Implementering av internettbasert pasientjournal i en helseinstitusjon

av

Henrik Buksholt
Pål Espen Nilsen

Masteroppgave i informasjons- og kommunikasjonsteknologi

Høgskolen i Agder
Fakultet for teknologi

Grimstad, mai 2007

Sammendrag

Det utvikles stadig flere internettjenester som gir nye og bedre muligheter for kommunikasjon og utveksling av informasjon. Det norske helsevesen har merket en stor etterspørsel fra pasienter og helsepersonell etter internettbaserte helseløsninger som vil forenkle hverdagen. De første internettbaserte helsetjenestene eksisterer, men disse er helt i startfasen og det er nærmest uendelige muligheter for hva slags tjenester en skal kunne tilby i fremtiden.

Sårbarhetene relatert til internett og det strenge lovverket i Norge gjør slike tjenester vanskelig å gjennomføre. Løsningene som skal tilby slike tjenester over internett må derfor være solide, avanserte og i tråd med Norges lovverk.

MinJournal-løsningen tilfredsstiller lovverket og har en tilfredsstillende sikkerhet både for pasienter og helsepersonell. Vi har tatt for oss de lover og bestemmelser som gjelder ved implementering av et slikt system samt beskrevet aktuell sikkerhetsteknologi. Relatert til implementeringen av MinJournal ved Evjeklinikken har vi utviklet fem skjemaer som skal tas i bruk av pasientene så fort systemet blir operativt. Skjemaene er basert på eksisterende skjemaer i papirform. Ved transformasjonen til elektronisk format har vi beholdt funksjonaliteten til eksisterende skjema og samtidig gitt de et penere og mer brukervennlig utseende.

Mot slutten av oppgaven har vi gjennomgått og belyst endringene en overgang fra eksisterende løsning til internettbasert løsning vil føre med seg. Dette gjelder i hovedsak endringer i prosess- og dokumentflyt ved Evjeklinikken. Resultatene fra en implementering av MinJournal går i hovedsak ut på å bedre behandling og behandlingstilbud ved Evjeklinikken.

Forord

Denne oppgaven fullfører masterutdanningen i informasjons- og kommunikasjonsteknologi ved Høgskolen i Agder, avdeling Grimstad.

Oppgaven ble gitt av Evjeklinikken i samarbeid med IT-avdelingen på Rikshospitalet – Radiumhospitalet HF.

Arbeidet er gjennomført ved Høgskolen i Agder i tett samarbeid med Evjeklinikken og Rikshospitalet – Radiumhospitalet HF.

Vi vil rette en takk til følgende personer: Veileder for Høgskolen i Agder, Professor Andreas Prinz for verdifull veiledning og hjelp med oppgaven, prosjektleder ved Evjeklinikken, Tor-Ivar Karlsen, for juridisk veiledning og konstruktiv kritikk til rapporten. Ivar Berge og Rune Engh ved Rikshospitalet – Radiumhospitalet HF for teknisk informasjon og veiledning.

Grimstad, 29. Mai 2007

Henrik Buksholt Pål Espen Nilsen

Innholdsfortegnelse

Figurer

Eksempler

Forkortelser

CA	– Certificate Authority
CSS	– Cascading Stylesheet
DoS	– Denial of Service
DTD	– Document Type Definition
EEPROM	– Electronically Erasable Programmable Read Only Memory
HTML	– Hypertext Markup Language
HTTPS	– Hypertext Transfer Protocol Secure
IP	– Internet Protocol
IPSec	– Internet Protocol Security
OWQOL	– Obesity and Weight loss Quality of Life (questionnaire)
PKI	– Public Key Infrastructure
PIN	– Personal Identification Number
RC2/RC4	– Rivest Cipher / Ron's Code
RFID	– Radio-Frequency Identification
ROM	– Read Only Memory
ROS	– Risiko Og Sårbarhet
SGML	– Standard Generalized Markup Language
SSL	– Secure Sockets Layer
TCP	– Transmission Control Protocol
UTF	– Unicode Transformation Format
W3C	– World Wide Web Consortium
WEP	– Wireless Equivalent Privacy
WRSM	– Weight Related Symptom Measure
XForms	– XML Forms
XHTML	– Extensible Hypertext Markup Language
XML	– Extensible Markup Language
XPath	– XML Path Language
XSD	– XML Schema Definition
XSL	– Extensible Stylesheet Language

1 Innledning

1.1 Bakgrunn for oppgaven

Evjeklinikken (1) er et unikt helseforetak i Norge. Det er landets eneste medisinsk spesialiserte helseforetak for behandling av mennesker med sykelig overvekt. Sykelig overvekt vil si at pasientene har utviklet sykdommer som følge av overvekten eller er i risikogruppen for å utvikle følgesykdommer. Evjeklinikken har en behandlingsfilosofi som innebærer oppfølging over fem år, og i løpet av disse fem årene har pasientene korte opphold ved Evjeklinikken. Når de er hjemme får de tett oppfølging av fastlege og Evjeklinikken.

