
# Evaluering av sikkerhetsløsninger for helseportal

av

**Kent Anderson**
**Arnstein Hellestøl**

**Hovedoppgave til mastergraden i informasjons- og kommunikasjonsteknologi**

**Høgskolen i Agder**
**Grimstad, august 2004**

# Sammendrag

Dagens situasjon i helsevesenet er preget av lite samhandling og store forskjeller mellom de forskjellige aktørene. Behovet for nytenkning er derfor stort. Det er allerede satt i gang en del forsøksprosjekt som skal kunne dekke de behov som trengs.

I dette prosjektet ble modellen Contextual Design brukt for å innhente nærmere informasjon om de behov som trengs for samhandling i dagens helsevesen.

Etter at informasjonen var skaffet ble den brukt til å sette opp et scenario for en diabetespasient hvor elektronisk samhandling hadde blitt innført.

Videre blir det presentert to forskjellige løsningsforslag som hver for seg er en mulighet for hvordan samhandlingen i helsevesenet kan forbedres. De to løsningsforslagene er: felles database-løsning og portal–løsning. Felles database-løsningen går ut på at de forskjellige helseaktørene sender den viktigste informasjonen fra deres pasientjournaler inn i en felles database som alle helseaktørene har tilgang til. Portal–løsningen går ut på at pasienten eier sin egen journal. Derfor settes det opp en portal der han/hun kan gi innlogingsmuligheter og rettigheter, til de forskjellige helsedatabasene i helsesektoren, til den denne måtte ønske. Dermed kan disse aksessere pasientens journal.

De to løsningsforslagene ble satt opp mot Datatilsynets regelverk og sikkerhetsbestemmelser. Begge løsningsforslagene imøtekommer i følge denne rapporten Datatilsynets regelverk, mens portal–løsningen ikke kunne tilfredsstille Datatilsynets sikkerhetsbestemmelser.

Sikkerhetsteknologier ble presentert. Ut i fra disse ble det satt opp en sikkerhetsarkitektur for hvert løsningsforslag.

Presentasjonen av de to forskjellige sikkerhetsarkitekturene ble disse samkjørt med hvordan en diabetes pasient kan ta i bruk de to løsningsforslagene Disse sikkerhetsarkitekturene sikrer de sensitive opplysningene på best mulig måte, for å kunne tilfredsstille Datatilsynets krav.

De to løsningsforslagene ble evaluert med hensyn på regelverk, sikkerhetsbestemmelse og sikkerhetsarkitektur. Det ble da klart at felles database var den beste løsningen.

# Forord

Denne rapporten er en avsluttende hovedoppgave i masterutdanningen innenfor informasjons- og kommunikasjonsteknologi (IKT) ved Høgskolen i Agder, fakultet for teknologi i Grimstad. Faget IKT-6400 Hovedoppgave tilsvarer 30 studiepoeng

Oppgaven ble definert i samarbeid mellom Førstelektor Rune Fensli (HiA), Peter Jansen (Bouvet) og kandidatene. Arbeidet med oppgaven har pågått fra januar til september 2004

Vi vil takke Nils Kristian Fjærbu, Dr. Håvard Skjærvik og Dr. Arne Quist Paulsen for den nyttige informasjonen som ble gitt under samtalene med dem.

Vi vil også takke veileder Førstelektor Rune Fensli for nyttig veiledning gjennom prosjektperioden.

Grimstad, september 2004

Kent Anderson

Arnstein Hellestøl

# Innholdsfortegnelse

# Figurliste

# 1. Innledning

## *1.1 Oppgavetittel*

*"Evaluering av sikkerhetsløsninger for helseportal"*

## *1.2 Oppgavedefinisjon*

*Det skal foreslås en sikkerhetsarkitektur for en portal-løsning hvor sikkerhet, funksjonalitet og brukervennlighet vektlegges med utgangspunkt i en aktuell pasientsituasjon*
*Det er under utvikling nye tjenester beregnet for drift i et helsenett, hvor ulike aktører skal ha ulik tilgang til informasjon. Dette kan etableres gjennom portal-løsninger, hvor bruk av digital ID, rollebasert aksesskontroll og workflow-analyser er sentrale sikkerhetselementer. Pasientens rolle i fremtidens helsenett vil forsterkes gjennom aktiv bruk av systemer for egen innlegging av måledata enten manuelt eller gjennom automatiske løsninger. Det er viktig at slike løsninger kan tilfredsstille de sikkerhetsmessige og organisatoriske krav som stilles for sensitiv informasjon i et helsenett.*
*Det skal evalueres mulige løsninger for informasjonsflyt mellom ulike helsetjenester/nivåer i forhold til de krav som stilles i gjeldende lover og forskrifter, og ut i fra dette vurdere hvilke sikkerhetselementer som må implementeres for at løsningene skal gi akseptabel sikkerhet*

## *1.3 Bakgrunn for oppgaven*

Dagens helse-Norge består av mange forskjellige systemer for hvordan arbeidsoppgaver blir gjort. Noen sykehus har f.eks. gått helt over til Elektronisk Pasient Journal (EPJ). Sørlandet sykehus, Arendal (SSA) har makulert alle de gamle papirutgavene av pasientjournalene og gått helt over til EPJ. Andre sykehus har på den annen side lite bruk av EPJ og bruker de "gamle" papirutgavene av journalene. I tillegg brukes mye gule lapper og notater for å gi beskjeder til hverandre.

Det er ønskelig [se vedlegg B] med et felles helsenett hvor alle aktører, dvs. både sykehus, fastleger, kommune og pasient blir involvert og satt sammen på en helt annen måte enn hva som er tilfelle i dag.

Det jobbes kontinuerlig med dette og mange forsøksprosjekter er allerede på trappene (f.eks. pasientlink). En del kommuner har også pilotprosjekter for forskjellige pasienttyper (f. eks diabetes pasienter).

Førstelektor Rune Fensli har utarbeidet en oppgave som tar for seg nettopp hvordan et felles helsenett vil kunne fungere, Det finnes mange muligheter for hvordan et slikt system kan implementeres. Portal-løsning er en av dem.

Sikkerheten er den største hindringen på veien mot et samlet helse-Norge. Det er utarbeidet mange regelverk som kan være vanskelige å tilfredsstille i forhold til personvern og personopplysninger.

Denne oppgaven tar for seg mulige løsningsforslag for et felles helsenett. I oppgaven vil det bli sett på om det er mulig å presentere løsningsforslag der sikkerhet, lover og regler kan bli overholdt, og dermed gjør det mulig å samle alle aktørene innen helsevesenet til et felles nett.

## *1.4 Rapportens organisering*

Rapporten er delt opp i 11 hovedkapitler med tilhørende underkapitler. Den presenterer først eksempler på påbegynte og planlagte prosjekter innen elektronisk samhandling i helsevesenet.

I kapittel 3 blir det satt opp hypoteser for prosjektet. Videre i kapittel 4 tar rapporten for seg hvilke arbeidsmetoder og modeller som er brukt for å utarbeide oppgaven i prosjektperioden.

I kapittel 5 presenteres et scenario med forslag til løsninger. Disse løsningsforslagene blir videre kommentert i henhold til gjeldene regelverk, sikkerhet og sikkerhetsbestemmelser i kapittel 8.

Kapittel 6 tar for seg den teoretiske utredingen av de sikkerhetsteknologiene som blir brukt i sikkerhetsarkitekturen.

I kapittel 7 blir løsningsforslagene hver for seg satt opp arkitektonisk med hensyn på brukervennlighet, funksjonalitet og sikkerhet.

I kapittel 9 blir hvert enkelt løsningsforslag evaluert i forhold til regelverk, datatilsynets sikkerhetsbestemmelser og arkitektur. Det løsningsforslaget som sees på som det beste etter evalueringen blir valgt som det løsningsforslaget som ville vært ønskelig å gå for.

Kapittel 10 foretar en drøfting av scenarier, hypoteser og sikkerhetsarkitektur.

Konklusjonen for prosjektet kommer i kapittel 11.

# 2. Pågående prosjekter innen samhandling i helsesektoren

Samhandlingen mellom helseaktørene er i dag ganske ”gammeldags” i forhold til de it-mulighetene som finnes. Det er derfor kommet mange forslag til hvordan dette skal forbedres. I Tromsø er det gjort et forsøksprosjekt med kommunikasjon mellom lege og pasient over Internett. Dette prosjektet kalles Pasientlink. Danmark har vært en pioner innen samhandling i helsevesenet. Der er det nå satt i gang en helseportal som gjør at pasienten og helsesektoren kan kommunisere med hverandre.

Begge disse prosjektene blir presentert i dette kapittelet.

## *2.1. Pasientlink*

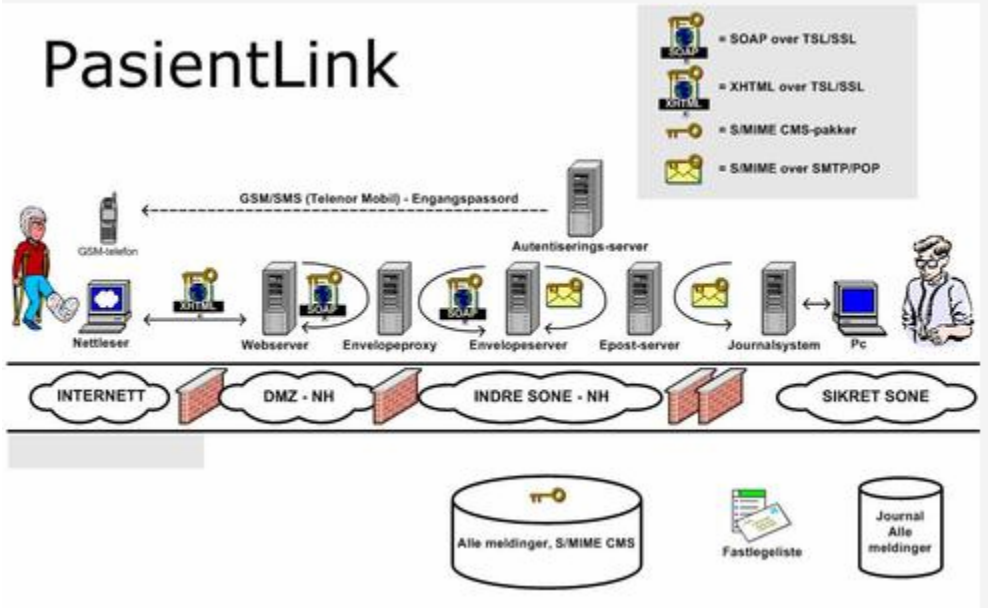
Pasientlink[1] er en ide som ble utarbeidet av Nasjonalt Senter for Telemedisin (NST) på oppdrag fra Sosial- og Helsedirektoratet, og gikk ut på at pasienten skulle kunne kontakte sin fastlege over Internett. Ved hjelp av en nettleser kan pasienten stille spørsmål til sin lege og lese svarene legen gir. Dette var et pilotprosjekt som varte mellom september 2002 og desember 2003. Det ble utført på sentrum legekontor i Tromsø og ble kjørt på Nordnorsk helsenett.

NST satte som et hovedkrav at løsningen skulle tilfredsstille Datatilsynets Personvernlov og ikke true helsenettets sikkerhet. Det ble derfor satt sterke krav til valg av arkitektur, som *”helseopplysninger skal ikke sendes til maskiner som ikke er tilstrekkelig sikret”[1]*, *”kommunikasjon som inneholder pasientsensitive opplysninger skal foregå i en sikret sone”[1]* og *”bruk av tofase autentisering som adgangskontroll”[1]*. Det siste kravet vil si at løsninger kun basert på passord ikke var nok. Derfor har NST brukt mobiltelefon som en tilleggsenhet.

NST har lagt vekt på at pasientlink skal være en billig tjeneste for pasienten. Derfor var løsninger som krevde fysisk installasjon hos pasienten og løsninger som krevde installasjon av programvare utelukket.

Det ble lagt vekt på å følge åpne standarder for meldingsutveksling, og å bruke den programvaren som er tilgjengelig på legekontoret fra før. Sikkerheten bygger på autentisering og kryptering. For en bedre teknisk beskrivelse av Pasientlink, se [2].

Under er det en figur som viser den arkitektoniske oppbyggingen av Pasientlink:




FIGUR 2.1. ARKITEKTONISK OPPBYGGING AV PASIENTLINK [2]

## *2.2. Helseportalen www.sundhed.dk*

Den danske helseportalen[3] ble opprettet i desember 2003, og gav den danske befolkningen en bedre oversikt over helsesektoren, medisiner og sykdommer. Portalen samlet hele helsesektoren på Internett. Dette gav pasientene og helseaktørene en mulighet til å kommunisere og holde oversikten over hverandre.

Ideen til å bruke en portal inn til helsenettet kommer av suksessen bankvirksomheten har hatt ved å bruke portal til nettbanker. Når de så hvor effektivt bankene kunne bruke nettet, mente helsetjenesten de kunne gjøre det på samme måte.

Portalen har tidlig vist seg som en suksess. Grunnen til dette kommer av at Danmark har vært en pioner innen kommunikasjon i helsevesenet. Allerede tidlig på nittitallet hadde de opprettet et nasjonalt helsenett.

For mer informasjon om den danske helseportalen, se [4]

# 3. Hypoteser

I dette kapittelet er det satt opp 3 hypoteser. Målet med hypotesene er å sette søkelyset på viktige elementer i forhold til å utvikle løsningsforslag. Disse hypotesene blir drøftet i kapittel 10.

## *3.1 De aktuelle hypotesene*

1. Felles database-løsning vil være teknisk mulig å implementere i henhold til Datatilsynets regelverk og Sikkerhetsbestemmelsene i personopplysnigsforeskriftene.

2. Portal-løsning vil ikke være teknisk mulig å implementere i henhold til Datatilsynets regelverk og Sikkerhetsbestemmelsene i personopplysnigsforeskriftene.

3. Både felles database og portal-løsning er mulig å implementere med dagens teknologi.

# 4. Metodekapittel

For å gjennomføre prosjektet ble det valgt en modell som det ble arbeidet etter. Den modellen som ble valgt for å sette arbeidsmåter i system, ble valgt på grunnlag av hva som passet best for arbeidsplanen. Den valgte modellen, Contextual Design blir presentert og nærmere beskrevet i delkapitlet under.

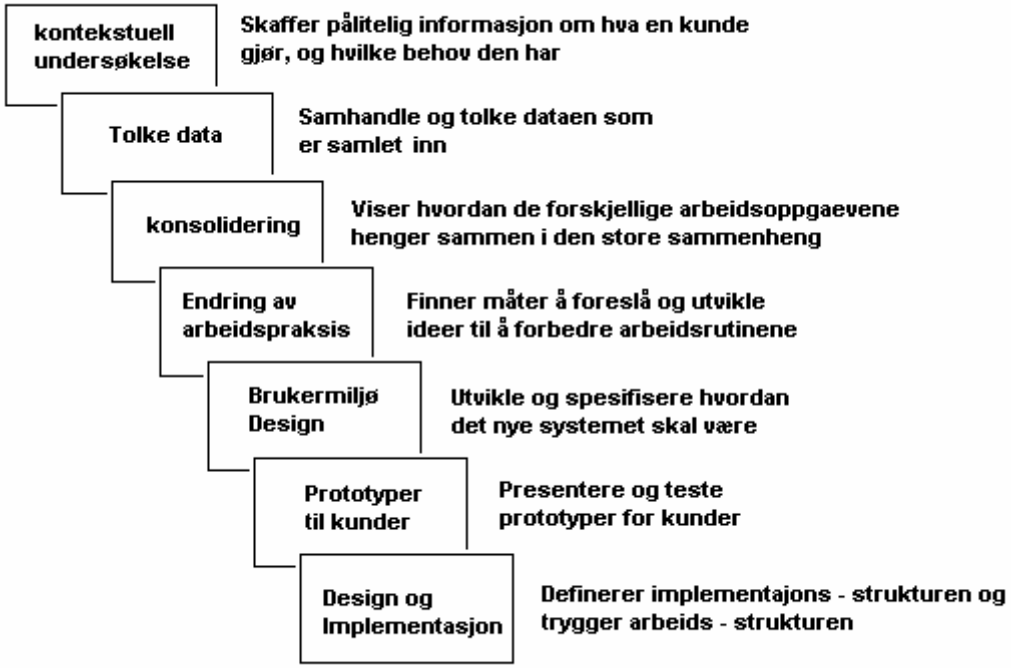
I vårt arbeid ble ikke hele modellen av Contextual Design brukt. Modellen har som mål å først gå ut til den aktuelle kunden for å samle informasjon til det videre arbeid. Når hele arbeidet er ferdig blir produktet, som er laget ut ifra den informasjonen som blir samlet inn, tatt med ut til kunden igjen for testing. For å løse denne oppgaven ble bare de første delene av Contextual Design brukt. Produktet (i dette tilfellet; våre løsningsforslag) ble ikke tatt med tilbake til de aktuelle partene for testing. Bruken av modellen ble i vårt tilfelle begrenset til å samle inn informasjon og strukturere denne, for så å bruke denne informasjonen til å utarbeide våre løsningsforslag.

Det ble sett på som viktig å få et scenario som lå så nært opp til en virkelig situasjon som mulig. Derfor ble det foretatt samtaler/intervju med tre forskjellige ressurspersoner innen helsevesenet.

## *4.1 Contextual Design*

Contextual Design [5] er en metode som har til mål å definere krav til kundeorienterte systemer. Selve designet av en modell har seks forskjellige deler. Den syvende delen av figuren under, er den delen der et system er ferdig utviklet og hvor dette systemet blir implementert i en organisasjon eller lignende.

Contextual Design ble brukt siden dette er en modell hvor kunden behov står i fokus. Vi stod på bar bakke i forhold til hvordan vi skulle utvikle løsningsforlag for den aktuelle problemstilling. Det var derfor viktig å få innformasjon fra den målgruppen oppgaven rettet seg mot




FIGUR 4.1 CONTEXTUAL DESIGN (OVERSATT ETTER [6])

Derfor går det an å si at Contextual design består av de seks forskjellige trinnene:

*Trinn 1: Kontekstuell undersøkelse*
*Trinn 2: Tolke data*
*Trinn 3: Konsolidering*
*Trinn 4: Endring av arbeidspraksis*
*Trinn 5: Bruker miljødesign*
*Trinn 6: Prototyper til kunder*

Vi begynte med å samle inn informasjon (trinn 1). Deretter følgte vi modellen videre til og med til trinn 5, som figuren over viser. Trinn 6 og 7 tar for seg hva som skjer etter at et løsningsforslag er foreslått, testing av løsningsforslaget og hvordan implementeringen av løsningsforslaget etter det er blitt ferdig testet blir gjort. Disse to trinnene ble ikke brukt i vårt prosjekt. Vi gikk aldri tilbake til de ressurspersonene informasjonen ble hentet fra. Siden det neste steget i prosjektet vil være å gå tilbake til ressurspersoner og interesserte parter med løsningsforslag for synspunkter og testing er allikevel trinn 6 av modellen nærmere beskrevet, sammen med de trinnene som ble brukt. Det vil ikke være noen nærmere beskrivelse av trinn 7, siden modellen er blitt slått sammen til 6 trinn.[5]

Under blir de forskjelllige trinnene [6] presentert.

