før de fikk tilgang. Ingen av de andre hadde hatt noe form for kontroll eller eksamen etter opplæring, for å sikre at de hadde nødvendig kompetanse til å håndtere programmene.

7.12.1 Dagens opplæring

Dagens opplæring varierer også fra kommune til kommune. Det som var likt for alle var at ingen gjennomgikk kurs før de fikk tilgang til fagprogrammet. En kommune hadde organiserte kurs som var delt i to, et for nybegynnere og et for de som hadde brukt systemet en stund. Tidligere fantes det ikke noe system på opplæringen i denne kommunen. Nå er det en ansatt som har dette som sin arbeidsoppgave, og det er kommet inn i faste former. En annen kommune hadde kurs for nyansatte. Tidligere måtte alle gjennom dette før de fikk tilgang. Da var det også en test alle måtte igjennom. Dette hadde de sluttet med uten at de helt visste hvorfor. Nå ventet de med å gjennomføre kurset til det var flere nyansatte. To av kommunene hadde ingen obligatoriske kurs, men opplæringen skjedde fra den ene ansatte til den andre. I en av kommune slet en også med å ha nok kapasitet til å foreta opplæring. De savnet en person som hadde ansvar for oppdatering, vedlikehold og opplæring i programmet. En kommune hadde ressurspersoner i hver avdeling som hadde ansvar for opplæring av nyansatte, og endringer når det ble innført nye ting.

Alle kommunene hadde etablert en ordning med opplæringsvakter. Her gikk en sammen med en annen ansatt som var kjent i avdelingen. I disse vaktene inngikk også opplæring i å bruke

fagsystemet og skrive rapport, men som det ble sagt av en. ”Hvor god den opplæringen er, avhenger av hvor dyktig den som skal lære bort er”.

I følge Reason skyldes 80 – 95 % av alle ulykker og feil menneskelig svikt. For å redusere antall menneskelig svikt trengs det kunnskap, som igjen forutsetter opplæring. Riktig bruk av elektroniske hjelpemidler kan være en forutseting for sikker behandling av pasienter. Da må det også være krav om at de som benytter programmene har et minimum av kunnskap. Feil bruk kan medføre store konsekvenser. Det holder heller ikke at opplæringen blir gitt etter at ansatte har fått tilgang. Det er spesielt når en er helt ny og ikke har noe kjennskap til programmet at det er lettest å gjøre feil. Det bør være et krav at alle ansatte før de får tilgang til fagprogrammet går igjennom en standard opplæring der de ikke bare får informasjon om hvordan programmet fungerer, men også gis innføring i hva som skal registreres. Dette kan selvfølgelig være vanskelig å gjennomføre. Alle kommunene hadde ordninger med opplæringsvakter. Dette kan være en god midlertidig løsning inntil ansatte kan delta på kurs. Det bør også være en form for godkjenning av den som skal foreta opplæringen og et fast opplegg for hva de skal gå igjennom.
Flere av lederne var som tidligere nevnt opptatt av at de ansatte glemte å dokumentere, at det språket som skrives er lett å lese og at det viktigste kommer fram. Dette bør også være en del av opplæringen. I tillegg bør det i opplæringen være med hvilke forpliktelser den enkelte ansatt har i forhold til personvern, hvilke svakheter programmet har, og konsekvenser ved at det gjøres feil. Her kan en ta utgangspunkt i de ROS-analysene som ”er” gjennomført. Opplæringen bør tilrettelegges ut fra den utdannelse de ansatte har, da de forskjellige yrkesgruppene vil ha forskjellige oppgaver. Det bør også være en form for testing for å sikre at en kan nok til å håndtere programmet. Det skal ikke være mulig å gjennomføre opplæring uten at en har tilegnet seg nødvendig kunnskap.

7.12.2 Vedlikeholdstrening

Ting endrer seg underveis. Dataprogrammene oppdateres og det legges inn nye funksjoner. Mennesker glemmer og kunnskap forsvinner. HRO-teorien legger vekt på kontinuerlig læring for å skape en sikker organisasjon. Kunnskap om data og bruken av den er også en kontinuerlig prosess. Flere av kommunene hadde tilbud om vedlikeholdstrening eller opplæring, men dette var frivillige. En bekreftet at sykepleierne i hennes avdeling deltok på

vedlikeholdsopplæring. ”Når du er sykepleier må du bare være oppdatert”.
En kommune hadde samling med alle superbrukerne en gang i måneden hvor de gikk igjennom hva som var nytt, men hadde ikke noe fast system for vedlikeholdetrening for alle ansatte. I en annen kommune gjennomgikk de endringer i programmet på personalmøter. En kommune hadde ikke noe system for vedlikeholdsopplæring.
Faren med frivillig opplæring er at det ofte er de som trenger det ”minst” som melder seg på, mens de som hadde trengt det mest ikke tørr eller vil. For å sikre at kompetansen hos de ansatte opprettholdes og utvikles etter som behovene endres, bør det være obligatorisk med vedlikeholdsopplæring ved faste tidspunkt, for eksempel annet hvert år. Det må også gjennomføres obligatoriske opplæring når det er store endringer i programmene eller endringer av rutiner.

7.13 Tilgangsstyring til programmene – ”Behov for å vite”

Ingen skal ha tilgang til opplysninger de ikke trenger for å utføre jobben. Alle kommunene hadde innført tilgangsstyring. Tidligere var det slik at de ansatte fikk tilganger til mange pasienter fordi det i programmene var vanskelig å få til gode nok skiller. Dette er nå blitt bedre og en kan skille ut pasienter avhengig av hvilken avdeling de tilhører og hvilken type tjeneste de får. Om noen år vil det sannsynligvis være mulig å gi kun tilgang til de pasientene en skal jobbe med den enkelte dagen. Dette vil selvfølgelig være med på å sikre at ansatte ikke får tilgang til opplysninger de ikke skal ha.
I tillegg er de forskjellige tilganger avhengig av hva slags utdannelse den enkelte har. Sykepleiere har større tilganger enn omsorgsarbeidere. I praksis innebærer det at de kan legge inn flere opplysninger som medisinkort, diagnoser m.m..