**Trinn 1 - kontekstuell undersøkelse**

Den første utfordringen for å kunne utvikle noe for noen, er å skjønne de behov målgruppen for et ferdig utviklet system/prosjekt har. Ved behov menes hva

målgruppen trenger, hvordan de jobber osv. *Kontekstuell undersøkelse* avdekker hvem kunden er og hvordan de nåværende arbeidsmetodene er.

For å få oversikt over de daglige rutinene og hvordan de forskjellige aktørene i helsevesenet jobber, er planen å ta kontakt med tre ressurspersoner innenfor tre forskjellige deler av helsevesenet (se kap.4.3). Etter disse samtalene skal informasjonen bli skrevet ned og behandlet.

### Trinn 2 – Tolke data

*"Måten folk jobber på er kompleks og full av detaljer"* [6]. Det er derfor viktig å behandle den informasjonen som har blitt hentet frem ved hjelp av *kontekstuell undersøkelse.* Denne behandlingen fører til at det kan settes opp ulike modeller for å sette forskjellige områder av en arbeidsplass i perspektiv. Eksempler på noen av disse modellene kan være *flytmodell,* som tar for seg kommunikasjon og koordinasjon, *sekvensmodell,* som viser detaljerte steg for å utføre en oppgave, og *fysisk modell,* som viser hvordan det fysiske miljøet støtter arbeidet.

Det vil i rapporten bli presentert flyt modeller av forskjellige typer.

### Trinn 3 – Konsolidering

Det er sjelden at et system blir designet bare for en enkelt kunde. Derfor blir den informasjonen som blir hentet inn fra en kunde ofte sammenlignet med informasjon fra andre kunder. Denne sammenligningen blir brukt for å kunne finne en felles plattform for mange kunder, slik at det ikke trengs å finne en ny plattform for hver kunde. For å utarbeide dette brukes en *Konsolideringsmodell.*

Den informasjonen som hentes inn i dette prosjektet er hentet inn fra tre forskjellige ledd av helsevesenet. Alle disse leddene har forskjellige ønsker, innarbeidede rutiner og arbeidsmetoder. Derfor må den informasjonen som hentes inn fra de tre leddene samkjøres for å kunne finne en felles løsning som kan tilfredsstille alle parter på best mulig måte.

### Trinn 4 – Endring av arbeidspraksis

I *endring av arbeidspraksis* - brukes den løsningen som har blitt funnet, som en felles løsning for alle kunder, til å se på hvordan arbeidspraksisen til kunden kan forandres og forbedres i forhold til dette. Videre blir det sett på hvordan den aktuelle teknologien som er tenkt brukt, kan forbedre og forenkle de daglige rutiner og arbeidsoppgaver. Det blir brukt gule lapper, skisser osv. på dette tidspunkt av prosessen.

Det vil i denne rapporten først bli sett på dagens situasjon, med tanke på en diabetespasient, og de utfordringer han/hun står overfor med sin sykdom. Deretter vil

det bli sett på løsningsforslag som også tar for seg hvordan en diabetespasient kan få hjelp av elektroniske hjelpemidler til å lette sin behandlingssituasjon.

**Trinn 5 – Brukermiljø design**

Den nye modellen som blir utarbeidet må støtte en god arbeidsflyt. Derfor blir det satt opp en plattform for hvordan denne flyten skal gå*. "Denne plattformen skal vise hver del av systemet, hvordan den støtter arbeidet som utføres av brukeren, hvilke funksjoner som er tilgjengelige i hver del og hvordan en bruker kommer til og fra andre deler av systemet uten å binde det opp mot et spesielt brukergrensesnitt".*[6]

Det vil senere i rapporten bli satt opp et eksempel på hvordan et grensesnitt mellom de forskjellige delene av løsningene fungerer sammen. Dette grensesnittet vil ikke være noe fastlagt grensesnitt, men en mulig løsning.

## *4.2 Vurdering av bruken av Contextual Design*

Det ble, som beskrevet i kapittelet over, brukt Contextual Design som arbeidsmodell i vårt prosjekt. Denne arbeidsmodellen var spesielt nyttig i begynnelsen av prosjektet da det ble samlet inn informasjon. Denne informasjonen gikk på helsevesenet, arbeidsmetoder i helsevesenet og diabetes. I ettertid ser vi at det hadde vært nyttig å hente inn informasjon om sikkerhets teknologier og bestemmelser på samme måte.

## *4.3 Intervju/samtaler med kommentarer*

Det ble arrangert møter med tre ressurspersoner på ulike områder innen helsevesenet. Disse møtene gav mye informasjon om hvordan dagens situasjon i helsevesenet er, og hvordan hver av de forskjellige ressurspersonene så på eventuelle forandringer med tanke på et felles helsenett.

De tre ressurspersonene som det ble foretatt samtaler med var:

*Nils Kristian Fjærbu, som jobber ved omsorgstjenesten i Grimstad kommune.*

*Dr. Håvard Skjærvik, privat praktiserende lege ved Stoa legesenter*

*Dr. Arne Quist-Paulsen, diabetesspesialist ved SSA*

# 5. Scenario

I dette kapittelet blir spørsmål/ opp et scenario. Scenarioet tar utgangspunkt i situasjonen til en diabetespasient med type 1-diabetes. Informasjonen som brukes er hentet fra et intervju med diabetesspesialist Arne Quist Paulsen.

Etter møtene/intervjuene kom det frem en del nye spørsmål/opplysninger som måtte svares på før det kunne settes opp et scenario og videre løsningsforslag. Under blir de spørsmålene som kom fram i samtalene nærmer diskutert.

***1.*** *For at et det skal være mulig for de forskjellige aktørene i helsevesenet å ha tilgang til en felles informasjonskilde, må først og fremst de grunnleggende systemene som de forskjellige aktørene bruker samkjøres. Her kan det f. eks nevnes at mange av sykehusene i Norge bruker forskjellige journalsystemer.*

Dagens arbeidsmetoder varierer veldig fra sykehus til sykehus. Noen sykehus har fortsatt ikke tatt i bruk EPJ i særlig stor grad, mens andre igjen har gått helt over til EPJ (f.eks. SSA). Dette fører til at det noen plasser må store forandringer til for å få gjennomført løsninger der alle har et felles helsenett. Dette kan fort ta mye tid, siden det kreves mye ressurser både økonomisk og arbeidsmessig for å gjennomføre.

På den annen side er det ikke noe problem å innføre et felles journalsystem med tanke på teknologien som allerede finnes.

***2.*** *Vil pasientenes verdier og interesser bli tatt hensyn til? I et slikt system må en passe på at de menneskelige verdier ikke blir glemt.*

I et system der mesteparten av kommunikasjonen foregår elektronisk vil det være viktig å ikke glemme at den menneskelige kontakten ikke kan erstattes. Med dagens teknologi er det mulig å lage opplegg for forskjellige pasienttyper, som vil gi pasienten mye av den oppfølgingen som trengs. Mange pasienter har ekstra stort behov for menneskelig omtanke og kontakt. Det er en viktig faktor at disse elementene i en pasients behandling ikke blir glemt.

Uansett er det nok ingen stor fare for at disse elementene blir glemt. Selv om en pasient kan få hjelp elektronisk til både selve behandlingen og til å forstå denne behandlingen bedre, vil alltid deler av en behandling bli gjort på et menneskelig plan, og derfor vil aldri de menneskelige verdiene bli glemt.

***3.*** *Hvem skal få rettigheter til å bruke systemet? Hvilke rettigheter skal de forskjellige aktørene ha?*

Alle aktørene av et felles helsenett skal ha mulighet for tilgang til det de har rettigheter til. Det er derfor viktig å sette klare grenser for hvilke rettigheter som tilhører hvem. Riktig bruk av disse rettighetene vil være viktig for å unngå konflikter med gjeldende lover og regler, f.eks. personvernloven.

Dette fører oss over på et annet viktig spørsmål.

***4.*** *Hvem er det som skal drifte og tildele rettigheter? Det vil være nødvendig med en ansvarlig part som har ansvaret. Hvem skal dette være?*

Datatilsynets regelverk vil legges til grunn for å avgjøre hvem som skal få hvilke rettigheter. Som tidligere nevnt vil også pasienten kunne avgjøre hvem han/hun vil skal få tillatelse til sine personopplysninger og i hvilke grad hver aktør skal ha tilgang til disse rettighetene.

***5.*** *For at det kunne innføres et slikt system må det finnes "kjøreregler" for hvordan rettighetene skal fordeles. For å styre dette må det legges til rette et nasjonalt lovverk*

Dette regelverket vil legges til grunn for å avgjøre hvem som skal få hvilke rettigheter. Som tidligere nevnt vil også pasienten kunne avgjøre hvem han/hun vil skal få tillatelse til sine personopplysninger og i hvilke grad hver aktør skal ha tilgang til disse rettighetene

***6.*** *Poenget med et slikt system vil være å øke kvaliteten til samme ressursbruk. Dette vil igjen øke effektiviteten. Vil dette skje?*

Meningen med å innføre et felles helsenett er å gjøre hverdagen lettere for både forskjellige typer helsepersonell og pasienter. Oppgaver skal kunne løses raskere samtidig som kvaliteten opprettholdes og økes. Et felles system, der informasjon ligger tilgjengelig for de som har rettigheter til den, vil føre til at informasjonsflyten vil gå raskere.

## *5.2 Dagens situasjon for en diabetes pasient*

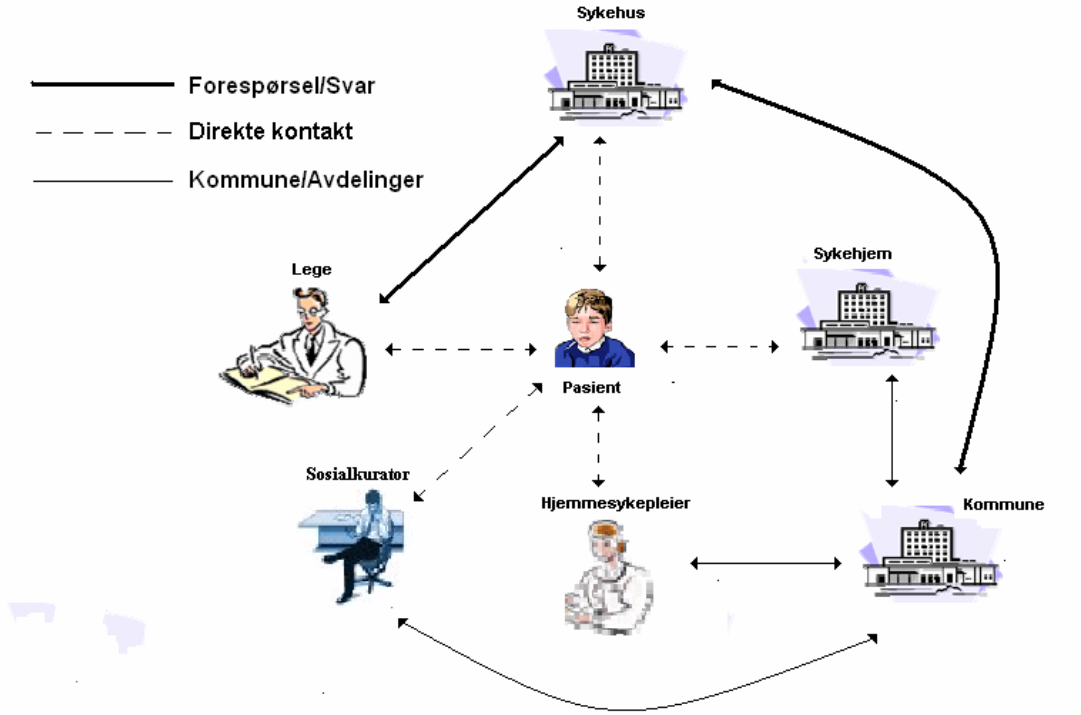
Ved oppdagelse av diabetes blir pasienten innlagt noen dager på sykehus. Her får pasienten full opplæring i hvordan livet vil bli framover, dvs. hvordan behandlingen foregår, hvordan måling av blodsukker foretas, hvordan disse skal forståes og hva slags kosthold pasienten bør ha. I tillegg får pasienten råd om arbeid, lån og trygd.

Etter opplæringsperioden vil pasienten gå periodisk til kontroll på sykehuset. I begynnelsen er pasienten inne hver uke, men etter hvert som pasienten blir tryggere på seg selv øker intervallet mellom hver kontroll. Når en pasient er fullerfaren, er han/hun inne til kontroll en gang i året på sykehuset og bruker fastlege ellers.

Måling av blodsukker gjør pasienten hjemme hos seg selv. Resultatene føres inn i en diabetesdagbok som pasienten tar med seg på hver legesjekk. Pasienten har også en egen journal, hvor det blir skrevet inn hvordan behandlingen blir foretatt, f.eks. mengden insulin som brukes, hvordan medisinforbruket er, hvilke prøver og undersøkelser som er foretatt i løpet av året og resultater av disse. Pasienten kan også gi en vurdering av sin egen livssituasjon i journalen.

Hvis pasienten går til fastlege for å foreta helsesjekk, må legen få tilsendt helsejournalen fra sykehuset.

En diabetespasient kan også ha hyppige møter med en sosialkurator som gir råd om hvilke valg pasienten kan ta videre.




FIGUR 5.1 DAGENS SITUASJON

Som man ser på figuren er det tre typer informasjonsflyt. Forespørsel/Svar, Direkte kontakt og Kommune/Avdelinger.

Forespørsel/Svar: fastlege eller kommunale avdelinger trenger deler av sykehusets pasientjournal ved behandling av pasient, og sender derfor en forespørsel om dette. Får så svar tilsendt via post eller faks.

Direkte kontakt: pasienten tar fysisk kontakt med fastlege, sykehus eller de kommunale underavdelinger for å foreta tester, behandling, kurs eller for å få råd.

Kommune/Avdelinger: Sosialkurator, hjemmesykepleier og sykehjem er alle kommunale avdelinger. Det kan være mulighet for at de forskjellige avdelingene bruker forskjellige informasjonssystemer. Dette må samkjøres før det kan foregå samhandling mellom dem.

## *5.3 Scenario-beskrivelse*

Scenarioet tar utgangspunkt i at det er oppdaget at en pasient har diabetes. Ut i fra dette sammenliknes dagens situasjon med hvordan det vil bli etter innføring av elektronisk samhandling, for å finne ut av hvilke forskjeller dette gir i en behandlingssituasjon.

Elektronisk samhandling kan ikke erstatte faglig personell når det gjelder opplæring av pasienten. Dette fordi man må ta hensyn til de menneskelige verdier, og at pasienten må få en fullgod opplæring i utstyret som skal brukes. Elektronisk samhandling kan derimot brukes som et hjelpemiddel til pasienten. Hvis han/hun, etter å ha kommet hjem, ikke føler seg helt trygg på elementer ved behandlingen, er det bare å ta i bruk de hjelpemidlene som ligger tilgjengelig i databasen. Hvis det skal tas i bruk database, må selvfølgelig pasienten også få opplæring i bruk av denne.

Ved hjemmebehandling fører pasienten dataene sine inn i bøker som taes med til hver lege sjekk. Dette kan nå elektronisk føres inn i en database. Med elektronisk samhandling kan dermed legen få hyppigere tilgang til pasientens data, og kan gi skriftlig tilbakemelding på disse

Hvis pasienten går til fastlege, må i dag fastlegen få pasientens helsejournal tilsendt fra sykehuset. Ved bruk av elektronisk samhandling, kan legen hente disse opplysningene rett ut av nettet.

Elektronisk samhandling kan redusere antall møter med sosialkurator. Pasienten kan bruke nettet til å stille spørsmål, som sosialkuratoren svarer på.

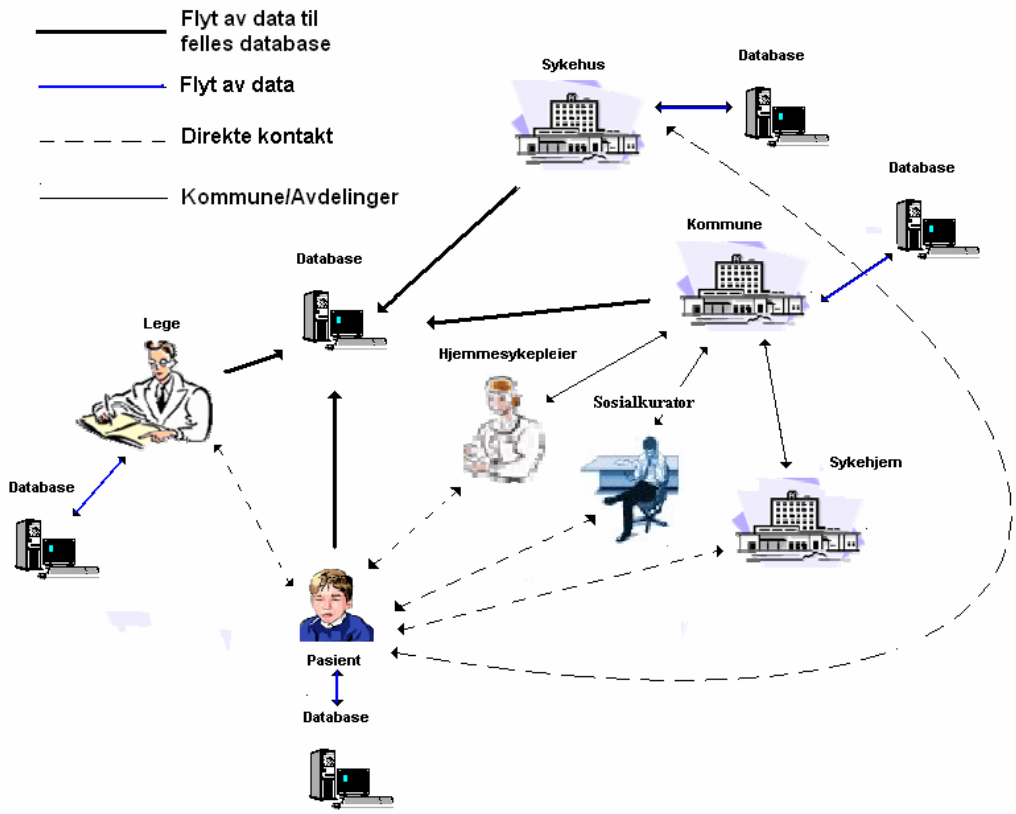
## *5.4 De forskjellige løsningsforslagene*

### 5.4.1 Løsningsforslag 1 – Felles database

Dette løsningsforslaget tar utgangspunkt i en felles database for pasient, sykehus og fastlege, pluss tjenestesykepleier, sosialkurator og sykehjem som styres av kommunen. Helseaktørene sender bare den mest nødvendige informasjonen fra sine egne journaler inn til databasen, slik at dette kan nyttes av de andre aktørene uten å bryte Datatilsynets regelverk med hensyn på personvern og lignende. F.eks. kan diabetesspesialisten daglig gå inn i databasen og sjekke den informasjonen pasienten har lagt inn, og dermed ha kontroll på pasientens målinger og tester.

Denne databasen styres av f.eks. sykehus eller kommune, etter hvem som tar seg råd til dette, i samtykke med pasient. Dvs. at pasienten ikke blir ført inn i databasen hvis denne ikke ønsker det.

På tegningen er det også tatt med den direkte kontakten mellom partene.




FIGUR 5.2 FELLES DATABASE

På denne tegningen er det fire forskjellige typer informasjonsflyt. Flyt av data til felles database, Flyt av data, Direkte kontakt og Kommune/Avdelinger. Direkte kontakt er forklart i delkapittel 5.1.

Flyt av data til felles database: De forskjellige helseaktørene sender informasjon fra sine databaser inn til fellesdatabasen.

Flyt av data: Flyt av data mellom helseaktørene og egen database.

Kommune/Avdelinger: De forskjellige avdelingene har samkjørt informasjonssystemene sine, og kommuniserer med Fellesdatabasen via kommunen.

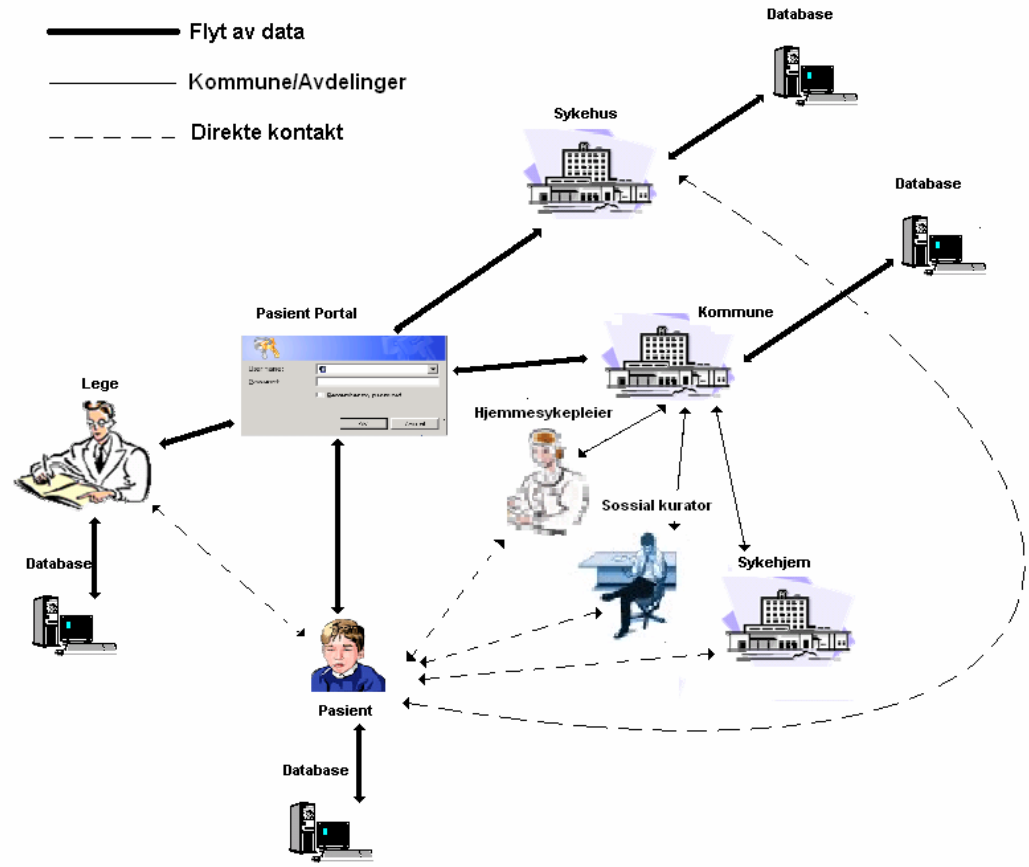
### 5.4.2 Løsningsforslag 2 – Portal-løsning

Denne løsningen går ut på at pasienten får satt opp sin egen portal. Det tas utgangspunkt i at pasienten eier sin egen journal, og har derfor full tilgang til denne.

Denne portalen kommer i tillegg til det systemet helsesektoren velger å bruke. Den gir pasienten muligheten til å gi innloggingsmuligheter til den han/hun ønsker. Det vil si at pasienten f.eks. kan gi sin fastlege mulighet til å logge seg inn i sykehusets

database og motsatt. Dermed kan pasienten gi full elektronisk kommunikasjon mellom helseaktørene og ha full kontroll over sin helse.

I tillegg til å styre innloggingsmulighetene, kan pasienten også styre lese- og skriverettighetene til portalen.




FIGUR 5.3 PORTAL-LØSNING

På tegningen under ser man at det er tre forskjellige typer informasjonsflyt. Flyt av data, Kommune/avdelinger og Direkte kontakt. Kommune/Avdelinger er presentert i kapittel 5.3.1 og Direkte kontakt er presentert i kapittel 5.1.

Flyt av data: Flyt av data gjennom en portal som styrer dataflyten mellom riktige helseaktører, slik at de forskjellige helseaktørene kan få tilgang til hverandres databaser.

## *5.5 Løsningsforslagene sammenlignet med pågående prosjekter*

# 6. Sikkerhetsteknologier

I dette kapittelet beskrives de forskjellige sikkerhets teknologiene som brukes til å sette opp en sikkerhetsarkitektur for de to løsningsforslagene. Disse sikkerhetsarkitekturene settes opp i kapittel 7.

## *6.1 Secure Socket Layer (SSL)*

Secure Socket Layer (SSL) [7] er en protokoll som sikrer overføring av data over Internett. Den er integrert i de fleste nettlesere og tjenere. SSL bruker privat/offentlig nøkkel for kryptering og dekryptering av data. For å kunne sette opp en SSL–forbindelse må tjeneren/databasen ha installert et digitalt sertifikat (se kap.6.2).

SSL tar i bruk to metoder for å sikre dataoverføring:

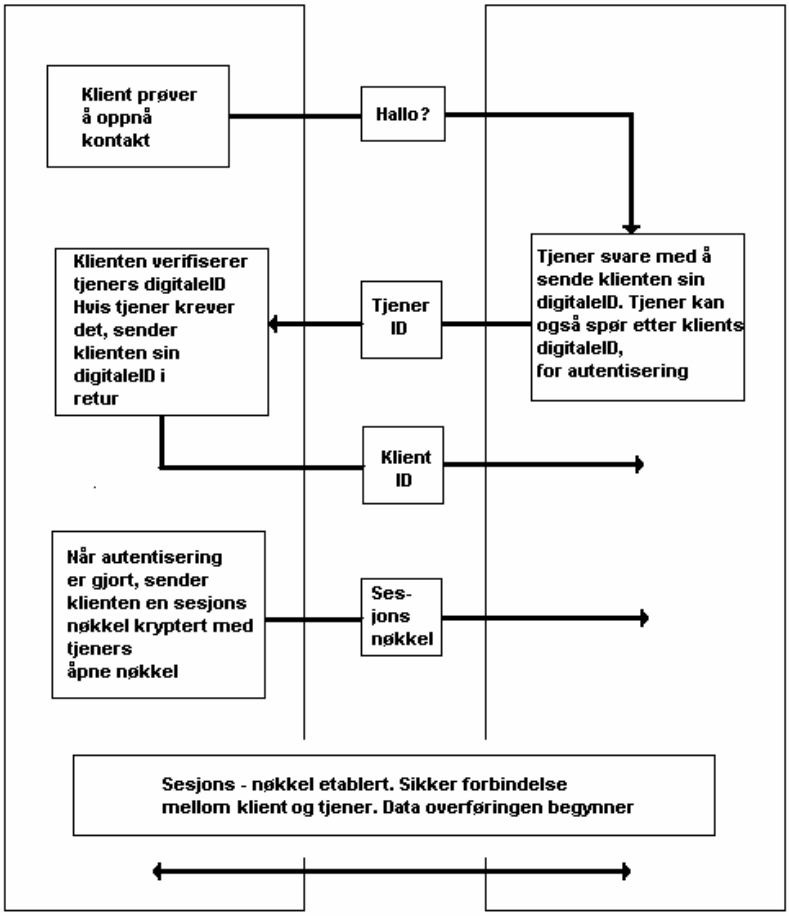
1. Autentisering

   Hvert digitalt sertifikat er bundet opp mot et spesielt domene. SA (se kap.6.2) utfører forskjellige tester for å bekrefte identiteten til den som bruker sertifikatet er riktig. For å sikre en bruker er det bare nødvendig å ha installert sertifikatet på det domenet det har blitt autentisert for.

2. Kryptering

   Kryptering er en prosess som gjør den informasjon/data som blir sendt uforståelig for alle andre enn den informasjonen er ment for.

SSL–protokollen begynner med en handshakefase som avtaler krypteringsalgoritme og nøkler. Samtidig autentiserer tjener seg mot brukeren. Autentiseringen kan også foregå motsatt vei. Altså at brukeren autentiserer seg mot tjeneren. All data blir kryptert ved hjelp av en spesiell sesjonsnøkkel. Etter at denne sesjonsnøkkelen er bestemt er den sikre linjen satt opp og overføringen av data kan begynne. Figuren nedenfor viser hvordan oppkoblingen av SSL foregår.




FIGUR 6.1 OPPKOBLING AV SSL[7]

Under følger en detaljert beskrivelse av hvordan SSL forbindelsen settes opp.

1. Det første som skjer når pasienten går inn på Internettsiden er at nettleseren sender sitt SSL versjonsnummer og kryptografien til serveren. Nettleseren sender sin kryptografi fordi den skal avtale med tjeneren hvilken nøkkelalgoritme som skal brukes.

2. Serveren sender så sitt SSL nummer, kryptografi og sitt digitale sertifikat til nettleseren. Som beskrevet i kapittel 6.2 om digitale sertifikat inkluderer serveren RSA åpen nøkkel, som er verifisert av et SA. Sertifikates åpne nøkkel har blitt kryptert av en privat nøkkel utstedt av et SA.

3. Nettleseren har en liste over SA-er og en tilhørende åpen nøkkel til hver av disse. Når nettleseren mottar sertifikatet fra serveren sjekker den sin liste for å se om den finner SA-et i sin liste. Gjør den ikke det blir pasienten varslet om at det ikke kan bli satt opp noen kryptert og autentisert tilkopling. Pasienten blir dermed nektet tilgang til nettsiden.

   Hvis nettleseren har SA-et i sin liste bruker den SA-ets åpne nøkkel til å dekryptere sertifikatet for å få serverens åpne nøkkel.

4. Nettleseren lager så en symmetrisk sesjonsnøkkel, krypterer den med serverens åpne nøkkel og senderen den krypterte sesjonsnøkkelen til serveren.

5. Nettleseren sender så en beskjed til serveren som informerer om at de fremtidige meldingene fra klienten vil være kryptert med den allerede bestemte sesjonsnøkkelen.

   Deretter sender den en kryptert melding om at nettleserens er ferdig med sin del av oppkoblingen (handshake).

6. Serveren sender en melding til nettleseren om at fremtidige meldinger fra tjeneren vil være kryptert med den allerede bestemte sesjonsnøkkelen.

   Deretter sender den en kryptert melding om at serveren er ferdig med sin del av oppkoblingen (handshake).

SSL-oppkoblingen er gjennomført.

## *6.2 Virtual Private Network (VPN)*

En VPN (Virtual Private Network) [8] er en autentiserings og krypteringskommunikasjonskanal som går over et åpent nettverk (F. eks Internett). VPN sørger for å opprette en tunnel mellom sender og mottaker av de sendte data. I stedet for at all data sendes åpent over Internett, kan denne dataen ved hjelp av VPN sendes kryptert og uleselig for andre gjennom VPN tunnelen

For at VPN skal kunne brukes kreves det at de to partene som skal bruke funksjonen har blitt enige om noen punkter på forhånd:

- Begge nettsteder/brukere må sette opp VPN støtte på nettverket. Dette kan gjøres i router, brannmur osv. Det finnes også egen VPN software
- Begge nettsteder/brukere må vite subnett adressen til det andre nettsted/bruker
- Begge nettsteder/brukere må avtale autentiserings mekanisme. De må også utlevere digitale sertifikater til hverandre.
- Begge Nettsteder/brukere må avtale krypterings metode/algoritme. De må også utlevere krypterings nøkler til hverandre

Det finnes to hovedtyper for tunnelering. Ende-til-ende tunnelering og node-til-node tunnelering. Ende-til-ende tunneler brukes for å opprette sikker kommunikasjon mellom to systemer, f. eks en arbeidsstasjon og en server. Her er de enkelte systemene ansvarlige for å etablere tunnelene, kryptere og autentisere dataene.

Node-til-node tunneler brukes for å kople sammen to ulike nettverk (LAN). De enkelte systemene (arbeidsstasjoner, servere) på de to LAN-ene kommuniserer som om de

skulle være på sammen nettverk, og VPN-systemer, ett på hvert LAN, overfører kommunikasjonen mellom de to nettverkene.

Som nevnt over finnes det flere muligheter for hvor VPN skal integreres. De to mest brukte metodene er VPN i brannmur og VPN i router. Disse metodene forklares mer detaljert nedenfor. VPN som egen software vil ikke bli beskrevet i detalj i denne rapporten.

**VPN i brannmur,** er den mest brukte metoden for integrering av VPN. Denne type bruk av VPN fører til en god sammenheng mellom brannmursikkerheten og den trafikken som skal slippes igjennom til enden av tunnelen.

Ulempen med denne type bruk av VPN kan være ytelsen. Hvis det er mye trafikk i nettverket og all denne trafikken krever høy kryptering, kan dette føre til overbelasting av nettverket. I et normalt belastet nettverk er sannsynligheten for at dette skjer liten.

**VPN i router.** Her er VPN-en integrert i Internett-routeren. Ved bruk av denne typen VPN vil all trafikk bli dekryptert før den kommer til brannmuren. Den store ulempen ved bruk av VPN i router er at sikkerheten er dårligere i forhold til i en brannmur. En ”hacker” kan lure trafikk, som for routeren ser ut som trafikk fra andre enden av tunnelen, forbi routeren.

## *6.3 Distribuert Database*

En distribuert database henter inn informasjon om de andre databasene i nettverket eller andre nettverk. Den oppdaterer seg selv jevnlig, eller den blir oppdatert da de henter informasjon fra andre nettverk når en bruker spør etter den. Distribuert database inneholder som regel ingen lagret data, men bare informasjon om hvor de forskjellige dataene ligger.

## *6.4 Digitale sertifikater*

Digitale sertifikater[9] er en måte å oppgi hvem man er elektronisk, dvs. en elektronisk legitimasjon. Dette er spesielt brukt over åpne nett som f.eks. Internett. Digitale sertifikater brukes også til å bevise at den digitale signaturen er gyldig og ekte.

For å bevise at sertifikatet er ekte må det være utstedt og signert av en Sertifikat Autoritet (SA). I Norge blir de fleste sertifikater utstedt av Telenor og Posten. Disse har gått sammen om et samarbeid som kalles ZebSign.

## 6.5 Digitale signaturer

Digitale signaturer[9] benyttes for å verifisere dataintegritet. Hvis et dokument blir forsøkt forandret på blir den digitale signaturen ugyldiggjort. Samtidig går det ikke an å forfalske en digital signatur.

Meningen med en digital signatur er å verifisere at f.eks. et mottatt dokument er fra den brukeren som senderen utgir for seg å være. Før sending underskriver senderen dokumentet med sin signatur. I tillegg fører den digitale signaturen til at mottakeren merker hvis dokumentet har blitt forandret på under sending.

Genereringen av en digital signatur utføres ofte av en offentlig nøkkel. Dette gjøres ved at avsenderen av informasjonen krypterer informasjonen ved hjelp av sin private nøkkel. Mottakeren kan så dekryptere meldingen ved hjelp av avsenders offentlige nøkkel. Hvis mottaker er sikker på at den offentlige nøkkelen tilhører avsender kan han være sikker på at meldingen kommer fra avsender og ingen andre.

Dette er ikke sikkert hvis en uvedkommed har fått tak i avsenders private nøkkel. For å unngå at dette skjer byttes ofte nøkkelparene etter en viss tid. Dermed vil det bli vanskeligere for uvedkommende å utgi seg for noen de ikke er.

## 6.6 Passordbeskyttelse

Meningen med passordbeskyttelse[9] er å begrense tilgangen til de som har aksessrettigheter. Passord blir brukt sammen med brukernavn. Dette er en ofte brukt metode i f.eks. nettbanker.

For at det ikke skal bli for enkelt må et passord inneholde minst seks tegn. Disse tegnene skal inneholde både bokstaver og tall. Det er også en ide å bare ha samme passordet i begrensede tidsperioder. Dvs. at hver bruker velger nytt passord f.eks. hver sjette måned. Passordet skal heller ikke ha noen bakgrunn i relaterte ting eller datoer til brukerne. Dette vil føre til at de blir lette å gjette. Dermed er det også lettere for andre brukere å gjette seg til passord og også benytte andres kontoer.