Henning Bang beskriver hvordan det i alle organisasjoner kan oppstå subkulturer som har sin egen oppfatning av virkeligheten. Forskjellige yrkesgrupper kan bli subkulturer som ”kniver” med andre om hvordan ting skal organiseres, og hvem som skal få se hva og gjøre hva. Det finnes i dag en rekke utdannelser innenfor helseområdet. I følge helsepersonloven § 48 er det 29 forskjellige yrkesgrupper som har egen autorisasjon som helsepersonell, og som har sin egen utdannelse. I tillegg kommer de med utdannelse innenfor sosialfag og pedagogikk. Nå arbeider ikke alle disse gruppene i kommunene. Likevel kan det oppstå konflikt med hvem som skal bestemme hva og hvilken kompetanse de enkelte yrkesgruppene har. ”Hvem vet

best".
Det kom i undersøkelsen ikke fram at dette var noe problem i de enkelte avdelinger og at tilgangene var akseptert av alle som arbeidet i avdelingen uansett utdannelse.
Alle som ble intervjuet var utdannet sykepleiere både avdelingsledere eller ansatte. Det kan tenkes at resultatet hadde blitt et annet om omsorgsarbeidere hadde fått samme spørsmål.

7.13.1 Ulikt syn på tilganger

Der det kom fram motsetninger var mellom forskjellige avdelinger. Alle lederne som ble intervjuet hadde opplevd at de ikke hadde fått nødvendig informasjon fra andre avdelinger som gjorde det vanskelig å utføre jobben tilfredsstillende. De hadde opplevd at det hadde oppstått uenighet mellom avdelinger om personvern og hvem som skal ha tilgang til hva. Følgende eksempler ble nevnt.
Det hadde vært en episode mellom psykisk helsevern og miljøtjenesten hvor det oppsto en uenighet. En ansatt i psykisk helsevern hadde vært på jobb og observert en pasient som var i ferd med å gå inn i en psykose og skrev en rapport som vedkommende ansatt mente var så personlig at ingen andre skulle se den. Dette var rett før en helg, og ukjente personer kom på jobb og fikk ikke nødvendige opplysninger, slik at de kunne ivareta pasienten på en god måte.
I en kommune hadde de hatt en episode hvor de var inne i en hjem hvor barnevernet også var inne. De ville ha gjort jobben helt annerledes om de hadde fått informasjon om dette på forhånd. Dette ble tatt opp og en så i ettertid at det burte vært håndtert på en annen måte.
"Stort sett går samarbeidet veldig bra. Likevel kan det bli slik at hver avdeling eier sine egne pasienter."
En annen kommune fortalte også om problem med psykiatri. "De holder opplysninger tettere inn mot brystet enn det som er ønskelig". Det har hendt at psykiatrien er inne og gir tjenester til pasienter som er innlagt på sykehjemmet og så holder de tilbake opplysninger som avdelingen hadde trengt i sitt daglige arbeid. "De har nok også strengere tilganger på fagsystemet enn det andre har. Vi opplever de ønsker å få mest mulig opplysninger fra oss, men er lite villig til å formidle tilbake".
Også i den siste kommunen hadde det vært diskusjoner mellom psykiatrien og hjemmetjenesten om hvilke opplysninger som skulle utveksles.

Argumentet for at en ikke ønsket å dele informasjon er et ønske om å beskytte brukerne. Dette er et godt argument, men en vil alltid kunne stille spørsmålet med hvem som skal avgjøre det.

At en i forskjellige avdelinger har forskjellige synspunkter på dette er ikke så sjelden. I følge Bang vil det kunne oppstå konflikter mellom avdelinger fordi en ønsker å beskytte egen kompetanse og det arbeidet en selv utfører.
Datatilsynet understreket viktigheten av at opplysninger er tilgjengelig når de trengs for å kunne ivareta riktig behandling. Taushetsplikten må aldri komme i veien for et godt tilbud til den enkelte pasient. I verste fall kan dette medføre fare for liv og helse. Taushetsplikten er til for å beskytte pasienten, ikke de ansatte og deres kompetanse. Det er pasienten som eier sine egne opplysninger og skal gi tillatelse til bruken, jmf. Personopplysningsloven § 9a. Viktig at pasienten får informasjon om hvem som får tilgang til opplysninger og hva de skal brukes til. Gjøres dette på en god måte oppstår det sjelden problemer. Dette ble også understreket av en av de som ble intervjuet. ”Vi er alt for lite flinke til å ta med pasientene i diskusjonen om hvem som skal få tilgang til deres helseopplysinger.” Uansett vil det alltid være pasientens beste som skal ivaretas. Hvordan dette gjøres, vil være et faglig spørsmål som det er ledernes ansvar å avgjøre. Samtidig er det viktig ar dette diskuteres i kommunen. Når det oppstår motsetninger mellom avdelinger innebærer ikke nødvendigvis det at den ene har rett og den andre feil. Som oftest ligger sannheten et sted i mellom, og diskusjoner kan bidra til at en får fram synspunkter en tidligere ikke har tenkt på og slik kan være med på å skape bedre rutiner og holdninger.

7.13.2 Erfaringer på tvers av avdelinger

Det er de som til daglig arbeider innfor fagområdet som kjenner problemstillingene og som best er i stand til å identifisere svakheter. Samtidig kan nærhet til området medføre at en ikke ser fordi det går så greit. I teorien om ”mindfulness” legges det vekt på at en trenger personer med forskjellig bakgrunn og kompetanse for lettere å se svakheten i organisasjonen. Norske kommuner er ikke bare hierarkisk inndelt. De er i tillegg inndelt etter de tjenestene de skal yte. Dette innebærer at de som arbeider i de forskjellige avdelingene har omtrent samme utdannelse og bakgrunn. Innenfor skolen har så å si alle en pedagogisk utdannelse, innenfor helse er det helseutdannelse som dominerer og innenfor teknisk har de fleste teknisk utdannelse. Det finnes få ingeniører innenfor pleie og omsorg. Ordtaket sier at like barn leker best, men er det også slik at like barn tenker likt og ser det samme, eller ”ikke” ser det samme. Til tross for at de fleste som jobber innenfor helsesektoren har samme type utdannelse, så er mennesker forskjellig og har en forskjellig bakgrunn som gjør at en ser forsjellig på ting. Det kan være forskjellig yrkeserfaring, alder, kjønn og nasjonalitet. Det er viktig å se på

forskjeller, som en styrke og ikke som en svakhet. Det er ikke alltid riktig å få alle til og tenke likt, noen ganger er det viktig å få de ansatte til og tenke forskjellig for på den måten få avdekket svakheter.
Andre i kommunen kan ha andre erfaringer og kan gi nye innpulser for å hindre at feil oppstår. Igjen handler det om å lære av hverandre. I tillegg til helse- og omsorgsektoren er det flere som arbeider med sensitive personopplysinger. NAV, PPT og barnevern som har mange av de samme problemstillinger som helse og omsorg. Det å diskutere felles problemstillinger rundt personvern og sikkerhet vil kunne gi gode innspill for alle parter. På den måten trekker en ikke bare på kompetanse i egen avdeling, men trekker med den som finnes i kommunen. Det var ikke i noen av de kommunene som ble undersøkt etablert noen kontakt på tvers av avdelinger, hvor en diskuterte personvern.

7.14 Logging

Alle kommunene foretok logging av trafikken i fagsystemet, men ingen tok ut logger ved faste tidspunkt for å kontrollere. Dette ble kun foretatt når det var misstanke om missbruk. Ingen hadde kjennskap til at det noen gang hadde skjedd at loggen var brukt eller om det var utarbeidet rutiner for hvordan den skulle brukes. Ingen kjente heller til om det var utarbeidet rutiner for hva som skjer om en oppdager at noen ansatte har foretatt noe ulovelige.
I følge Datatilsynets veileder om internkontroll og informasjonssikkerhet (5.8.3) er virksomheten pålagt å logge all bruk i fagsystemene**.** Dette blir enda sterkere understreket i høringsforslag til ny forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre. Hensikten med å føre logg er og oppdage om noe har prøvd å komme seg inn eller har utført noe ulovelig.

Det er enkelt å forstå hvorfor kommunene ikke gjennomgår loggene ved faste tidspunkt. For det første er det tidkrevende. For det andre kan det være at en ikke ønsker å foreta noen form for overvåking uten at det er misstanke. En ønsker å ha et tillitsforhold til de ansatte. Dette er et vanskelig spørsmål. Mange ansatte vil kunne oppleve gjennomgangen av logger uten at det foreligger noen form for misstanke som overvåking. Ingen organisasjon er tjent med ansatte som føler seg utrygge og mistrodd. Gjensidig tillit er viktig for et godt arbeidsmiljø. Vi lever i et samfunn hvor hver enkelt av oss blir stadig mer overvåket, selv om det ikke er misstanke om noe kriminelt. Opplevelsen av å være overvåket er aldri en god følelse. Diskusjonen rundt

EU sitt datalagringsdirektiv viser hvor betent diskusjonen er. Mange legger vekt på at en ikke skal overvåkes før det er misstanke. I kommunene overvåker en alle, i tilfelle noen skulle gjøre noe galt. I forbindelse med utskrift av logger er det viktig å finne fram til en løsning som alle føler seg bekvem med. Før en iverksetter rutiner for gjennomgang av logger bør dette ha vært diskutert med de ansatte og at det må være full åpenhet om den løsningen som velges. I denne diskusjonen er det viktig å understreke er at grunnen til at det foretas logging er og sikre pasientenes privatliv. Ved at alle ansatte behandles likt er ingen er mer misstenkt enn andre. Samtidig må ikke det å føre logg bli en unnskylding for ikke og ha gode rutiner for å hindre missbruk. Når det oppdages missbruk på loggen er allerede skaden skjedd.

7.15 Melde inn til Datatilsynet

”Det er det vi lurer på om har skjedd” var svaret fra en av lederne på spørsmålet om kommunen hadde meldt inn Datatilsynet hvilke opplysninger en behandlet. De andre hadde ingen kunnskap om det hadde skjedd, men de regnet med at det var ivaretatt av de som var høyere i systemet. Også her går det igjen at de som arbeider med sensitive opplysninger til daglig vet lite om hvilke krav som stilles og forventer at det er andre i systemet som ivaretar dette.

7.16 Mangel på backup kan få katastrofale konsekvenser.

Ingen av de som ble spurt kjente nøyaktig til hvordan backup rutinene var i kommunene, men de fleste visste at det ble foretatt backup en gang i løpet av døgnet. Ingen hadde heller opplevd at data hadde forsvunnet på grunn av mangel på backup.
Alle som har benyttet data en periode har opplevd å slette noe som ikke skulle slettes. Stort sett fører det ikke til annet enn mer jobb og en del ergrelse. I en kommune kan imidlertid sletting av opplysninger få store konsekvenser. Derfor skal det i alle kommuner være et system for backup som skal sikre at de data som er lagret ikke forsvinner, selv om de skulle bli slettet eller maskiner bli ødelagt på grunn av brann eller vannskalder. Kommuner skal ha gode rutiner for backup og sikring av data. De fleste kommuner har egen IT avdelinger som har ansvar for den daglige driften av både utstyr og programvare. De som ikke har egen avdeling kjøper denne tjenesten av andre, eller har en felles løsning for flere kommuner. Innenfor IKT-drift er sikkerhet viktig da dette er hjerte i hele den elektroniske databehandlingen. Feil som medfører at data forsvinner eller at utstyr ødelegges kan for en