## 6.7 Brannmurteknologi

*"En brannmur er et system eller en gruppe systemer som utfører aksesskontroll når trafikken går gjennom et aksesspunkt i et nettverk. Etter at nivået på tilkoblingen er satt, er brannmurens jobb å sikre at det ikke slippes igjennom uønsket trafikk" [oversatt fra 8]*

De tre mest vanlige type brannmurer[8] er:

- Statisk pakkefiltrering
- Dynamisk pakkefiltrering
- Proxy

Under vil disse typene bli beskrevet nærmere.

### Statisk pakkefiltrering

Statisk pakkefiltrering[8] bruker den informasjonen som ligger i headeren til å kontrollere trafikken. Den informasjonen som ligger i headeren er:

- Destinasjon og kilde IP – adresse eller subnett
- Destinasjon og kilde portnummer
- TCP flagg

Informasjonen fra en pakke blir sammenlignet med det som denne type brannmur slipper igjennom. Hvis informasjonen den finner ikke stemmer overens som den skal, blir pakken kastet.

Statisk pakkefiltrering blir sett på som en noe primitiv type brannmur, spesielt imot angrep som er av den mer avanserte typen. Derfor brukes mange ganger bare en ruter i stedet for denne typen, siden en ruter kan utføre samme type sjekk på egenhånd.

### Dynamisk pakkefiltrering

En dynamisk pakkefiltreringsbrannmur[8] har samme funksjonene som en statisk pakkefiltreringsbrannmur. Men den har en viktig tilleggsfunksjon, tilstandstabell. Det vil si at den hele tiden fører en tilstandstabell over de forskjellige tilkoplingene. Hvis det f.eks. blir sendt en ”fikset” pakke som ser ut som den kommer innenfra det nettverket som brannmuren beskytter, vil brannmuren oppdage dette siden den ikke har noen informasjon om at det er blitt opprettet en tilkobling fra innsiden i sin tilstandstabell.

**Proxy brannmur**

Ingen av de to foregående brannmurene som er beskrevet har noen form for sjekk av hva som egentlig er inne i pakken (nyttelasten). En kan si at en Proxy[8] er en overgangsplattform for trafikkflyten mellom to nettverk. Pakkene går gjennom Proxyen som undersøker nyttelasten. Noen ganger forandrer Proxyen nyttelasten slik at den skal passe inn i det nettverket den beskytter. F.eks. kan dette være ukjent Java-kode som ikke passer inn i nettverket.

Proxy kan også sørge for anonymitet når man er ute på Internett. Dette blir ordnet på den måten at Proxyen fjerner kilde IP-adressen og erstatter den med sin egen. Dermed kan man ”surfe” på sider som er beskyttet under denne Proxy brannmuren samtidig som den skjuler hvor en egentlig kommer ifra.

Proxy brannmur anses for å være tryggere enn f.eks. dynamisk pakkefiltrering siden den undersøker nyttelasten og ikke bare headeren.

## *6.8 Aksesskontroll*

Med aksesskontroll[8] menes det at kun de som er autorisert på forhånd har tilgang til informasjon. Det finnes to forskjellige aksesskontrolltyper:

*Mandatory Access Control (MAC).* De systemene som bruker MAC har man flere sikkerhetsnivåer og hver person i organisasjonen må klareres for et visst nivå. Denne typen aksesskontroll har ofte vært brukt i militære sammenhenger.

*Discretionary Access Control (DAC).* For organisasjoner som bruker DAC, er aksesskontroll basert på at hver informasjonsenhet ”eies” av en person, og det er opp til denne personen å gi videre tillatelser til å aksessere denne informasjonen. DAC har tidligere vært brukt i sivile organisasjoner og bedrifter

## *6.9 Rollebasert aksesskontroll*

Ved rollebasert aksesskontroll[10] er alle brukerne av systemet tildelt en rolle. Tilgangsrettigheter gis på bakgrunn av hva som er nødvendig i forhold til hvilke rolle hver enkel bruker har i f.eks. en organisasjon. Dette blir sett på som en enkel måte å styre aksesskontrollen på. Rollene kan bli bestemt ut ifra f.eks. hvilke posisjon en bruker har i en organisasjon eller hva som brukeren har behov for. Ofte går rollebasert aksesskontroll hånd i hånd med hvor langt opp i organisasjonshierarkiet en bruker er.

Man kan dele opp Rollebasert Aksesskontroll i to deler, statisk og dynamisk roller. Statisk rolle vil si at en bruker blir tildelt en fast rolle som sjelden blir forandret. Det betyr at en bruker med statisk rolle har samme aksessmuligheter hele tiden. Forandringer kan forekomme, men dette skjer sjelden.

Dynamisk rolle vil si at rollen en bruker har i organisasjonen skifter. Dermed må også tilgangsrettighetene skifte etter hvilke rolle brukeren har. En forutsetning for bruk av dynamiske roller er at rollefordelingen kan styres automatisk av systemet basert på informasjon lagret i systemets datalagre, uten noen form for manuell styring. Fordeler med denne formen for aksesskontroll er at det forenkler og forbedrer definering, endring og administrering av aksessrettigheter, samt at det muliggjør at én person kan ha ulike aksessrettigheter til ulike tider, avhengig av rollen personen innehar på aksesstidspunktet.

# 7 Forslag til sikkerhetsarkitektur

Dette kapittelet tar først og fremst for seg hva som må til for å få en sikker innformasjonsflyt i de to løsningsforslagene. Først blir de generelle punktene for sikkerhetsfunksjonalitet presentert. Deretter vil vi vise hvordan sikkerhetsoppbygningen i de to løsningsforslagene ser ut.

Kapittelet presenterer også et eksempel på hvordan et tenkt brukergrensesnitt, og bruk av dette for en diabetespasient, vil kunne se ut. Dette brukergrensesnittet vil være noe forenklet i forhold til hvordan det ville sett ut etter en innføring av et av løsningsforslagene, men vil gi en god indikasjon på hvordan funksjonaliteten vil være. Det vil også bli presentert hvilke sikkerhetsfunksjoner som blir brukt i forhold til diabetespasient-eksemplet.

## *7.1 Generell sikkerhetsfunksjonalitet*

### 7.1.1 Sikkerhet og konfidensialitet

For at et system som inneholder personlige opplysninger (sensitive opplysninger) skal kunne brukes kreves det full beskyttelse av disse opplysningene. Det vil si at de opplysninger som ligger i for eksempel en felles helsedatabase kun kan aksesseres av personen som eier opplysningene og de denne personen har gitt tillatelse til å gjøre det. For at dette skal kunne gjennomføres må det iverksettes sikkerhetstiltak som fører til at det blir full konfidensialitet rundt disse opplysningene.

Det første som må gjøres for å sikre disse opplysningene er å innføre:

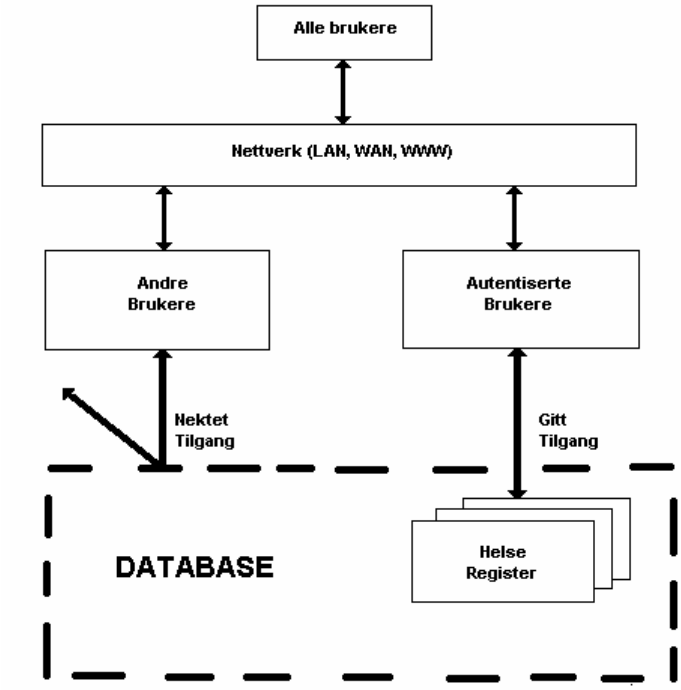
**Autentisering**, som er en prosess hvor en bruker identifiserer seg for et system eller beviser sine rettigheter til å benytte en identitet i et system.

**Tilgangskontroll:** Når en brukeridentitet er etablert/gjenkjent er det mulig å avgjøre om brukeren har lov til å for eksempel aksessere en fil. Med tilgangskontroll kan man også begrense tilgangen til å gjelde bare enkelte deler. Alt etter hvor mye rettigheter denne brukeren har.

**Autorisering:** betegner prosessen som gir en bruker lov til å gjøre noe i systemet. Denne prosessen kommer inn mellom autentisering og tilgangskontroll.

Disse tre prosessene vil bli mer inngående beskrevet senere i kapittelet.

Figuren under viser et bilde på hvordan en autentisert bruker får lov til å aksessere en database hvor helseopplysninger ligger, mens en bruker som ikke har autentisert seg blir avvist.




FIGUR 7.1 AUTENTISERT/IKKE AUTENTISERT

Selv om de tre nevnte prosessene sikrer at brukeren som vil bruke systemet er en kjent bruker som har rettigheter til å bruke systemet er ikke dataene som blir sendt sikret enda. All data som sendes over nettet er i utgangspunktet leselig for alle. Det er derfor nødvendig å gjøre noe slik at all informasjon som sendes blir uleselig for alle andre enn de som sender og mottar den. For å sikre dette brukes en **krypteringsprosess**. Denne prosessen brukes allerede under autentiseringen av en bruker, siden det ofte brukes både brukernavn og passord når en bruker registrerer seg. Ved bruk av kryptering vil både brukernavn og passord være uleselig når disse blir sendt til databasen for autentisering/registrering og godkjenning. Også denne prosessen vil bli mer inngående beskrevet senere i kapittelet.

### 7.1.2 Autentisering

Ved bruk av autentisering i Web-tjenester er det viktig å skille mellom to hovedtyper autentisering, brukerautentisering og sesjonsautentisering. Når en bruker autentiseres gjøres dette først ved bruk av passord (se passordsbeskyttelse kap. 6.6), digitalt sertifikat (se Kap 6.4) og digitale signaturer (se Kap.6.5) Deretter genererer Web-serveren sende over denne identifikatoren hver gang den henter en side fra serveren og dermed autentisere seg selv. Brukerautentiseringen foregår en gang hver sesjon, mens sesjonsautentiseringen foregår hver gang nettleseren kobler seg opp mot serveren.

Når en brukeridentifisering gjøres over nettet kan dette gjøres på ulike måter. Det finnes innebygde mekanismer for dette i http–protokollen. Men det finnes også forskjellige applikasjoner som tar seg av dette.

### 7.1.3 Autorisering

Det er veldig viktig å beskytte sensitiv informasjon. Det er derfor viktig å passe på hvem som har tilgang til hva. Autorisering vil si at informasjonen som ligger tilgjengelig kan graderes i forhold til mye de forskjellige brukerne av systemet har rett til å få innsyn i. I mange tilfeller avgjøres dette med hvor mye ansvar hver enkelt har. Man kan også si hvilke rolle hver enkelt har.

Ved rollebasert aksesskontroll[10] er alle brukerne av systemet tildelt en rolle. Tilgangsrettigheter gis på bakgrunn av hva som er nødvendig i forhold til hvilke rolle hver enkelt bruker har i f.eks. en organisasjon. Dette blir sett på som en enkel måte å styre aksesskontrollen på. Rollene kan bli bestemt ut ifra f.eks. hvilke posisjon en bruker har i en organisasjon eller hva brukeren har behov for. Ofte går rollebasert aksesskontroll hånd i hånd med hvor langt opp i organisasjonshierarkiet en bruker er.

Man kan dele opp rollebasert aksesskontroll i to deler, statisk og dynamisk roller. Statisk rolle vil si at en bruker blir tildelt en fast rolle som sjelden blir forandret. Det betyr at en bruker med statisk rolle har samme aksessmuligheter hele tiden. Forandringer kan forekomme, men dette skjer sjelden.

Dynamisk rolle vil si at rollen en bruker har i organisasjonen skifter. Dermed må også tilgangsrettighetene skifte etter hvilke rolle brukeren har. En forutsetning for bruk av dynamiske roller er at rollefordelingen kan styres automatisk av systemet basert på informasjon lagret i systemets datalagre, uten noen form for manuell styring. Fordeler med denne formen for aksesskontroll er at det forenkler og forbedrer definering, endring og administrering av aksessrettigheter, samt at det muliggjør at én person kan ha ulike aksessrettigheter til ulike tider, avhengig av rollen personen innehar på aksesstidspunktet.

For eksempel har en lege en annen rolle en sykepleier som jobber ved et sykehus. Dermed vil de to ha forskjellig rettigheter i forhold til en EPJ (Elektronisk Pasient Journal)

### 7.1.4 Tilgangskontroll

En bruker av et system får tildelt ulike rettigheter etter hvilke rolle denne personen har. Ved bruk av innlogging ut i fra brukernavn/passord brukes et register. Når en bruker logger på med sitt brukernavn/passord sjekkes dette opp mot registeret. Rettighetene til denne brukeren gis ut i fra hvilke rettigheter som ligger lagret på han/henne i dette registeret.

### 7.1.5 Kryptering

Som beskrevet tidligere er ikke en forbindelse sikker selv om den er satt opp ved hjelp av autentiseringsmekanismer. Dataflyten som går over denne forbindelsen sendes fortsatt åpen. For å unngå at dataflyten er leselig for andre enn senderen og mottaker bruker kryptering. Det vil si at de dataene som blir sendt gjøres uleselig for alle andre enn de som sender og mottar de sendte dataene. Dermed kan ikke en

ukjent tredjepart lese de dataene som blir sendt. Internett i seg selv inneholder ikke noen funksjoner som sørger for kryptering av data.

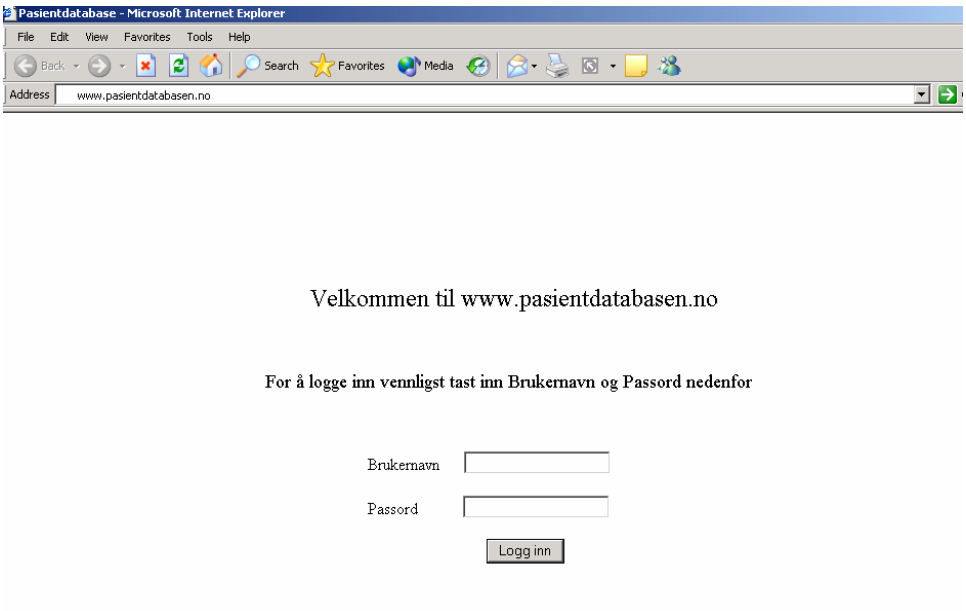
## 7.2 Sikkerhetsarkitekturen i løsningsforslagene

Her vil det bli presentert en sikkerhetsarkitektur for databaseløsningen. For bedre å vise hvordan de forskjellige typer sikkerhetsmekanismer som er valgt brukt, vises denne sikkerhetsarkitekturen i forhold til et eksempel/scenario med en diabetespasient.

Diabetespasienten har nettopp kommet hjem fra opplæringen som er gitt ved sykehuset. Han/hun skal nå begynne å måle blodsukkeret. Måling av blodsukker gjør pasienten hjemme hos seg selv. Resultatene føres inn i en elektronisk diabetesdagbok som ligger i den felles databasen. Pasienten har også en egen journal, hvor det blir skrevet inn hvordan behandlingen blir foretatt, f.eks. mengden insulin som brukes, hvordan medisinforbruket er, hvilke prøver og undersøkelser som er foretatt i løpet av året og resultater av disse. Pasienten kan også gi en vurdering av sin egen livssituasjon i journalen. Alt dette foregår elektronisk. I eksemplet som skal brukes ser vi på hvordan de forskjellige sikkerhetsmekanismene virker når pasienten legger inn sine måledata og hvordan sikkerhetsmekanismene fungerer når en lege ved sykehuset sjekker resultatene til pasienten.

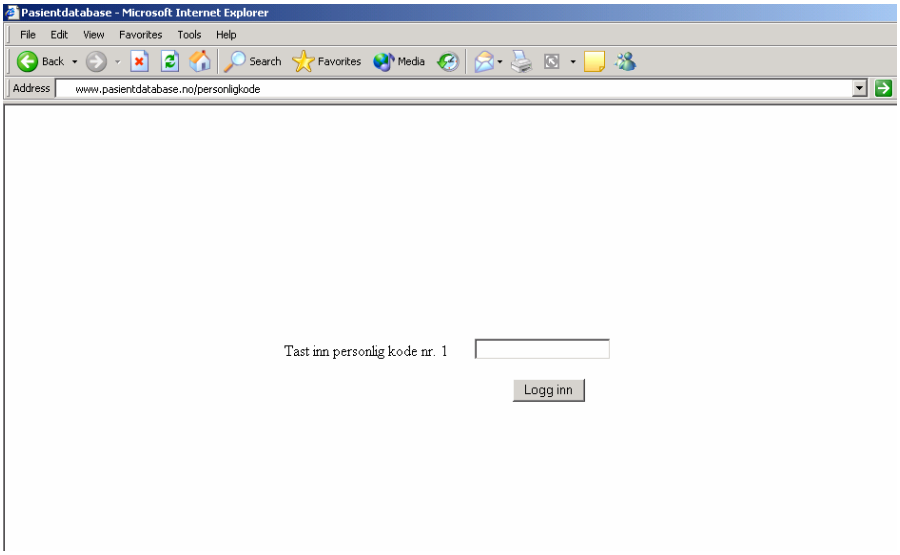
### 7.2.1 Sikkerhetsarkitekturen i databaseløsningen

**Grensesnitt**
Slik brukergrensesnittet er tenkt skal pasienten logge seg inn via en Internettside. På denne Internettsiden får pasienten opp en dialogboks der han/hun blir bedt om å skrive inn sitt brukernavn og passord.