kommune få fatale konsekvenser for driften. For å sikre at dette ikke kan skje tas det backup en gang i døgnet. I tillegg tas det uke- og måneders backup. Som ekstra sikkerhet skal backupen som vanligvis er taper lagres et annet sted enn der serverne er. Grunnen til dette er først og fremst brann. Skulle det begynne å brenne i serverrommet har en i alle fall kopier av data. Igjen handler det om å legge inn redundans som kan fange opp feil som oppstår. I HRO teorien legges dette inn som en viktig forutsetning. Skulle ett system svikte er det et annet som overtar. Det er nok i de fleste kommuner lett å få aksept for at en trenger gode backupsystemer, da de fleste vil forstå at dersom alle opplysninger forsvinne, vil det kunne få katastrofale konsekvenser.

7.17 Behandling av sensitive opplysninger utenfor sikre områder

Flere av de som ble intervjuet hadde kommet over dører som sto opp inn til vaktrom og medisinpermer som lå åpne uten at det var ansatte til stede. Det var i kommunene manglende rutiner for sikring av de områdene hvor sensitive opplysninger ble behandlet. I en kommune hadde en rutiner for at alle skulle logge seg ut av datamaskinen når en var ferdig. Ingen av de andre kjente til noen skriftelige rutiner for sikring av områdene, men det var uskrevne regler om at en låste døra til rom hvor det ble behandlet sensitive opplysninger når ingen var tilstede. Åpne dører er en stor utfordring. Det kan være lett for uvedkommende å komme seg inn og få tilgang til sensitive opplysninger. Selv om datamaskiner er skrudd av kan det skje at rapporter, medisinkort eller epikriser ligger tilgjengelig. Selv om en benytter elektronisk fagprogram vil det alltid være behov for å ha noen opplysninger på papir. En person som kommer inn vil kunne både lese og kopiere opplysninger uten at noen oppdager det.
Dette ble spesielt nevnt fra en av lederne som understreket at når en går fra jobb skal alle papirer som inneholder personopplysinger være forsvarig nedlåst. Fra en kommune ble det fremhevet at dette var noe de stadig tok opp og minnet hverandre om. Dette handler om holdninger. I ”mindfulnes” teorien understrekes det at de ansatte hele tiden må være opptatt av at det kan oppstå ny svikt som en tidligere ikke har oppdaget. Igjen handler det om å ha sikkerhet i ryggmagen.
Erfaring tilsier at alle ikke klare det. Det er behov for sikkerhetssystemer som fanger opp når noen gjør feil. Måten å løse problemet med åpne dører er at en enten har smekklås, eller det som blir mer og mer vanlig, kortleser hvor bare autoriserte personene har tilgang. Samtidig er det alltid en balanse hvor sikkert det skal være. På de fleste sykehjem kan en komme og gå

som en vil. I alle fall på dagtid. På ettermiddag og kveld må en ringe på. Dette kan selvfølgelig gå utover sikkerheten, men som en av sykepleierne sa: ”Dette er jo et hjem, ikke et fengsel, her skal pårørende få komme og gå som de vil”. ”Livet er kort, så vi må prøve å gjøre det beste ut av det også i den siste fasen” Det er viktig å definere hva som skal være åpent og hva som skal være låst. Vaktrommet og andre rom hvor det oppbevares personalopplysninger bør alltid være låst når det ikke er ansatte tilstede.

Det vil bli en ny utfordring når kommunene etter hvert begynner med håndholdte enheter som gjør det mulig å logge seg på fagprogrammet når en er ute hos pasienten. Ingen av de kommunene hvor det ble foretatt intervju hadde begynt med dette ennå, men noen kommuner har startet opp og andre er i ferd med å planlegge det. Slik systemet er i dag vil en få de samme tilgangene på den bærbare enheten som en har når en logger seg på fagsystemet via en datamaskin på et vaktrom. I et hjem vil de ansatte være alene og en har ingen kontroll med hvem som får tilgang til personopplysninger. En vil da miste de sikkerhetsrutinene som er etablert ved at sensitive opplysninger skal behandles på et vaktrom eller kontor. Selv om teknikken etter hvert vil bli bedre og en kan begrense innsyn til kun å gjelde den pasienten en er hos, vil en ikke ha oversikt over hva som skjer i den enkeltes hjem. Dette vil setter ekstra krav til de ansatte om å være bevisst på hvordan en bruker enheten.

7.18 Sikkert nettverk?

I kommunene ligger fagsystemer i et sikkert datanett. Dette for å sikre at sensitive opplysninger bare blir behandlet av autorisert personell, og at det ikke er mulig å få tilgang til internett eller lagre opplysninger på eksterne lagringsmedia. I følge Datatilsynet er det pr. i dag ikke mulig å sikre dette uten og etabler et eget lokket nettverk.

For å spare både penger og plass benytter de fleste kommuner nettverksskrivere. Fordelen er at mange kan benytte den samme skriveren. I alle kommuner hadde en opplevd at utskrifter var kommet ut på feil skriver fordi de som skrev ut ikke hadde definert riktig skriver. Siden skriverne er lagt i sikkert nettverk vil det være begrenset hvor mange skrivere en utskrift kan komme til, men det er fullt mulig at en utskrift fra en avdeling kan komme ut på en skriver i en annen avdeling. I en kommune som ikke var med i undersøkelsen er det et felles sikkert nettverk hvor det er mulig for en i barnevernet å velge en skriver som er i hjemmetjenesten.