FIGUR 7.2 PÅLOGGING AV PASIENT(DATABASE)

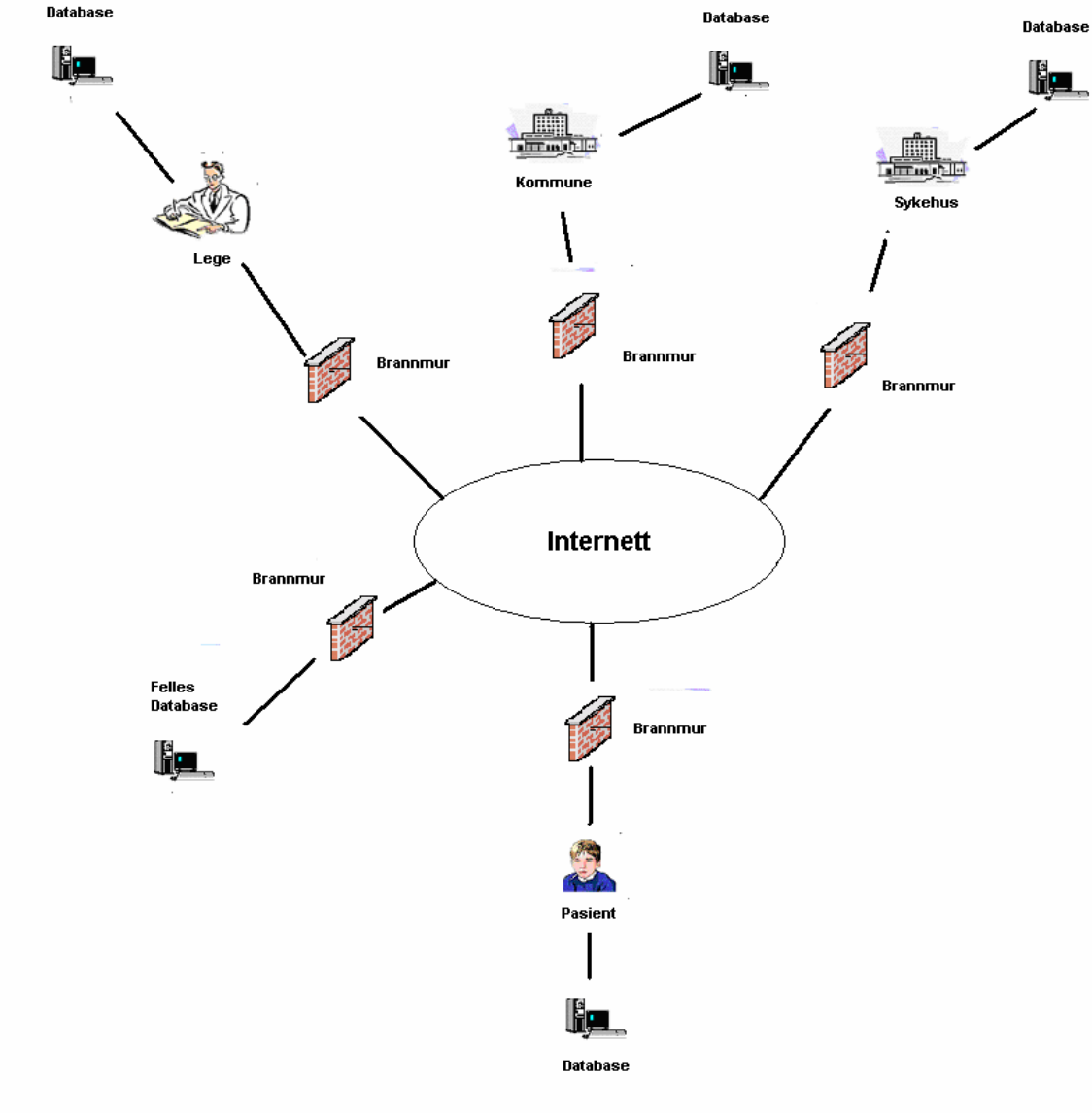
Både brukernavn og passord (se passordsbeskyttelse kap 6.6) er bestemt av pasienten selv og er registrert i databasen. Når pasienten har skrevet inn disse og trykket på innloggingsboksen får han/hun opp en ny side. Her møter pasienten en ny dialogboks som spør pasienten etter en hemmelig kode.




FIGUR 7.3 HEMMELIG KODE(DATABASE)

Denne hemmelige koden har pasienten mottatt via post på et kodekort som inneholder et visst antall koder som kan brukes en gang i riktig rekkefølge. Dette er samme prinsippet som brukes av mange nettbanker i dag.

## Sikkerheten som brukes bak grensesnittet




FIGUR 7.4 SIKKERHETSARKITEKTUR(DATABASE)

Den nevnte diabetespasienten har tatt sine daglige målinger av blodsukkernivået. Han/hun skal skrive inn dette i sin elektroniske dagbok som ligger i den felles databasen. Pasienten åpner sin nettleser. Deretter skriver han/hun inn adressen til den nettsiden som brukes for å gå videre inn i den felles databasen. Det blir da satt opp en forbindelse mellom nettleser og nett serveren. Forbindelsen som settes opp er en SSL forbindelse (se kap. 6.1). Kort sagt kan man si at SSL er en sikker forbindelse siden all data som blir sendt gjennom den er kryptert.

Når pasienten nå møter siden der han/hun skal skrive inn brukernavn og passord er den sikre forbindelsen allerede satt opp. Dermed er det ingen som kan se den informasjonen som blir sendt. Videre får pasienten opp en ny side med en ny dialogboks hvor han/hun skal skrive inn den hemmelige koden.

Når den hemmelige koden er skrevet inn og alt er riktig utført har pasienten registrert seg i databasen. Han/hun får å opp de forskjellige delene av den informasjonen som ligger tilgjengelig i databasen. Videre kan pasienten klikke seg inn på den delen (for eksempel den elektroniske dagboken) som han/hun vil, og kan lese og skrive inn informasjon her.

I databasen ligger det et register over de forskjellige brukerne. Ut ifra hvilke bruker som logger seg på blir det tildelt hvilke rettigheter hver av brukerne skal ha.

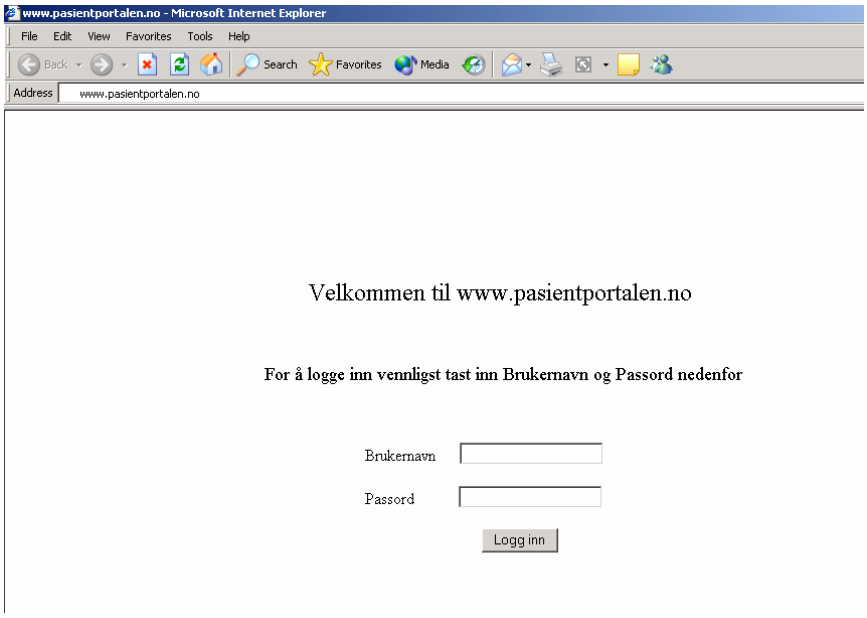
Når en lege har gått igjennom den samme innloggingsprosedyren som en pasient, møter denne legen en liste over hvilke pasienter han/hun har tilgang til. Videre kan da legen velge den pasienten som han/hun ønsker å få eller skrive inn informasjon om. Når legen logger inn vil hvilke rettigheter han/hun har i forhold til hver pasient avgjøres ut ifra brukerrettigheter som er tildelt i registeret.

Det er satt opp brannmur (se kap 6.7) på hver database for å beskytte mot ”hacker angrep”. Disse brannmurene logger også den trafikken som går inn til databasen.

### 7.2.2 Sikkerhetsarkitekturen i portalløsningen

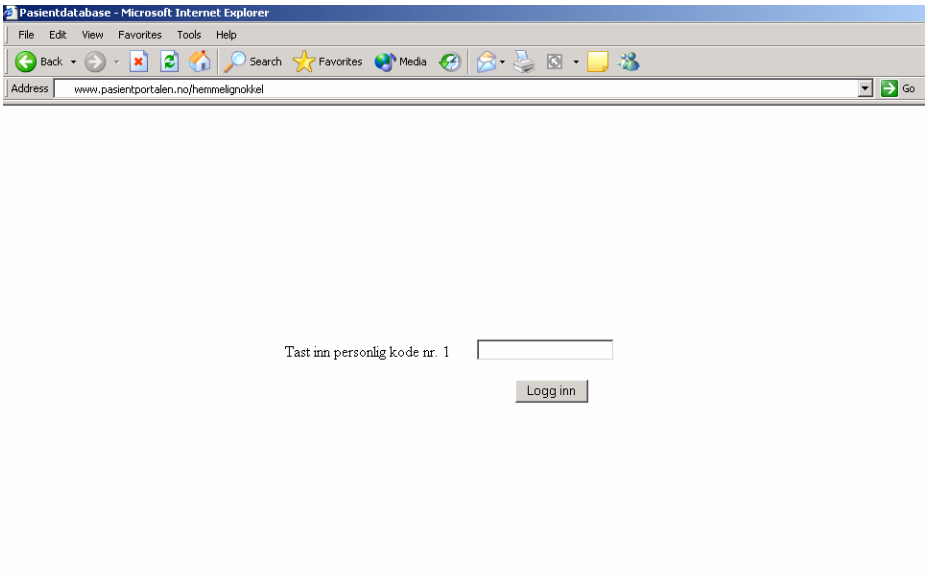
**Grensesnitt**

Selve innloggingsprosessen er lik som i databaseløsningen men blir beskrevet på nytt her også. Slik brukergrensesnittet er tenkt skal pasienten logge seg inn via en Internettportal. På denne Internettsiden får pasienten opp en dialogboks der han/hun blir bedt om å skrive inn sitt brukernavn og passord.




FIGUR 7.5 PÅLOGGING AV PASIENT(PORTAL)

Både brukernavn og passord (se passordsbeskyttelse kap 6.7) er bestemt av pasienten selv og er registrert i den distribuerte databasen. Det er en titrodd tredjepart som drifter den distribuerte databasen. Når pasienten har skrevet inn disse og trykket på innloggingsboksen får han/hun opp en ny side. Her møter pasienten en ny dialogboks som spør pasienten etter en hemmelig kode.

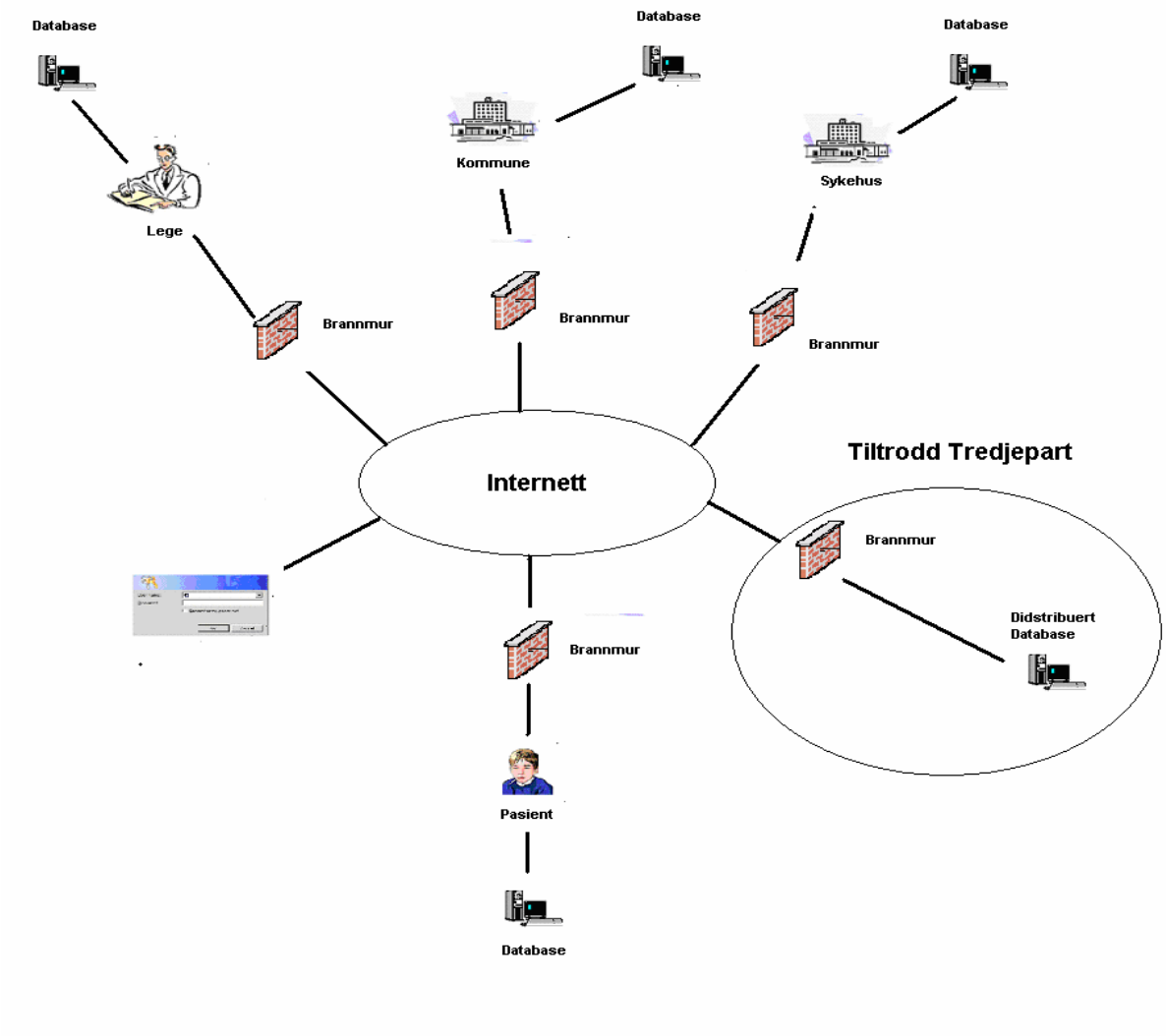



FIGUR 7.6 PERSONLIG KODE(PORTAL)

Denne hemmelige koden har pasienten mottatt via post på et kodekort som inneholder et visst antall koder som kan brukes en gang i riktig rekkefølge. Dette er samme prinsippet som brukes av mange nettbanker i dag.

Videre får pasienten opp en ny side som inneholder forskjellig informasjon og linker som er tilgjengelig for pasienten. Denne informasjonen kan være nyheter eller hjelp til fremgangsmåte. Linkene kan være linker til historikk på andre undersøkelser, linker til de forskjellige databasene som ligger tilgjengelig osv. Pasienten, som skal skrive inn sine måleresultater i den elektroniske dagboken, klikker på linken til sykehusdatabasen. Videre kommer pasienten inn i sykehusdatabasen hvor hans/hennes journal og også den elektroniske dagboken ligger. Pasienten kan nå skrive inn sine måleresultater i databasen.

## Sikkerhetsfunksjonene som brukes bak grensesnittet




FIGUR 7.7 SIKKERHETSARKITEKTUR(PORTAL)

Den nevnte diabetespasienten har tatt sine daglige målinger av blodsukkernivået. Han/hun skal skrive inn dette i sin elektroniske dagbok som ligger i sykehusets database. Pasienten åpner sin nettleser. Deretter skriver han/hun inn adressen til den nettsiden som brukes for å få opp portalen som han/hun skal logge inn via. Det blir da satt opp en forbindelse mellom nettleser og nettserveren. Nettserveren setter videre opp en forbindelse mellom seg selv og den distribuerte databasen(se Kap 6.3). Forbindelsene som settes opp er en SSL forbindelse (se kap. 6.1). Kort sagt kan man si at SSL er en sikker forbindelse siden all data som blir sendt gjennom den er kryptert.

Når pasienten nå møter siden/portalen der han/hun skal skrive inn brukernavn og passord er den sikre forbindelse allerede satt opp. Dermed er det ingen som kan se den informasjonen som blir sendt. Videre får pasienten opp en ny side med en ny dialogboks hvor han/hun skal skrive inn den hemmelige koden.

Når den hemmelige koden er skrevet inn og alt er riktig utført har pasienten registrert seg i den distribuerte databasen. I den distribuerte databasen ligger det et register over hvem som har tilgang til den distribuerte databasen og dermed også hvilke rettigheter de forskjellige personene har.

Når pasienten har kommet inn i den distribuerte databasen får han/hun opp forskjellig informasjon og linker. Informasjonen kan være nyheter, hjelp osv. Linkene vil for eksempel være linker til de forskjellige databasene som er tilgjengelig, historikk over tidligere behandlinger osv. All denne informasjonen er tilgjengelig for pasienten pga. den distribuerte databasen (se kap. 6.3) som idet pasienten logger inn, henter informasjon om hva som er tilgjengelig for han/hun i de forskjellige andre databasene (lege, sykehus og kommune).

Videre velger pasienten den databasen han/hun ønsker å aksessere ved å trykke på linken som ligger tilgjengelig. I dette tilfellet sykehusdatabasen. Det settes da opp en VPN-tunnel mellom den distribuerte databasen og sykehusdatabasen. Denne VPN-tunnelen settes opp av brannmuren som ligger foran den distribuerte databasen. Det vil si at funksjonalitet for å sette opp en VPN-tunnel ligger integrert i brannmuren (se ”VPN i brannmur” Kap.6.2)

Pasienten får nå tilgang til sin elektroniske dagbok i sykehusdatabasen og kan skrive inn sine måleresultater i denne.