Nå sa alle de som ble intervjuet at dette hadde blitt mye bedre etter at det var tatt opp, og en hadde begrenset antatt skriver en hadde tilgang til.
Et annet problem de fleste som ble intervjuet hadde opplevd, var at utskrifter ble liggende på skrivere slik at andre kunne lese dem, ta dem med seg ved en feil, eller at de på annen måte kom på avveie. Det er fort gjort å glemme å hente en utskrift i en travel hverdag, med stadige avbrudd.
Løsningen for disse problemene er at det på skrivere som benyttes av flere personer legges inn krav om personlige passord eller at en trekker nøkkelkort for å få utskriften. Igjen handler det om penger, da slike løsninger er dyrere.

7.19 Oppdatering av programmer

Alle de som ble intervjuet kjente til at oppdateringer av fagprogrammet ble gjort av IT avdelingen, enten sammen med leverandøren eller systemansvarlig for programmet. Alle ga utrykk for at de opplevde at dette var godt ivaretatt, uten at en var helt sikker på hvordan det ble gjort.
Ingen dataprogram er ferdig utviklet når de kommer på markede. Det kommer nesten alltid fram feil og mangler en ikke klarte å oppdage under testing. Når en i sin tid innførte fagprogrammene innenfor helse og omsorg oppdaget en tidlig at det var feil som kunne få konsekvenser. Feilene ble meldt inn til leverandøren som så sendte ut oppgraderinger som kommunen måtte legge inn i programmene.
Kravene til programmene endres, blant annet kommer det nye krav til innrapportering av statistikker som skal hentes ut fra fagprogram. Et eksempel på dette er IPLOS (Individuell pleie og omsorgs statistikk) som ble innført for noen år siden. Her skal alle data tas direkte ut av programme og etter at de er kryptert sendes til SSB. For å få dette til krevdes det stor oppgraderinger av fagprogrammene.
For å sikre at programmene blir riktig oppgradert må det være utarbeidet rutiner for hvordan dette gjøres. Oppgraderinger av programmer kan være teknisk krevende, og det er viktig at de som utfører det har nok kunnskaper til å unngå at det oppstå problemer. Dette må gjøres i et samarbeid mellom de som har IT kunnskap og personer som kjenner fagområdet godt, for å sikre at alle modulene i programmene funger som det skal, og at opplysninger ikke forsvinner. Dette er også i tråd med HRO-teorien om at en skal trekke på den kompetansen som er i organisasjonen for å unngå feil, eller få rettet de opp før det skaper problemer. De fleste

kommunene har egen IT-avdelingen som har bygd seg opp en god kompetanse om kommunens nettverk og de programmer som kommunen bruker. Ved bruk av den kompetansen som er i kommunen, bygger en opp lokal kompetanse som medfører at en unngår å gjøre feil. Nærhet skaper trygghet.

7.20 Viruskontroll

Ingen av de som ble intervjuet hadde noe kunnskap om hvordan dette ble gjort, men de tok det som selvfølge at dette ble godt ivaretatt.
Ved siden av å oppdatere programmene er det viktig å ha god kontroll med virus. Da internett ble innført dukket det opp en ny type problemer som en tidligere ikke hadde hatt før virus, som om de fikk lov til herje fritt kunne slette alle data. Samtidig med at virusene begynte å komme på internett ble det utviklet programmer som fant virusene og slettet dem før de fikk gjort noe skade. I dag finnes det en rekke virusprogrammer på markede. For at de skal ha noen nytte må de oppdateres kontinuerlig. Alle kommuner må ha gode rutiner for å sikre at nettverket ikke blir infisert av virus.

8 Konklusjon

I denne oppgaven har jeg sett på hvordan kommunene ivaretar personvernet og hvilke farer manglende rutiner og kontroll kan medføre for de personene som mottar helsetjenester. Personvern har gjennom mange år vært regulert gjennom lover og forskrifter. Bruk av elektroniske hjelpemidler som fagprogrammer i kommunene er heller ikke noe nytt, og lover og forskrifter for personvern burte derfor være godt kjent i kommunene. Kommunene har hatt god tid på seg til å utarbeide rutiner, og innarbeide de i virksomheten.

Jeg har valgt kun å intervjue de som til daglig jobber med pasienter og ikke topplederne i kommunen. Grunnen er at det er innenfor helse- og omsorg en arbeidet med de pasienter som er mest sårbare ovenfor feil som gjøres innenfor personvern. Foretas det feil her vil det få større konsekvenser enn om det skjer høyere oppe i systemet fordi det er her registrering og behandling skjer.

8.1 Mangel på rutiner

Det som var mest påfallende var mangel på rutiner. Ingen av de kommunene som ble undersøkt hadde skriftelige rutiner for personvern, som var kjent for de ansatte i avdelingene. Det fantes noen rutiner, men for alle manglet det et en overordnet beskrivelse av hvordan personvernet skulle ivaretas.

At de ansatte ikke kjente rutinene for backup og sikring av rom hvor det oppbevares servere og annet datautstyr er ikke så rart. Disse rutinene er det bare IKT personell som arbeider med det til daglig som skal kjenne.

Det er langt verre at det mangler rutiner for den daglige sikringen av personopplysninger ute i avdelingene. Dette kan om det ikke tas tak i få store konsekvenser. Spesielt når det komme ansatte inn som ikke kjenner alle de uskrevende rutinene.

8.2 Mangel på kontroll

Det funnet som var mest alvorig var mangel på kontroll av de opplysninger som legges inn om den enkelte pasient. I dag foregår nesten all dokumentasjon elektronisk. Det er de opplysningene som legges inn i fagsystemet som er sanne. I en hektisk hverdag er det lett å gjøre feil. En glemmer å dokumentere eller skriver på feil person. Ved at det ikke er utarbeidet faste rutiner som fanger dette opp kan feil bli værende, og få konsekvenser for den enkelte pasient på et seinere tidspunkt. Opplysninger som lagres om den enkelte pasient må være så korrekte og utfyllende at en ukjent ved å lese dem er i stand til å foreta nødvendig behandling.