Når en lege har gått igjennom den samme innloggingsprosedyren som en pasient møter denne legen en liste over hvilke pasienter han/hun har tilgang til. Videre kan da legen velge den pasienten som han/hun ønsker å få eller skrive inn informasjon om. Når legen logger inn vil hvilke rettigheter han/hun har i forhold til hver pasient avgjøres ut ifra brukerrettigheter som er tildelt i registeret.

Alle sikkerhetsfunksjonene når en lege logger inn vil være de samme som for en pasient. Nå kan legen lese de måleresultatene pasienten har skrevet inn og eventuelt gi kommentarer og råd i forhold til disse som pasienten kan lese neste gang han/hun logger på.

Det er satt opp brannmur (se kap 6.7) på hver database for å beskytte mot ”hacker angrep”. Disse brannmurene logger også den trafikken som går inn til databasen.

Brannmurene inneholder også funksjonalitet for å kunne sette opp VPN-tunneler.

# 8. Regelverk og sikkerhetsbestemmelser med kommentarer

Det finnes masse lover og forskrifter som må tas hensyn til. Det skal vurderes om det er mulighet for gjennomslag av rapportens scenario og løsningsforslag i forhold til disse lovene.

De aktuelle paragrafene i hver lov vil vurderes hver for seg for å gi et helhetlig bilde av de mulighetene som finnes.

## *8.1 Personopplysningsloven*

*"Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. Det vil si at når opplysninger behandles skal det tas hensyn til personlig integritet og privatlivets fred*."[11]

### 8.1.1 § 3. Saklig virkeområde

I følge *§ 3. (saklig virkeområde)* gjelder personopplysningsloven for:

- *"a) behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler, og"[11]*
- *"b) annen behandling av personopplysninger når disse inngår eller skal inngå i et personregister" [11]*.

Det vil si at begge løsningsforslagene, siden all behandlingen av opplysninger skjer ved hjelp av elektroniske hjelpemidler, vil komme under denne loven. Her vil ikke løsningsforslagene skille seg fra hverandre.

### 8.1.2 § 8. Vilkår for å behandle personopplysninger

*§ 8* sier blant annet at: "*Personopplysninger (jf. §2 nr1) bare kan behandles dersom den registrerte har samtykket".[11]*

Juridisk sett er det ingen grunn til at pasienten ikke kan eie sin egen journal, og dermed alle opplysninger om seg selv [se vedlegg B] For at det skal kunne innføres et helsenett der pasientens opplysninger ligger lagret på en felles database, og forskjellige typer helsepersonell skal kunne aksisere disse opplysningene, må en pasient i følge *§ 8* ha gitt samtykke til dette.

I løsningsforslag 1 – felles database vil det kunne være lettere for en pasient å gi samtykke til lagring av sine personopplysninger, siden det ikke er alle opplysninger som ligger lagret på databasen, men bare de mest nødvendige.

Løsningsforslag 2 tar sikte på en portal-løsning, hvor alle brukere som har fått tillatelse til det, kan få tilgang til alle personopplysninger om hver enkelt pasient. Dette kan bli vanskeligere for en pasient å gi tillatelse til. Fordelen her er at det er pasienten selv som bestemmer hvem som skal ha tilgang. Han/hun kan også bestemme hvilke journaler (pasient, sykehus, fastlege, kommune) hver bruker skal få tilgang til.

### 8.1.3 § 9 Behandling av sensitive personopplysninger

*§ 9* sier at: "*sensitive personopplysninger (jf. §2 nr 8 kan bare behandles dersom behandlingen oppfyller et av vilkårene i § 8* "

Det er *§ 2 nr 8c* som tar for seg helseopplysninger. I tillegg til denne paragrafen og *§ 8,* må også alle punktene under *§ 9* [11] gjelde.

De løsningsforslagene som er satt opp i prosjektet strider imot *§ 9* siden alle punktene i første ledd av paragrafen må dekkes, men *§ 9 andre ledd* sier:

> *"Ideelle sammenslutninger og stiftelser kan behandle sensitive personopplysninger innenfor rammen av sin virksomhet selv om behandlingen ikke oppfyller et av vilkårene i første ledd bokstav a - h. Behandlingen kan bare omfatte opplysninger om medlemmer eller personer som på grunn av sammenslutningens eller stiftelsens formål frivillig er i regelmessig kontakt med den, og bare opplysninger som innsamles gjennom denne kontakten. Personopplysningene kan ikke utleveres uten at den registrerte samtykker."[11]*

Hvis en da ser på helsevesenet som en ideell sammenslutning, og de forskjellige aktørene i helsevesenet (pasient, sykehus, fastlege, kommune) som stiftelser, vil løsningsforslagene tilfredsstille andre ledd og dermed også hele *§ 9* i personopplysningsloven.

På den annen side, om en ikke ser på helsevesenet som en sammenslutning og de forskjellige aktørene som stiftelser, vil ikke løsningsforlagene oppfylle de lover og regler som gjelder per i dag.

Også tredje ledd av *§ 9* kan åpne for løsningsforslagene. Den sier at:

> *"Datatilsynet kan bestemme at sensitive personopplysninger kan behandles også i andre tilfeller dersom viktige samfunnsinteresser tilsier det og det settes i verk tiltak for å sikre den registrertes interesser"[11].*

Ifølge tredje ledd må altså Datatilsynet gi spesiell tillatelse for at det skal kunne innføres en felles database for hele helsevesenet. Eller innføre en permanent lovendring som tillater dette.

### 8.1.4 § 13. Informasjonssikkerhet

Det meste av *§ 13* er vist nedenfor og sier

> *"Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger."*
>
> *"For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den behandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for Datatilsynet og Personvernnemnda."*
>
> *"En behandlingsansvarlig som lar andre få tilgang til personopplysninger, f.eks. en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd."[11]*

Denne paragrafen sier det meste om hvilke informasjonssikkerhetstyper som er nødvendig for at den personlige informasjonen kan behandles. Det er opp til den behandlingsansvarlige å se til at sikkerheten opprettholdes. Det vil si at det i et helsevesen må finnes en ansvarlige part. Denne ansvarlige parten må ha til oppgave å se til at alle sikkerhetskrav er tatt hensyn til. En annen oppgave for en sikkerhetsansvarlig ville være å tildele rettigheter til de forskjellige aktørene som bruker systemet.

Så lenge denne ansvarlige parten finnes, og pasienten i tillegg er med og bestemmer hvem som skal ha tilgang og også hvor mye tilgang som skal gis, vil denne paragrafen ikke skape noen hindring for noen av partene.

Hvem den ansvarlige part skal være er vanskelig å fastslå. Det kan f.eks. være sykehus, kommune eller staten. Det kan også være en uavhengig tredjepart som drifter og styrer nettet.

Det vil i tillegg være nødvendig med en god sikkerhetsarkitektur som sikrer konfidensialitet. Begge løsningsforslagene har dette.

### 8.1.5 § 15. Databehandlerens rådighet over personopplysninger

*§ 15* sier ar:
*"En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.*
*I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13." [11]*

Denne paragrafen omhandler som *§ 13* at det må finne en ansvarlig part som har ansvaret for at alt foregår på en sikker og riktig måte. Et felles helsenett, om det er en felles database-løsning eller en portal-løsning, vil ikke være mulig å gjennomføre uten denne ansvarlige parten.

I database-løsningen er det sykehus, kommune, stat eller en tiltrodd tredjepart som er den ansvarlige parten.

I portal-løsningen er det i utgangspunktet pasienten som er den ansvarlige part. Pasienten kan også få hjelp av en tiltrodd tredjepart

### 8.1.6 § 33. Konsesjonsplikt

Av *§ 33* går det klart frem at ved behandling av sensitive opplysninger kreves det konsesjonsplikt:

> *"Det kreves konsesjon fra Datatilsynet for å behandle sensitive personopplysninger. Dette gjelder likevel ikke for behandling av sensitive personopplysninger som er avgitt uoppfordret"[11]*

Av denne paragrafen går det klart frem at Datatilsynet må gi konsesjonsplikt til alle prosjekter og planer som tar mål av seg til å kunne tilby personopplysninger og sensitive opplysninger.

I database-løsningen velger pasienten selv om han/hun skal ha sine opplysninger lagret i databasen. I portal-løsningen er det pasienten som bestemmer hvem som har tilgang til sine journaler. Derfor kan man si at disse sensitive opplysingene er avgitt uoppfordret i begge løsningsforslagene.

## *8.2 Lov om helseregistre og behandling av helseopplysninger*

*"Formålet med denne loven er å bidra til å gi helsetjenesten og helseforvaltningen informasjon og kunnskap uten å krenke personvernet, slik at helsehjelp kan gis på en forsvarlig og effektiv måte. Loven skal sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekelig kvalitet på helseopplysninger." [12]*

### 8.2.1 § 3. Saklig virkeområde

*§ 3 i Lov om helse registre og behandling av helseopplysninger* sier at:

> *" Loven gjelder for*
>
> *1.behandling av helseopplysninger i helseforvaltningen og helsetjenesten som skjer helt eller delvis med elektroniske hjelpemidler for å fremme formål som beskrevet i § 1, og*
> *2. annen behandling av helseopplysninger i helseforvaltningen og helsetjenesten til slike formål, når helseopplysningene inngår eller skal inngå i et helseregister."[12]*

For løsningsforslagene i prosjektet vil det først og fremst være første ledd av *§ 3* som vil gjelde, En ser ut ifra denne paragrafen at det vil være helt nødvendig å tilfredsstille denne loven for å kunne bygge et felles helsenett.

### 8.2.2 § 16. Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet

Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet er noen av de viktigste faktorene når det gjelder sikring av sensitive og personlige opplysninger. For at det skal kunne fungere med et felles helsenett og for at dette nettet skal få aksept er det nødvendig at denne paragrafen dekkes. *§ 16* sier:

> *"Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger.*
>
> *For å oppnå tilfredsstillende informasjonssikkerhet skal den databehandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den databehandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.*
>
> *En databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd."[12]*

Også i denne paragrafen kommer nødvendigheten av å ha et ansvarlig ledd, som styrer et eventuelt felles helsenett frem.

En ser i tillegg at det er veldig viktig å kunne dokumentere alt som er planlagt og tenkt utført. Dette er spesielt viktig ikke bare for å tilfredstile lovverket, men også for å kunne skape tillit hos tvilende parter.

Begge løsningsforslagene er godt dokumentert.

## *8.3 Fra lov om pasientrettigheter*

*"Lovens formål er å bidra til å sikre befolkningen lik tilgang på helsehjelp av god kvalitet ved å gi pasienter rettigheter overfor helsetjenesten. Lovens bestemmelser skal bidra til å fremme tillitsforholdet mellom pasient og helsetjeneste og ivareta respekten for den enkelte pasients liv, integritet og menneskeverd."[13]*

### 8.3.1 § 5-1. Rett til innsyn i journal

Første ledd i *§ 5-1 lov om pasientrettigheter* sier:

> *"Pasienten har rett til innsyn i journalen sin med bilag og har etter særskilt forespørsel rett til kopi. Pasienten har etter forespørsel rett til en enkel og kortfattet forklaring av faguttrykk eller lignende."[13]*

I begge løsningene som blir presentert ser en at hver pasient har fulle rettigheter til å sjekke sine journaler. Pasienten har fulle leserettigheter på hva som til en hver tid blir ført inn i journalen

Andre ledd lyder som følger:

> *"Pasienten kan nektes innsyn i opplysninger i journalen dersom dette er påtrengende nødvendig for å hindre fare for liv eller alvorlig helseskade for pasienten selv, eller innsyn er klart utilrådelig av hensyn til personer som står pasienten nær."[13]*

For at andre ledd skal overholdes i et felles helsenett må den behandlingsansvarlige part tre inn for å gi pasienten færre rettigheter til den felles journalen som ligger i databasen. Eventuelt ta ifra pasienten alle rettigheter. Igjen ser man hvor viktig en kontrollinnstans i et slikt nett vil være.

## *8.4 Fra lov om helsepersonell*

*"Lovens formål er å bidra til sikkerhet for pasienter og kvalitet i helsetjenesten samt tillit til helsepersonell og helsetjeneste"[14].*

### 8.4.1 § 46. Elektronisk pasientjournal

*§ 46* Sier at:

"*Pasientjournal kan føres elektronisk."[14]*

Det er derfor ingenting i veien for å ha alle journaler lagret i en felles database, eller som i portal løsningen, der det finnes mange databaser som flere parter har tilgang til. Det finnes allerede mange sykehus som fører sine journaler elektronisk. SSA er et av foregangssykehusene. De har lagret alle sine journaler elektronisk og makulert de gamle papirutgavene av journalene.

## 8.5 Evaluering av Datatilsynets sikkerhetsbestemmelser

For at det skal være mulig å gjennomføre en portal-løsning eller felles database for helsevesenet må informasjonssikkerheten være av topp standard. Dette er viktig for at personvernet skal opprettholdes [15].

Begrepet informasjonssikkerhet omfatter:

> *-"Sikring av konfidensialitet, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene".[15]*
>
> *-"Sikring av integritet, dvs. beskyttelse mot utilsiktet endring av opplysningene".[15]*
>
> *-"Sikring av tilgjenglighet, dvs. sørge for at tilstrekkelig og relevante opplysninger er til stede" [15].*

For å få en tilfredsstillende evaluering av sikkerheten, brukes Datatilsynets rapport *"Sikkerhetsbestemmelsene i Personopplysningsforeskriftene"* som sammenlikningsgrunnlag. Denne forskriften kom til på grunn av at Personopplysningsloven 1. januar 2001 erstattet personregistreringsloven fra 1978, og omfatter krav til informasjonssikkerhet ved behandling av personopplysninger

De to første paragrafene omhandler selve lovverket. De blir dermed ikke evaluert i denne rapporten.

### 8.5.1 § 2-3 Sikkerhetsledelse

**Bestemmelse:**

*"Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges.*

*Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål.*

*Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.*

*Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.*

*Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi."[15]*

**Kommentar:**

Sikkerhetsledelsen skal, i dette tilfellet, bli tatt hånd om av en ansvarlig part. Det vil si sykehus, kommune, Staten eller en uavhengig tredje part. På forhånd er det utarbeidet en sikkerhetsstruktur som skal være retningslinjer. Videre skal den behandlingsansvarlige evaluere denne strukturen og eventuelt gjøre de forandringer som må til.

I portal-løsningen er det pasienten som er den styrende part og som selv bestemmer hvem som har tilgang til sine opplysninger, men også her kan det være en styrende part som passer på at retningslinjene blir overholdt.

### 8.5.2 § 2-4 Risikovurdering

**Bestemmelse:**

*"Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.*

*Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.*

*Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og § 2-2.*

*Resultatet av risikovurderingen skal dokumenteres."[15]*

**Kommentar:**

Den av sykehus, kommune, stat eller uavhengig tredjepart som styrer databasen, vil ha kompetent personell og moderne utstyr. Derfor er det ingen problem å utføre de risikovurderingene som er nevnt ovenfor.

Den uavhengige tredjepart, som styrer sikkerheten i portalen, har i utgangspunktet ingen rettigheter til å lese pasientens journal. Derfor kan det være veldig vanskelig for denne å utføre en fullstendig risikovurdering. Pasienten kan selvfølgelig gi leserettigheter, men det vil uansett være veldig kostbart å ha folk ansatt for å ta seg av risikovurderingen. Pasienten kan selvfølgelig gjøre dette selv, men da må denne ha utstyr og kompetanse til det.

### 8.5.3 § 2-5 Sikkerhetsrevisjon

**Bestemmelse:**

*"Sikkerhetsrevisjonen av bruk av informasjonssystemer skal gjennomføres jevnlig.*

*Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandør.*

*Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6.*

*Resultat fra sikkerhetsrevisjonen skal dokumenteres."[15]*

**Kommentar:**

Som for risikovurdering, vil den av alternativene som skal styre den felles databasen ha kompetanse og utstyr til å foreta sikkerhetsrevisjonen.

I motsetning til ved risikovurdering vil ikke de som styrer sikkerheten i portalen måtte ha leserettigheter til pasientens journaler for å utføre sikkerhetsrevisjon. Likevel vil det bli veldig kostbart for pasienten hvis det skal ansettes folk til utføre dette. Pasienten kan igjen utføre dette selv, men som ved risikovurdering trengs det utstyr og kompetanse.

### 8.5.4 § 2-6 Avvik

**Bestemmelse:**

*"Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.*

*Avviksbehandling skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.*

*Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal datatilsynet varsles.*

*Resultatet fra avviksbehandling skal dokumenteres."[15]*

**Kommentar:**

På samme måte som ved risikovurdering og sikkerhetsrevisjon, vil også avvik kunne behandles for felles-database ideen. Siden det bare er den mest nødvendige informasjonen som blir lagt inn i felles-databasen, vil den ikke inneholde så mye sensitivt personopplysning.

Portalløsningen vil gi de samme problemene som i kap.7.5.2.

### 8.5.5 § 2-7 Organisering

**Bestemmelse:**

*"Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.*

*Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.*

*Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.*

*Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.*

*Bruk av informasjonssystemet som har betydning for innformasjonssikkerheten, skal utføres i henhold til fastlagte rutiner."[15]*

**Kommentar:**

Så store institusjoner som sykehus, stat og kommune har tilgang til utstyr og teknologi som sikrer informasjonsdokumentasjon. Den ansvarlige part sørger for dokumentasjonen i database-løsningen.

Det er pasienten som er den behandlingsansvarlige ved portal-løsningen. Han/hun har sjelden god nok økonomi til forskjellig utstyr og teknologi som trengs til dokumenteringen. Hvis pasienten gir dette ansvaret til utenforstående part, vil også disse oppgavene bli utført på pasientens regning.

### 8.5.6 § 2-8 Personell

**Bestemmelse:**

*"Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.*

*Medarbeiderne skal ha nødvendig kunnskap for å bruke innformasjonssystemet i samsvar med de rutiner som er fastlagt.*

*Autorisert bruk av informasjonssystemet skal registreres."[15]*

**Kommentar:**

Sykehus, stat, kommune osv har mange ansatte. Det kan derfor være mulighet for at noen av disse vil prøve å logge seg ulovlig inn i systemet. Dette unngåes ved rollebasert aksess (se kap.6.9) og passordbeskyttelse (se kap.6.6). De ansatte i disse institusjonene bør kunne få opplæring i den nødvendige kunnskap som trengs i samsvar med de rutiner som er fastlagt.