8.3 Mangel på avviksbehandling

I tillegg kom det fram at det i liten grad ble meldt fra om avvik når det ble oppdaget feil. De feil som oppsto ble løst der og da. Mangel på avviksmeldinger vil som oftest medføre at feil ikke blir synliggjort, og en foretar ikke nødvendige endringer for å hindre at ting skjer igjen. Totalt sett kan dette medføre en holdning hos de ansatte om at det ikke er så farlig. Det går jo stort sett bra, og ingen i vår avdeling har fått feil behandling på grunn av feil i fagsystemet.

I tillegg vil mangel på avvik medføre at lederne i organisasjonen ikke ser problemene og regner med at alt er i orden.

8.4 Manglende opplæring

Det kom også fram mangelfull opplæring av de som skulle benytte programmene. I de fleste kommunene fikk de ansatte tilgang uten at de hadde gjennomgått noe formell opplæring eller avlagt noe testing på at de har nødvendig kunnskap.

Vi lever i en tid hvor kravet til kunnskap stadig øker. Begrepet livslang læring blir stadig mer og mer aktuelt. Selv om de fleste som i dag arbeider innenfor helsesektoren har en grunnutdannelse vil denne aldri være nok for et helt arbeidsliv. Alle vil uansett arbeid ha behov for å tilegne seg ny kunnskap. Dette er ikke noe vi selv kan velge, men en forutsetning for å være i arbeid. Det er derfor ikke urimelig at en innenfor den kommunale helsetjenesten stilles krav om at alle ansatte skal gjennomgå opplæring i bruken av elektroniske fagprogram, og etter opplæring dokumentere at de innehar nødvendig kunnskap. Spesielt når en setter dette opp mot de konsekvenser feil bruk kan få for den enkelte pasient.

8.5 Forskjellen mellom ledere og ansatt

Ved å velge både avdelingsledere og ansatte uten lederansvar har jeg sett på om det er noen forskjell på deres synspunkter.
Det kom i undersøkelsen ikke fram at det var markant forskjell mellom leder og ansatt i deres forståelse av hvor viktig personvern var. Alle var enige at det å beskytte den enkeltes personvern var viktig, og noe en måtte ha fokus på i det daglige. De hadde også en felles oppfatning av at det var viktig å ha mer fokus på personvern og at dette er et område en kan og bør bli bedre på. Nå kan grunnen til at det ikke kom frem markerte forskjeller også være at spørsmålene i undersøkelsen ikke hadde nok fokus på motsetningene.

8.6 Forskjeller mellom kulturer

I de enkelte avdelinger kom det ikke fram motsetningsforhold mellom forskjellige yrkesgrupper. En av grunnene kan selvfølgelig være at det kun var sykepleiere som ble intervjuet. Samtidig vet en at personer som arbeider sammen over tid lettere skaper en felles oppfatning av virkeligheten og derfor lettere definerer hvordan arbeidet skal fordeles. Der det kom fram motsetninger var mellom avdelinger. Her har en mindre kjennskap til hverandre og det vil lettere kunne oppstå missforståelser eller uenighet, fordi en tror mye om de andre uten

å vite.

8.7 Forskjell mellom kommunene

Det kom ikke fram noen markant forskjell mellom de enkelte kommuner. En kan ikke ut fra undersøkelsen trekke noen konklusjon på om det er en sammenheng mellom størrelsen på kommunene og personvernet. For å finne ut av det måtte en ha foretatt en mye større undersøkelse.

8.8 Hvem har ansvar for at personvernet ivaretas

I følge personopplysningsloven er det den som til daglig har ansvar for virksomheten som også har ansvar for at personvernet ivaretas. I en kommune er dette rådmann. Selv om denne personen har ansvaret må oppgaven delegeres. Det vil være naturlig at det gjøres til den som har det daglig ansvaret for de enhetene som behandler personopplysninger. I denne sammenheng innebærer det tjenestesjefene for helse- og omsorgstjenestene.
Når en ser resultatet av undersøkelsen kan det se ut som lederne ikke tar personvente nok på alvor, eller mangler forståelse av de konsekvenser manglende rutiner innebærer.
En ting er at personlige opplysninger kan komme på avveie. Dette kan medføre ubehag for den personen det gjelder. Noe helt annet er at det kan skje feilbehandling fordi det legges inn feil opplysninger, eller det mangler opplysninger.

Vi står foran store endringer innenfor den kommunale helsetjenesten. Det vil stille krav til økt kompetanse innenfor flere områder, også bruk av data. Denne kunnskapen gjelder ikke bare de som arbeider daglig med pasienter og benytter fagprogrammer, men like mye lederne på alle nivå. Har ikke lederne nødvendig kunnskap om bruk av data, vil de ikke være i stand til å foreta de nødvendige valg for de utfordringene som kommunene kommer til å få. Det gjelder både hvilke programmer en skal velge, og definere hvilken kunnskap den ansatte skal besitte. Ledere uten datakunnskap vil heller ikke være i stand til å vurdere hvilke farer mangel på datasikkerhet kan medføre for de personene en skal gi tjenester til.

8.9 Datatilsynets rolle

Datatilsynet er etter forholdene et lite tilsyn med få resurser til å foreta tilsyn i alle kommuner. De er lokalisert i Oslo og har ingen distriktkontor. Resursene har heller ikke økt i takt med den enorme utviklingen som har vært innenfor elektronisk databehandling.
For å sikre at kommuner og andre som behandler sensitive opplysninger ivaretar personvernet må det etableres bedre kontroll. Det er lite sannsynlig at Datatilsynet vil etablere seg med distriktskontor slik som for eksempel Arbeidstilsynet. En må derfor finne andre måter og sikre at personvernet ivaretas på. Dette kan gjøres ved at en legger noe av ansvaret til fylkesmann. I dag har fylkesmann ansvaret for oppfølging av helsetjenesten gjennom Helsetilsynet. Skille mellom databehandling og pasientbehandling vil bare bli mindre ved at bruk av data vil inngå mer og mer i pasientbehandlingen.
Hvorfor ikke legge tilsynet med personvernet i helsesektoren under fylkesmannen ved Helsetilsynet? Dette forutsetter selvfølgelig at Fylkesmannen har nødvendig kunnskap til å ivareta denne funksjonen.