Siden det egentlig er pasienten som er den behandlingsansvarlige ved portal-løsningen, så vil det ikke by på så mange problemer angående personell. Hvis pasienten gir dette ansvaret til en uavhengig tredjepart, kan dette løses på samme måte som ved felles database-løsningen.

### 8.5.7 § 2-9 Taushetsplikt

**Bestemmelse:**

*"Medarbeider hos den behandlingsansvarlige skal pålegges taushetsplikt forpersonopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten."[15]*

**Kommentar:**

Uansett hvilken løsning som velges, og hvem som er den behandlingsansvarlige, er det ingen problem å pålegge taushetsplikt. Problemet blir å overholde dette, men dette er veldig vanskelig å kontrollere.

### 8.5.8 § 2-10 Fysisk sikring

**Bestemmelse:**

*"Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger eller forskriften her*

*Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten.*

*Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger."[15]*

**Kommentar:**

Ved store institusjoner som sykehus, stat og kommune, vil det ikke være vanskelig å ha utstyret som brukes til å behandle sensitive opplysninger innelåst. Ved bruk av nøkkelkort, som bare er tildelt de behandlingsansvarlige, vil bare det personell som

er autorisert ha adgang til utstyret. Det kan også tas i bruk kameraovervåkning og/eller søke hjelp hos et vekterselskap.

Hjemme hos pasienten er det ikke så lett å sikre utstyret på samme måte, men pasienten kan selvfølgelig også låse inn utstyret.

### 8.5.9 § 2-11 Sikring av konfidensialitet

**Bestemmelse:**

*"Det skal treffes tiltak mot uautorisert innsyn i personopplyninger hvor konfidensialitet er nødvendig.*

*Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten.*

*Personopplysninger som overføres elektronisk ved hjelp avoverføringsmedium utenfor den behandlingsansvarlige fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.*

*For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte.*

*Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slette fra lagringsmediet."[15]*

**Kommentar:**
Ved hjelp av brannmurer (se kap.6.7), digitalt sertifikat (se kap.6.4), digitalt signatur (se kap.6.5), passordbeskyttelse (se kap.6.6), SSL (se kap.6.1), aksess kontroll (se kap.6.8) og rollebasert aksess kontroll (se kap.6.9) vil både felles database-løsningen og portal-løsningen kunne sikre konfidensialitet.

### 8.5.10 § 2-12 Sikring av tilgjengelighet

**Bestemmelse:**

*"Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig*

*Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten.*

*Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk*

*Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres."[15]*

**Kommentar:**

Som i kap.8.5.9 vil disse teknologiene også sikre tilgjengeligheten til både felles database og portal-løsningen.

### 8.5.11 § 2-13 Sikring av integritet

**Bestemmelse:**

*"Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig*

*Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten,*

*Det skal treffes tiltak mot ødeleggende programvare."[15]*

**Kommentar:**

Som i kap. 8.5.9 og kap. 8.5.10 brukes disse teknologiene til å sikre integritet.

### 8.5.12 § 2-14 Sikkerhetstiltak

**Bestemmelse:**

*"Sikkerhetstiltakene skal hindre uautorisert bruk av informasjonssystemene og gjøre det mulig å oppdage forsøk på slik bruk*

*Forsøk på uautorisert bruk av informasjonssystemet skal registreres*

*Sikkerhetstiltakene skal omfatte tiltak som ikke kan påvirke eller omgås av medarbeiderne og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.*

*Sikkerhetstiltak skal dokumenteres."[15]*

**Kommentar:**

Bruk av passordbeskyttelse (se kap.6.6) og rollebasert aksesskontroll (se kap.6.9) hindrer uautorisert bruk av systemet.

Ved bruk av brannmurer (se kap.6.7) vil all trafikk i begge løsningsforslagene bli logget.

### 8.5.13 § 2-15 Sikkerhet hos andre virksomheter

**Bestemmelse:**

*"Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.*

*Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysingsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register*

*Leverandører som gjennomfører sikkerhetstiltak, eller gjør en annen bruk av informasjonssystemet på den behandlingsansvarlige vegne, skal tilfredsstille kravene i dette kapittelet*

*Den behandlingsansvarlige skal etablere klare ansvars – og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale*

*Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnelig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet."[15]*

**Kommentar:**

Alle aktørene i helsevesenet er allerede pålagt strenge sikkerhetskrav og vil derfor tilfredsstille de gitte sikkerhetskrav i denne paragrafen. Den eneste aktøren som kan få problemer med sikkerhetskravene er pasienten.

### 8.5.14 § 2-16 Dokumentasjon

**Bestemmelse:**

*"Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten skal dokumenteres.*

*Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.*

*Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registrering av alle andre hendelser med betyding for informasjonssikkerheten."[15]*

**Kommentar:**

Store institusjoner som sykehus, stat og kommune har utstyr og ressurser til å lagre alle nødvendige opplysninger så lenge de er pålagt dette.

Pasienten har trolig ikke mulighet til å tilfredsstille disse kravene.

# 9. Evaluering av løsningsforslag

I dette kapittelet skal det utføres en evaluering av de to løsningsforslagene, og gjøres et valg om hvilken som skal satses på.

## *9.1 Felles database*

Felles database-løsningen går ut på at hver helseaktør legger de viktigste opplysningene i hver pasientjournal inn i en felles database. Så lenge det bare er den viktigste informasjonen som blir lagt ut i databasen, er det mye enklere å følge Datatilsynets lovverk. F.eks. er det lettere å følge personvernsloven når det ikke finnes så mange personsensitive opplysninger i databasen.

Problemet med at bare de viktigste opplysningene blir lagt ut, er at de forskjellige helseaktørene ikke får en fullgod tjeneste i forhold til de mulighetene som finnes.

At databasen blir driftet av en stor institusjon som sykehus, kommune eller stat, gjør at den blir driftet av kyndig personell, og med moderne teknologi. I tillegg vil utstyret kunne oppbevares i godt fysisk sikrede rom. Dette gjør at denne løsningen også følger Datatilsynets sikkerhetsbestemmelser.

Arkitektonisk er felles database-løsningen satt opp på en meget brukervennlig måte, og med sterkt hensyn på sikkerhet.

## *9.2 Portalløsning*

Portalløsningen går ut på at pasienten eier sin egen journal, og kan dermed gi de han/hun måtte ønske innsynsrett i de forskjellige helseaktørenes pasientjournal. Dette gir muligheten til en fullgod samhandling mellom de forskjellige helseaktørene, og dermed et mye bedre helsetilbud til pasienten.

Problemet med denne løsningen er at det blir lagt ut mange sensitive opplysninger. Dette gjør det vanskelig å holde seg innen Datatilsynets regelverk. I følge denne rapporten vil portal-løsningen likevel holde seg innen regelverket.

Det er pasienten som ”drifter” denne portalen, dvs. styrer inngangsrett. Dette gjør det vanskelig å følge Datatilsynets sikkerhetsbestemmelser. Grunnen til dette er at ikke alle pasienter kan ha den faglige kompetansen til å følge disse bestemmelsene, ikke alle har godt nok utstyr. Det er også vanskelig å ha en god fysisk sikring. Pasienten kan få hjelp av den aktøren som kontrollerer sikkerheten i portalen, men dette vil øke kostnadene betraktelig.

Arkitektonisk er portalen satt opp meget brukervennlig, og med sterkt hensyn på det sikkerhetsmessige.

## *9.3 Valg av løsning*

Med syn på hvilken av løsningene som gir best samhandling, er det ikke tvil om at valget burde bli portal–løsningen. Den gir full innsiktsrett i de forskjellige pasientjournalene, i motsetning til felles database-løsningen som bare gir innsikt til de viktigste opplysningene.

Når det gjelder Datatilsynets regelverk og sikkerhetsbestemmelser er felles database det klart beste valget. Den bryter etter denne rapporten verken noen av reglene eller sikkerhetsbestemmelsene. Portalløsningen derimot byr på problemer angående sikkerhetsbestemmelsene, på grunn av mye sensitiv informasjon og sannsynlig dårligere driftskompetanse.

Med hensyn på den arkitektoniske oppbygningen stiller de to løsningene ganske likt nå det gjelder funksjonalitet, brukervennlighet og sikkerhet. Det settes kanskje mer krav til sikkerheten i portalløsningen, siden man beveger seg ut og inn av den sikre sonen, men med løsningen i denne rapporten (se kap. 7.2.2), skal ikke det by på noe problem.

Vedrørende valg av løsningsforslag settes Datatilsynets krav foran alt. Følger ikke løsningen Datatilsynets regler og sikkerhetsbestemmelser, vil den ikke være lovlig i bruk. **Felles database** er derfor den løsningen som velges. Den gir også en tilfredsstillende samhandling, selv om den ikke når opp til portalløsningens. Hvis derimot Datatilsynet i fremtiden skulle lette på sine krav, ville sannsynligvis portalløsningen vært valget.

# 10. Drøfting av resultat

I dette kapittelet vil scenarioet og de forskjellige hypotesene bli drøftet. Scenarioet blir drøftet i henhold til den valgte løsningen. Felles database.

## *10.1 Drøfting av scenario*

For at en diabetespasient skal kunne ha god nytte av en felles database, må han/hun kunne bruke de funksjonene denne løsningen tilbyr. Det vil derfor være veldig viktig at en pasient, samtidig som han/hun får opplæring for behandlingen av sin sykdom, også får god opplæring i bruken av databasen. Brukervennlighet er derfor viktig. På en annen side er de fleste Diabetes 1-pasienter unge folk som har erfaring ved bruk av PC eller lett kan lære seg dette. Derfor bør ikke opplæringen by på noen særlige problemer.

Selv om pasienten får god opplæring både når det gjelder sykdom og bruken av database, kan visse elementer skape usikkerhet. Det er da mulig for diabetesspesialisten å legge inn hjelpemidler for pasienten, siden legen har skriverettigheter til visse områder av databasen.

Når en pasient begynner sin hjemmebehandling kan han/hun legge sine måleresultater inn i databasen. Dermed kan diabetesspesialisten kontinuerlig følge med på disse resultatene og eventuelt legge inn kommentarer til pasienten i sin del av databasen. Dette vil igjen føre til at pasienten ikke trenger å gå så ofte til sin lege. Pasienten vil spare tid på dette, men behandlingskvaliteten vil kunne gå ned, siden den menneskelige kontakten mellom partene ikke blir så god.

Etter at pasienten har vært syk en stund, kan han/hun bytte fra diabetesspesialist på sykehuset til sin egen fastlege. De opplysninger fastlegen trenger for å fortsette behandlingen kan ved bruk av databasen hentes rett ut fra denne, isteden for at disse opplysningene må søkes sendt fra sykehus. Spørsmålet vil være om det er sikkert nok å kunne hente informasjon på den måten, men med alle sikkerhetstiltakene som er gjort bør dette være sikrere enn å sende via faks eller post. Ulempen med felles database-løsningen vil være at journalen er ufullstendig. Den informasjonen som ligger i databasen er den viktigste, derfor bør dette være tilstrekkelig. Selv om behandlingen er overtatt av fastlege kan allikevel diabetesspesialisten følge med på utviklingen hvis dette er nødvendig.

Sosialkuratoren som er underliggende kommunen har i oppgave å gi råd om de fremtidige valg pasienten kan ta, med tanke på arbeid, lån og trygd. Pasienten kan stille spørsmål i sin del av databasen, som sosialkurator kan svare på i sin. Dette vil først og fremst være et hjelpemiddel, men det kan aldri erstatte den menneskelige kontakten helt.

## *10.2 Drøfting av hypoteser*

### 10.2.1 Hypotese 1

*Felles database-løsning vil være teknisk mulig å implementere i henhold til Datatilsynets regelverk og Sikkerhetsbestemmelsene i personopplysnigsforeskriftene.*

For at det i hele tatt skal være mulig å ha sensitive opplysninger om en person liggende tilgjengelig for andre, må personen som dette omhandler gi sitt samtykke. I database-løsningen er det ikke alle opplysninger som ligger tilgjengelig. Det vil derfor kunne være lettere for en person å gi tillatelse til dette. Hvis en ikke ønsker å ha sine opplysninger i databasen, er dette valgfritt. Siden det ikke ligger så mye sensitiv informasjon tilgjengelig, vil det være lettere å holde seg innenfor Datatilsynets lovverk.

Det er mange måter å tolke regelverket på. Det er mulig at database-løsningen kan stride mot noen av paragrafene i regelverket, men sånn som de er tolket i denne rapporten strider ikke løsningen mot de lover som gjelder. Ingen av forfatterne av denne rapporten har bakgrunn innen jus, og har derfor ikke de største forutsetningene til å tolke regelverket. Det kan derfor være at en person med juridisk bakgrunn hadde tolket lovverket annerledes.

I databaseløsningen er det sykehus, stat, kommune eller en uavhengig tredjepart som drifter samhandlingen. Både sykehus, stat og kommune har store ressurser og kyndig personell som kan ta på seg og løse de kravene som er satt til sikkerhetsbestemmelsene. Spørsmålet er om noen av de tre partene vil ta seg råd til dette. I det lange løp vil dette kunne være besparende både når det gjelder tid og penger. Derfor vil dette sannsynligvis føre til at noen tar på seg denne oppgaven. Dette vil sannsynligvis også gjelde hvis en uavhengig tredjepart står for driftingen. Skal de få ansvaret for et så stort prosjekt, må bedriften kunne innfri en del tøffe krav, som videre gjør dem egnet til driftingen.

Sikkerhetsbestemmelsene setter også høye krav til datasikkerhet. I database-løsningen legges det stor vekt på sikkerhetsarkitekturen. I database-løsningens sikkerhetsarkitektur er det brukt sikkerhetsteknologier som skal kunne tilfredsstille de krav som er satt i sikkerhetsbestemmelsene.

### 10.2.2 Hypotese 2

*Portal-løsning vil <u>ikke</u> være teknisk mulig å implementere i henhold til Datatilsynets regelverk og Sikkerhetsbestemmelsene i personopplysnigsforeskriftene.*

Som beskrevet i kap.10.2.1 må den personen informasjonen omhandler gi samtykke hvis sensitive opplysninger skal ligge tilgjengelig for andre. I portalløsningen er det denne personen som direkte gir de forskjellige aktørene tillatelse til å aksessere og lese sine opplysninger. Spørsmålet blir da om denne personen har kompetanse til å avgjøre hvem som bør ha tilgang til sine opplysninger. Portal-løsningen tar

utgangspunkt i at pasienten eier sin egen journal. Hvis dette stemmer, bør det forventes at han/hun skal kunne bestemme hvem som skal ha tilgang til sin journal.

Portalløsningen går ut på at pasienten og de forskjellige helseaktørene skal kunne få tilgang til hverandres databaser. Derfor får man også tilgang til mer sensitiv informasjon en ved database-løsningen. Likevel ble det i denne rapportens tolkning av regelverket ikke funnet noen motforestilninger mot en portal-løsning (se kap 8). Igjen må det sies at forfatterne av denne rapporten ikke har noen juridisk bakgrunn.

Tilgangskontrollen til portalen styres av pasienten. Pasienten har normalt ikke kompetanse eller teknisk utstyr til å holde seg innenfor Datatilsynets sikkerhetsbestemmelser (det finnes selvfølgelig unntak). Han/hun trenger da kursing og nytt utstyr, noe som nok kan bli for ressurskrevende.

### 10.2.3 Hypotese 3

.

*Både felles database og portal-løsning er mulig å implementere med dagens teknologi.*

Den teknologien som finnes på dagens marked er mer enn god nok til å kunne dekke de behov som trengs på både kommunikasjons og sikkerhets siden. Det er allerede gjennomført en del prøveprosjekter som viser at dagens teknologi er tilstrekkelig (se kap.2).

Problemet vil ligge i å innføre den samme teknologien på alle områder. I dagens helsevesen finnes det både sykehus som helt har gått over til EPJ og det finnes sykehus som forsatt er på ”gule lapper” stadiet. Det første som må skje for at det i hele tatt kan bli noe felles helsenett, både når det gjelder felles database og en portal-løsning, er at alle innfører EPJ. Videre stilles det krav til at det enten innføres samme EPJ over hele linjen, eller det innføres en felles plattform som gjør at de forskjellige typer EPJ kan prate sammen.

Å innføre et system hvor alle i helsevesenet kan samarbeide på et plan, vil kreve både store arbeidsmessige og økonomiske ressurser.

## *10.3. Drøfting Av Sikkerhetsarkitektur*

I begge løsningsforslagene er det lagt stor vekt på innloggingsprosedyren. I tillegg til vanlig innlogging med brukernavn/passord er det også en ekstra kode som må tastes inn av bruker. Vi har valgt å bruke et kodekort som sendes ut til de forskjellige brukerne via posten. Dette er samme prinsipp som brukes av mange nettbanker. Systemet som brukes av nettbanker sees på som sikker. Det finnes mange alternativer til dette kodekortet. Smartkort og mobiltelefon(SMS) (som brukes av pasientlink) er noen av disse alternativene. Alle alternativene har sine fordeler/ulemper.

Kodekortet sendes i posten. Skulle kodekortet komme på avveie er det en fare for at dette kan bli misbrukt, selv om det trengs både brukernavn/passord for at kodekortet kan brukes. Sjansene bør være små for at dette skal kunne skje. Som nevnt har kodekort allerede vært lenge i bruk av nettbank, det sees derfor på som sikkert. sjansen er også stor for at en eventuell bruker allerede kjenner tll bruken av dette. Å bruke kodekort trenger heller ikke mye administrasjon. Kortet kan også brukes lenge siden det inneholder et stort antall koder. Et eksempel på at dette fungerer er den danske helseportalen sundhedsnet som bygger sine prinsipper på funksjonaliteten til nettbanker.

Fordelen med SMS er sikkerheten. Man får koden tilsendt der og da, og derfor vanskelig for uvedkommende å snappe opp. Ulempen vil være at en er nødt til å ha en mobil telefon for at dette systemet skal kunne brukes. En annen ulempe vil være at det vil koste penger for hver gang en mottar en ny kode.

Smartkort trenger en kortleser som står med pcen. Dette vil koste penger for brukeren. Det vil også være vanskelig å bruke andre steder en hjemme. Smartkort vil på den annen side sees på som å være veldig sikkert og lett å bruke når man er hjemme.

For å sette opp sikre forbindelser med kryptering og autentisering ble SSL brukt. Fordelen med SSL er at den er integrert i de fleste nettlesere og nett servere. Den blir derfor lett å administrere i tillegg til at de fleste brukere har støtte for bruk av SSL.. Det trengs heller ikke noe ekstra software eller applikasjoner for å sette opp en SSL forbindelse. Dataflyten kunne blitt gjort sikrere ved å opprette en VPN-tunnel. Da ville all dataflyt gått igjennom en tunnel som er sikrere enn en kryptert forbindlese. VPN krever på den annen side myer mer administrasjon enn SSL. Den er ikke integrert i noen av system komponentene. For å kunne bruke VPN må denne funksjonen enten integreres i f. eks brannmur eller router. Den kan også legges til ved hjelp av egen software. VPN er ofte i bruk i nett der det eksisteres flere avskilte nettverk. I database løsningen er det bare en server som skal administreres og det er derfor ikke noe utpreget fordel å bruke VPN kontra SSL. SSL ble derfor valgt, siden det er lettere å administrere i tillegg til at det ikke krever så store ressurser som VPN.

# 11. Konklusjon

Innføringen av et felles helsenett, enten det gjelder en felles database-løsning eller en portal–løsning, vil føre til at alle aktørene innenfor helsesektoren kan samhandle på et mye større plan enn det som er tilfelle med dagens situasjon. Utfordringen vil ligge i å komme frem til en løsning, som i tillegg til å tilby en god helsetjeneste, vil kunne tilfredsstille de krav som settes til sikring av sensitive opplysninger. Det finnes i dag mange lover og regler for hvordan slike opplysninger skal behandles. Disse regelverkene er utarbeidet av Datatilsynet.

Metodekapittelet viser at det ved hjelp av Contextual Design er mulig å innhente relevant informasjon for hva som er nødvendig for å avdekke ønsker og muligheter ved innføringen av et felles helsenett. For å kunne få fullt utbytte av denne modellen bør løsningsforslagene, som blir utarbeidet fra den innhentede informasjonen, tas med ut igjen til kunden. I dette tilfellet helseaktørene.

Prosjektet avdekker at det er behov for større samhandling i helsevesenet. Den avdekker også at det jobbes kontinuerlig for å dekke dette behovet, men at det ennå gjenstår mye arbeid før dette kan bli realisert.

De to løsningsforslagene som er utarbeidet i denne rapporten er begge teknisk mulig å gjennomføre med dagens teknologi. Utfordringen her vil ligge i å samkjøre alle aktørene på en felles plattform. For å kunne gjøre dette kreves mye arbeid og økonomiske ressurser.

I denne rapporten kommer det frem at både felles database- og portal–løsningen holder seg innefor de krav som stilles i de forskjellige lovene utarbeidet av datatilsynet.

Sikkerhetsbestemmelsen utarbeidet av Datatilsynet er vanskeligere å tilfredsstille for det ene løsningsforslaget. Databaseløsningen driftes av store institusjoner som sykehus, stat eller kommune. Den kan også bli driftet av en utenforstående tredje part. Derfor finnes det nok ressurser og kompetent personell til å tilfredsstille sikkerhetsbestemmelsene. Portal–løsningen må derimot driftes av pasienten selv. Pasienten vil ikke ha kompetanse eller ressurser til å utføre dette. Portal–løsningen vil derfor ikke tilfredsstille kravene i sikkerhetsbestemmelsene.

Med hensyn på den arkitektoniske oppbygningen stiller de to løsningene ganske likt når det gjelder funksjonalitet, brukervennlighet og sikkerhet. Begge løsningsforslags arkitektoniske oppbygning støtter de teknologiske krav som settes i sikkerhetsbestemmelsene.

Vedrørende valg av løsningsforslag settes Datatilsynets krav foran alt. Følger ikke løsningen Datatilsynets regler eller sikkerhetsbestemmelser, vil den ikke være lovlig i bruk. Felles database er derfor den løsningen som velges. Den gir også en tilfredsstillende samhandling, selv om den ikke når opp til portalløsningens. Hvis derimot Datatilsynet i fremtiden skulle lette på sine krav, ville sannsynligvis portalløsningen vært valget.

# Referanser


[1] http://www.telemed.no/cparticle58175-7457.html

[2] http://www.telemed.no/cparticle58176-7457.html

[3] http://www.sundhed.dk/wps/portal/_s.155/1836

[4] The Danish eHeallth experience: One Portal for Citizens and Professionals

[5] Beyer, H. Holtzblatt, K. (1998). Contextual Design. Morgan Kaufmann Publishers

[6] http://www.incent.com/cd/cdhow.html

[7] http://www.knowledgestorm.com/collateral/WTP/50565_12711_89737_ssl_eng.pdf

[8] Chris Brenton, Camron Hunt, Active Defense A Comprehensive Guide to Network Security

[9] T. Daler, R. Gulbrandsen, T.A. Høie, B. Melgård, T. Sjølstad,Håndbok i datasikkerhet – informasjonsteknologi og risikostyring

[10] Joon S. Park, Ravi Sandhu og Gail-Joon Ahn, Role Based Access Control on the Web, George Mason University og University of North Carolina at Charlotte

[11] http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-20000414-031.html&dep=alle&titt=personopplysningsloven&

[12] http://www.lovdata.no/all/nl-20010518-024.html

[13] http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19990702-063.html&dep=alle&titt=pasientrettigheter&

[14] http://www.lovdata.no/cgi-wift/wiftldles?doc=/usr/www/lovdata/all/nl-19990702-064.html&dep=alle&titt=helsepersonell&

[15] http://www.datatilsynet.no/dtweb/attachment/610/SV100_00.pdf

[16] http://helmersol.nr.no/haandbok/html/hb.html

[17] http://docs.communitye.net/module1/basic_concepts

# Liste Over Definisjoner

Her er en liste med oversikt over de forskjellige definisjonene og forkortelsene, med betydninger som er brukt i rapporten.

1) **personopplysning**: opplysninger og vurderinger som kan knyttes til en enkeltperson,

2) **behandling av personopplysninger:** enhver bruk av personopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,

3) **personregister:** registre, fortegnelser m.v. der personopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen,

4) **behandlingsansvarlig:** den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes,

5) **databehandler:** den som behandler personopplysninger på vegne av den behandlingsansvarlige,

6) **registrert:** den som en personopplysning kan knyttes til,

7) **samtykke:** en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av opplysninger om seg selv,

8) **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.

9) **helseopplysninger:** taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller av betydning for helseforhold, som kan knyttes til en enkeltperson,

10) **avidentifiserte helseopplysninger:** helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson, og hvor identitet bare kan tilbakeføres ved sammenstilling med de samme opplysninger som tidligere ble fjernet,

11) **anonyme opplysninger:** opplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, slik at opplysningene ikke lenger kan knyttes til en enkeltperson,

12) **pseudonyme helseopplysninger:** helseopplysninger der identitet er kryptert eller skjult på annet vis, men likevel individualisert slik at det lar seg gjøre å følge hver person gjennom helsesystemet uten at identiteten røpes,

13) **behandling av helseopplysninger:** enhver formålsbestemt bruk av helseopplysninger, som f.eks. innsamling, registrering, sammenstilling, lagring og utlevering eller en kombinasjon av slike bruksmåter,

14) **helseregister:** registre, fortegnelser, m.v. der helseopplysninger er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen,

15) **behandlingsrettet helseregister:** journal- og informasjonssystem eller annet helseregister som har til formål å gi grunnlag for handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende eller rehabiliterende mål i forhold til den enkelte pasient og som utføres av helsepersonell, samt administrasjon av slike handlinger,

16) **databehandlingsansvarlig:** den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven,

17) **databehandler:** den som behandler helseopplysninger på vegne av den databehandlingsansvarlige,

18) **registrert**: den som helseopplysninger kan knyttes til,

19) **samtykke:** en frivillig, uttrykkelig og informert erklæring fra den registrerte om at han eller hun godtar behandling av helseopplysninger om seg selv

20) **pasient:** en person som henvender seg til helsetjenesten med anmodning om helsehjelp, eller som helsetjenesten gir eller tilbyr helsehjelp i det enkelte tilfelle;

21) **pasientens pårørende:** den pasienten oppgir som pårørende og nærmeste pårørende. Dersom pasienten er ute av stand til å oppgi pårørende, skal nærmeste pårørende være den som i størst utstrekning har varig og løpende kontakt med pasienten, likevel slik at det tas utgangspunkt i følgende rekkefølge: ektefelle, registrert partner, personer som lever i ekteskapslignende eller partnerskapslignende samboerskap med pasienten, myndige barn, foreldre eller andre med foreldreansvaret, myndige søsken, besteforeldre, andre familiemedlemmer som står pasienten nær, verge eller hjelpeverge;

22**) helsehjelp:** handlinger som har forebyggende, diagnostisk, behandlende, helsebevarende, rehabiliterende eller pleie- og omsorgsformål og som er utført av helsepersonell;

23**)** **helsetjenesten:** primærhelsetjenesten, spesialisthelsetjenesten og tannhelsetjenesten

24) **helsepersonell:** personer som nevnt i lov om helsepersonell § 3.

Vedlegg

## *Vedlegg A. Spørsmål til informasjonsmøter*

Dagens situasjon.....
Hva syntes du om.....
Kunne du tenke deg å bruke.....
Hvordan tror du muligheten for gjennomslag.....
Dine ideer.....

Hvor aktiv er du i bruken av elektroniske hjelpemidler i ditt arbeid?

- E-mail
- PDA
- Nett
- Elektronisk journal

Hva synes du om måten kommunikasjonen foregår i dagens helsevesen?

Hva synes du om vår modell?

- I forhold til personvern
- I forhold til flyt av data
- Svakheter
- Forslag til forandringer/forbedringer

Kunne du tenke deg å bruke denne modellen?

Hva vet du om regelverket til datatilsynet?

- Er det for strengt etter din mening?
- Tror du vår modell kan bli godtatt?

Er bruken av elektroniske hjelpemidler i dagens situasjon stor?

- Synes du den bør blir det?

Har du noe erfaring med at dine pasienter bruker elektronisk hjelpemidler?

Hvordan går informasjonsflyten i hjemmepleien/kommunen?

- pasient
- mellom hverandre
- kommunen

Synes du den kommunikasjonen som går mellom de forskjellige leddene i dag er god?

- Hva kan bli bedre?
- Eksempler

Har du noen eksempler på informasjonen ikke har kommet skikkelig frem?

## *Vedlegg B. Sammendrag av informasjonsmøter*

### Nils Kristian Fjærbu

Dyrere med IT: Det vil på kort sikt bli vanvittig dyrt å innføre IT. Men på lengre sikt kan det lønne seg.

Oracle har en introdusert en løsning som kan brukes i dag.

Innenfor hver kommune er det lov med fri flyt av informasjon. Men hvis en skal over i en annen kommune er det brannmur og ingen informasjonsflyt er lov.

Det er begynt en innføring av bærbart utstyr til alle innenfor helsevesenet.

Uansett hva som blir innført på alltid de etiske perspektiver bli tatt vare på. Noen av den informasjonen som går på menneskelig plan kan ikke bli kuttet ut. Dette kan for eksempel være behandling av en pasient som akkurat har blitt utskrevet og som trenger å få tilpasset hjemme sitt ut ifra sin lidelse

Informasjonsflyten fra sykehuset går i dag skriftelig. Fjærbu mente at de ønsket elektronisk kommunikasjon og en felles journal.

Brikke i huden. Mye bedre sikkerhet, mye bedre økonomisk. Men etisk er ikke dette veldig bra.

Hvis det er nødløsning blir regelverket brutt.

Hvis informasjon trenges på et hjemmebesøk må hjemmesykepleieren ringe eller oppsøke kontoret hvor den aktuelle pasienten hører til.

Er det egentlig så mye sikrere å ringe for å få tak i informasjon i forhold til å hente den rett ut ifra en database.

Fordel med database er at du ser hvem som har vært inne på den. Isteden for at hvem som helst kan ”snoke” rundt å lese dagens journaler. Verifisering. Her kan man også skille mellom forskjellige nivåer av tilgang.

Det trengs et system mellom sykehus og kommune. Hele verden kommer til å bli en hel kommune.

Uansett hvor mye IT som blir innført vil det alltid være fare for menneskelig svikt.

## Håvard Skjærvik

Kommunikasjonen foregår i dag på et veldig enkelt plan. Gjerne på små gule lapper. Dette gjelder internt på sykehuset. Med slike lapper er det stor fare for at de forsvinner osv.

Tildelte og graderte rettigheter. Dette kan lett ordnes med dagens teknologi, men spørsmålet er hvem som skal styre det hele. Det bør sitte et styrende organ på toppen som tar seg av alt dette. Dette organet bør også passe på at ting går rett for seg.

Det er ikke lov å sende sensitive opplyninger over Epost.

Fremtiden blir helt klart at hver pasient eier sin egen journal. Det skulle bare mangle. Det finne ingen juridiske motforestillinger mot at dette ikke er realistisk.

Legen har plikt til å skjerme sine pasienter. Hvis det er opplysninger som legen mener at pasienten ikke har godt av å høre bør legen holde tilbake denne informasjonen.

Det er vanlig at det er stor skepsis til datasikkerhet. Men det er jo allerede bevist at slike systemer kan lages. Nettbank.

Arendal Sykehus har innført full bruk av EPJ. De har skannet inn alle pasientenes journaler. Og makulert papirutgavene. Alle legene har full tilgang til alle journalene. Men en lege har ingen rett til å gå inn på en journal som ikke tilhører en av hans pasienter. Det blir derfor registrert hvem som går inn i hver journal. Til denne registreringen brukes et innloggings system Det finnes også noe som kalles blålys. Det vil si at i en nød situasjon har en lege lov til å gå inn på en journal han ellers ikke hadde rett til å åpne. Dette systemet har ført til at det er mindre sjanse for å miste informasjon pluss at det over lengre tid har vist seg å føre til økonomisk gevinst

Det er full mulig teknisk sett å sende røntgen mellom sykehus men det er ikke lov. Det er ikke vanskelig å kryptere.

Hvis informasjon skal sendes mellom leger må pasienten gi skriftelig samtykke.

Det er mulig å bruke kort isteden for database.

Utfordring – alle aktører i samme database. Det er ikke sikkert at aktørene vil at andre aktører skal ha tilgang til sin data. Før dette er mulig må det innføres et felles EPJ system for alle. I dagens situasjon finnes det mange forskjellige journal systemer Eller samhandlingssystemer som gjør at de forskjellige systemene kan brukes sammen.

For at det kunne innføres et slikt system må det finnes ”kjøreregler” for hvordan rettighetene skal fordeles. For å styre dette må det legges til rette et nasjonalt lovverk.

I Arendal brukes et system som kalles DIPS. Dette er et innloggingssystem.

Brukervennlighet et viktig i et system. Da blir det letter å lære for de som skal ta det i bruk. Dette vil spare tid og penger.

I dag er pasienten lite involvert i sin sykdom. I fremtiden vil en pasient spille en større rolle i sin egen behandling og dermed også vite mer om sin sykdom. Dette kan gjøres ved at pasienten involveres i helsevesenets IT-nettverk. Og at det er finnes hjelpeverktøy som pasienten skjønner.

Helsevesenet er konservativt og har dermed vanskelig for å innføre nye ting.

I Arendal har det blitt innført nye metoder å forberede en opperasjon. Før ble det brukt møte virksomhet foran hver opperasjon. På møte ble opperasjonen planlagt og deretter skrevet ned på et papir. Nå er det innfør opperasjons ”maler” som ligger på nettverket. Dette sparer masse tid og ressurser. Når dette systemet først ble foreslått var det stor skepsis. Nå som det er innført og i bruk er alle veldig godt fornøyde med systemet.

Det vi vil oppnå med å innføre IT er å øke kvaliteten til samme ressursbruk. Dette vil igjen øke effektiviteten.

Utviklingen av et fullgodt journal system er veldig dyrt

## Arne Quist Paulsen

Sykehuset bør kunne respons på det pasienten skriver inn i journalen. Det vil si toveis kommunikasjon i databasen.

Ved sykdom må diabetes pasienter sjekke blodsukker verdier oftere. ’

Alle svar på kontrollprøver, som ikke er klare, når pasienten er inne på sykehuset til sjekk, sendes via brev hjem til pasienten. Dette kunne vært gjort elektronisk ved hjelp av en database.

Sykehuset sender gjerne en data utskrift av resepten til pasienten isteden for apoteket. Hvis pasienten ber om det sendes resepten til apoteket.

Type 1 diabetes: Fåes typisk av unge mennesker. Kroppen klarer ikke å produsere insulin og må tilføres dette. Behandlingen begynner med en opplæringsperiode, Der pasienten blir lagt inn noen dager. En doktor lærer opp pasienten til å kunne utføre behandling og om sykdommen generelt. Spesial sykepleier lærer opp pasienten til hvordan han skal utføre de forskjellige målingene og til å kunne skjønne resultatene. Pasienten kan sel velge hvilke måle utstyr han vil ha. I tillegg må pasienten ha en samtale med en kostholds ekspert der han får vite hva han kan spise og drikke. Pasienten har også en samtale med en  Sosial kurator som gir råd om yrkesvalg, lån og trygd. Under opplæring av pasienter er det individuell opplæring av hver pasient. Det er blitt prøvd gruppevis, men dette ga ikke like gode resultater.

Databasen kan ikke erstatte opplæringen, men den kan være et godt hjelpemiddel for råd og tips.

En pasient går periodisk til kontroll på sykehuset, I begynnelsen er han inne hver uke, men etter hvert som pasienten blir tryggere på seg selv øker intervallet mellom hver kontroll. Når en pasient er fullerfaren er han inne til kontroll en gang i året på sykehuset og bruker fastlege ellers. Etter hvert kan pasienten velge vekk sykehuset og heller gå til et legesenter.

Velger sprøyter og penner selv. Får deretter resept.

En pasient måler blodsukker hjemme jevnlig. Resultatene av disse målingene føres inn i bok som legen sjekker med hver kontroll. Disse resultatene hadde vært mye greier å ført inn i en database. Da kunne legen sjekket resultatene oftere.

Oversikt skjema over prøve resultatene sendes til fastlegen. Dette hadde vært enklere og mindre ressurskrevende hvis fastlegen bare kunne hentet dette ut av en database.

Fordeler med bruk av en database er: Pasienten har samlet alle sine opplysninger på et sted, lege og liknende kan bruke databasen til å kommunisere med pasienten, veldig greit hvis en pasient flytter. Stor lagringskapasitet. Men må ikke glemme toveis kommunikasjon.

Ulemper: Hvis databasen skulle gå ned. Lammer dette hele systemet.