Datatilsynet har en rekke sanksjonsmuligheter for de som ikke følger lovverket. Dette bør brukes mer bevisst ovenfor kommuner som ikke følger opp karvene til personvern.

8.10 Gjennomgang av lover og forskrifter

Når lover ikke blir fulgt er det viktig å stille spørsmål om hvorfor. Årsakene er sikkert mange, men det kan være viktig å stille spørsmål om det lovverket som er utarbeidet er hensiktsmessig. I dag er det et detaljert lovverk som regulerer personvernet. I tillegg kommer både forskrifter, normer og veiledere. Blir det for mye å holde styr på for den enkelte kommune? Er det mulig å forenkle det uten at det går utover sikkerheten? Dette er et tema som ligger utenfor denne oppgaven, men jeg synes likevel det er viktig å stille spørsmålet. Kommunene skal i dag forholde seg til et uttall av lover og regler. Kan de bli så mange at en ikke klarer å ha oversikt?

8.11 Generalisering

I undersøkelsen er det foretatt undersøkelse i bare noen få kommuner. Det er derfor viktig å stille spørsmål om resultatene som kom fram er representative for kommunene. Eller er dette

bare noe som gjelder for de kommunene jeg undersøkte? Det finnes selvfølgelig variasjoner fra kommune til kommune, som det vil finnes variasjoner innad i den enkelte kommune. Hadde jeg brukt andre informanter i den enkelte kommunen kunne også svarene blitt forskjellig ut fa den enkeltes opplevelse og holdninger. Allikevel mener jeg å se en klar trend. Svarene var stort sett like i alle kommunene. I tillegg er det i de tilsyn som Datatilsynet har foretatt kommet fram mye av det samme. Spesielt ser en mye av den samme trenden i den siste spørreundersøkelsen fra 2010 hvor Datatilsynet fortok en henvendelse til alle landes kommuner. Det mangler mye på at den behandlingen som foretas av personopplysninger i norske kommuner er forsvarlig.

9 Litraturliste

Aven, Terje - Boyesen, Marit – Njå, Ove – Olsen, Kjell Harald – Sandve, Kjell: Samfunnssikkerhet, Universitetsforlaget 2004

Aune, Irene Henriksen IKT for helsepersonell, Akribe 2007

Bang, Henning: Organisasjonskultur, Tano, 1988

Brusoson, Nils og. Olsen, John P ”Kan organisasjonsforming Velges?” Kapittel 1 i boken av samme forfattere: ”Makten at reformera” Stockholm: Carlsson 1990

Datatilsynet, En veiledning om internkontroll og informasjonssikkerhet, 2009

Datatilsynet, Risikovudering av informasjonssystem, 2009

Datatilsynet: Årsmelding 2003, Utdrag av omtalen av Datatilsynets tilsynsvirksomhet

Datatilsynet: RAPPORT FRA TILSYN Saksnummer: 2004/1825 Tilsynsdato: 11.01.2005 Rapportdato: 02.02.2005 Tilsynsobjekt: Horten kommune Sted: Horten,

Datatilsynet: Veiledning i informasjonssikkerhet for kommuner og fylker 2005

Datatilsynet: Kommuneundersøkelsen 2010 – 2011, 2011

Det kongelige arbeids- og administrasjonsdepartement: St.meld. nr. 17 (2002-2003) Om statlig tilsyn

Det kongelige helse- og omsorgsdepartement: St.meld. nr. 47 (2008- 2009) Samhandlingsreformen Rett behandling – på rett sted – til rett tid.

Det kongelige helse- og omsorgsdepartement: Forslag til forskrift om informasjonssikkerhet, tilgangssyring og tilgang til helseopplysninger i behandlingsrettede helseregister, 2010

Jacobsen, Dag Ingvar: Hvordan gjennomføre undersøkelser? 2. utgave Høyskoleforlaget 2005

Reason, James: Managing the Risks of Organizational Accidents, Ashgate 1997

Schein, Edgard H., Organisasjonspsykologi 3 utgave, Tano 1983

Statskonsult, Rapport 2002: 12 (Be)Grep om tilsyn, gjennomgang av statlig tilsynsordninger 2002

Sosial- og helsedirektoratet: Norm for informasjonssikkerhet i helsesektoren, 2006

Rosness, Ragnar, Guttormsen, Geir, Steiro, Trygve, Tinmannsvik, Ranveig K. og. Herrera, Ivonne A: Organisational Accidents and Resilient Organisation: Five Perspectives, revison 1, Sintef report STF38 A 04403, 2004

Lover:

Lov om behandling av personopplysninger

Lov om helseregistre og behandling av helseopplysninger

Lov om Schengen informasjonssystem

Lov om helsepersonell m.v.

Forskrifter:

Forskrift om behandling av personopplysninger

Forskrift om pasientjournal

Personopplysningsforskriften

Websider

www.bt.no Bergens Tidende

www.nrk.no NRK

www.rbnett.no Romsdals Budstikke

www.abcnyheter.no abcnyheter

www.nhn.no/om-oss Virksomheten Norsk Helsenett AS

www.datatilsynet.no Datatilsynet

www.personvernnemnda.no Personvernnemnda

www.oslo.kommune.no Oslo kommune

www.utsira.kommune.no Utsira kommune

www.siste.no Siste.no

10 Vedlegg

INTERVJUMAL (leder)

Personopplysninger

Navn:

Arbeidssted:

Type arbeid:

Hvor lenge ansatt:

Utdannelse:

Hva slags type jobb har du?

Hvor lenge har du hatt den?

Hvor ofte bruker du data i jobben?

Hva innebærer bruken?

Opplæring

Hvilken type opplæring fikk du før du fikk tilganger til fagsystemet?

Hvilken type opplæring får de ansatte?

Når får de den?

Blir det foretatt noen test, prøve får ansatte får tilgang

Har dere noen form for vedlikeholdsopplæring?

Rutiner

Er det utarbeidet skriftlige rutiner for backup av data i kommunen?

Kjenner du til hva de rutinene innebærer?

Hvem har ansvar for oppgraderinger og vedlikehold av fagprogram?

Er det utarbeidet skriftelige rutiner for dette?

Er det utarbeidet rutiner for datasikkerhet i organisasjonen?

I følge Personopplysningsforskriften § 2-16 skal det foreligge dokumentasjon for hvilke rutiner som er utarbeidet og som har betydning for informasjonssikkerheten.

Hva inneholder de?

Er disse gjennomgått og godkjent av ledelsen?
Personopplysningsforskriften § 2-3 påbeker at virksomheten ledelse har ansvar for at bestemmelsene i forskriften følges. Videre stilles det krav om at informasjonssystemene skal jevnelig gjennomgås for å kartlegge om det er hensiktsmessig forhold til virksomhetens behov.
Blir dette gjort og i tilfelle når var siste gangen?

Hvem er med på gjennomgangen?

Hva ble resultatet av gjennomgangen?

Er det gitt melding til Datatilsynet om hvilke opplysninger virksomheten behandler?
I følge personopplysningsloven kap. VI. Skal virksomheten senest 30 dager før behandlingen ta til melde fra til Datatilsynet. Er dette gjort og er det rutiner som ivaretar dette.

Er det utarbeidet noen rutiner for kontroll av det som føres av opplysninger er riktig. Leses av en annen person.

Føres det logg for det som gjøres inne i fagprogrammene? Hva skjer om en oppdager missbruk?

Avvik

Er det utarbeidet rutiner for avgangskontroll?
Hvem har ansvar for å definere hvilke tilganger de ansatte skal ha.

Har du noen ganger oppdaget at det mangler opplysninger, er skrevet inn feil eller skrevet på opplysninger på feil bruker?

I tilfelle ja, hva gjorde du med det?

Hva skjer når det oppdages fei

Er det nedskrevne rutiner på hva en skal gjøre når en oppdager feil

Er det akseptert for å melde fra om feil også når andre har gjort de.

Har du erfaring med at det har oppstått farlige situasjoner på grunn av feil ved datasikkerhet.
Gitt feil medisiner
Iverksatt feil behandling

Har det skjedd at sensitive opplysninger har kommet på avveie?

Har det fått noen konsekvenser?

Er personvern et tema som diskuteres i avdelingen og i tilfelle hvor ofte?

Diskuteres det i ledergruppa?

Opplever du at dette er et tema som ledelsen i kommunen er opptatt av?

I tilfelle ja, på hvilken måte?

Diskuteres det på tvers av avdelinger, skole, barnevern, NAV

Er du selv opptatt av hvordan personvernet varetas i det daglige arbeidet

Hvordan jobbes det med personvern i kommunene. Grupper.

Er det lov å komme med kritikk, eller si ifra om feil som oppstår. Blir ansatte oppmuntrer til å komme med forslag til forbedringer.

Hva må til for at du skal oppleve at datasikkerhet blir et viktig tema på din arbeidsplass?

Opplever du at det er motsetning mellom avdelingene i synet på sikkehet.

INTERVJUMAL (Ansatte i avdelingen)

Personopplysninger

Navn:

Arbeidssted:

Type arbeid:

Hvor lenge ansatt:

Utdannelse:

Jobb innhold

Hva slags type jobb har du?

Hvor lenge har du hatt den?

Hvor ofte bruker du data i jobben?

Hva innebærer bruken?

Opplæring

Hvilken type opplæring fikk på fagsystemet?

Fikk du opplæring får du fikk tilgang

Har dere noen form for vedlikeholdsopplæring?

Rutiner

Har du kjennskap til om det i kommunen er utarbeidet skriftelige rutiner for hvordan sensitive opplysninger skal håndteres?

Når var sist du så eller leste disse?

Veit du hva de innholder?

Hvor du kan finne de?

Er det utarbeidet noen rutiner for kontroll av det som føres av opplysninger er riktig. Leses av en annen person.

Avvik

Har du tilganger til opplysninger om brukere eller pasienter som du ikke jobber med?

Har du noen ganger oppdaget at det mangler opplysninger, er skrevet inn feil eller skrevet på opplysninger på feil bruker?

I tilfelle ja, hva gjorde du med det?

Hva skjer når det oppdages feil?

Er det nedskrevne rutiner på hva en skal gjøre når en oppdager feil?

Har du erfaring med at det har oppstått farlige situasjoner på grunn av feil ved datasikkerhet?
Gitt feil medisiner?
Iverksatt feil behandling?

Har det skjedd at sensitive opplysninger har kommet på avveie?

Har det fått noen konsekvenser?

Er dette et tema som diskuteres i avdelingen og i tilfelle hvor ofte

Opplever du at dette er et tema som ledelsen i kommunen er opptatt av?

I tilfelle ja, på hvilken måte?

Er du selv opptatt av hvordan personvernet varetas i det daglige arbeidet?

I tilfelle hvorfor, eller hvorfor ikke?

Er det lov å komme med kritikk, komme med forslag til forbedringer, si ifra om feil som oppstår.

Er det aksept for å melde fra om feil også når andre har gjort de.

Er det enighet om datasikkerhet i kommune

Opplever du at det er forskjellig syn på hva som er viktig?