Oppfølgingen av pasienter, fra Evjeklinikkens side, skjer hovedsakelig over telefon, men dette er tidkrevende. Dette hadde spart både Evjeklinikken, fastlege og pasient mye tid om det meste av kommunikasjonen og informasjonsflyten gikk over internett. De vil uansett fortsette med kontakt over telefon da dette fungerer utmerket for å motivere pasientene, men generell informasjon og opplysninger vil fungere bedre gjennom et elektronisk og internettbasert verktøy. Det finnes flere slike verktøy som er relevante, men Evjeklinikken har valgt å implementere og bruke MinJournal (2).

MinJournal er et prosjekt som ledes av Rikshospitalet – Radiumhospitalet HF og består av en rekke helseforetak og -institusjoner i Norge, inkludert Evjeklinikken. Målet med prosjektet er å utvikle en nasjonal internettbasert pasientjournal som skal gjøre det mulig for pasienter og helsepersonell å utveksle informasjon på en enkel og lovlig måte.

Utviklingen av et system for utveksling av informasjon på en enkel måte er ikke komplisert. Utfordringen er at den aktuelle løsningen må være i tråd med lovverket. Det er strenge regler for utveksling av sensitive persondata, spesielt når utvekslingen skal foregå over internett. Internett er et usikkert medium og det er ikke forsvarlig å utveksle sensitive data uten noen form for sikkerhet.

Evjeklinikkens deltakelse i dette prosjektet gjør det mulig med enda tettere oppfølging av pasienter. Tanken er at Evjeklinikken, fastlege, fagfolk og pasient skal få tilgang til MinJournal for å ha muligheten til å lese journalopplysninger og informasjon som er relevant.

1.2 Oppgavebeskrivelse

Prosjektet MinJournal søker å utvikle en internettbasert pasientjournal til bruk i helsetjenesten. Prosjektet ledes av Rikshospitalet – Radiumhospitalet HF og består av en rekke helseforetak og -institusjoner, blant annet Evjeklinikken. Hovedmålet med denne internettbaserte pasientjournalen er å gjøre det mulig for pasienter og helsepersonell å utveksle informasjon på en enklere og sikrere måte.

Oppgaven vil være å bistå i implementeringen av MinJournal på Evjeklinikken, og å identifisere og drøfte ulike praktiske og teoretiske problemstillinger i tilknytning til dette.

Oppgaven vil bestå av tre deler, der del én er å utvikle fire skjemaer til MinJournal. Disse skal utvikles i XML og være tilpasset Evjeklinikkens behov.

Del to innebærer å tilpasse en meldingstjeneste i MinJournal som Evjeklinikken kan bruke mellom ansatte og pasienter.
Del tre vil være teoretisk, der det gjøres rede for juridiske beskrankninger knyttet til håndtering av sensitive persondata i et internettbasert system. I tillegg vil denne delen inneholde en beskrivelse av hvordan Evjeklinikken i praksis imøtekommer de ovenfor nevnte juridiske beskrankningene.

1.3 Avgrensninger

Vi presiserer at vi vil kun bistå i implementeringen av MinJournal. Hovedfokuset vårt vil ligge på skjemautformingen og tilpasning av MinJournal, samt den teoretiske delen med beskrivelse av teknologi som er brukt og juridiske aspekter ved en slik implementering. Når det kommer til sikkerheten i MinJournal skal vi altså kun beskrive den og vise til eventuelle sårbarheter ved denne teknologien.

MinJournal er en portal som skal inneholde mange tjenester og muligheter i nær fremtid. Prosjektet MinJournal er ennå i startfasen og på langt nær slik de har ønske om at sluttproduktet skal fremstå. Det er derfor en del avgrensninger i oppgaven relatert til tilpasning av MinJournal på Evjeklinikken.

Vi skal utvikle skjemaene som Evjeklinikken skal bruke i MinJournal og tilpasse disse på best mulig måte med tanke på utseende og brukervennlighet. Videre skal vi se på meldingstjenesten og tilpasse denne så godt det går til Evjeklinikken og deres behov.

Vi skal altså ikke gjøre noe med MinJournal som innebærer endring av løsningen slik den er nå. Heller ikke endring av Evjeklinikkens rutiner inngår i vår oppgave, kun en vurdering av dem.

Rutinene for å motta og behandle de utfylte skjemaene, samt teknologien som blir brukt til dette, vil ikke være en del av vår oppgave. Det vi derimot skal gjøre er å beskrive hvordan denne prosessen er nå, før implementeringen av MinJournal, og hvordan denne prosessen vil bli etter implementering.

1.4 Rapportens oppbygging

I kapittel 2 gir vi en innføring og beskriver teorien som underbygger prosjektet. Det blir en innføring i de forskjellige relevante standardene og teknologiene som ligger bak MinJournal.

Videre vil vi beskrive den implementerte sikkerheten som ligger i bunn av
MinJournal-systemet, og en del som omhandler de juridiske beskrankninger og lovverket som gjelder ved bruk av et slikt system.

I kapittel 3 viser vi til hva andre har gjort med lignende systemer. Det innebærer også å beskrive hva som er gjort på Rikshospitalet – Radiumhospitalet HF angående utviklingen og implementeringen av MinJournal.

I kapittel 4 presenterer vi resultatene våre og gir en god gjennomgang av MinJournal hos Evjeklinikken. Vi vil også beskrive hvordan vi har løst oppgaven og fått det resultatet vi har fått.

Kapittel 5 inneholder drøfting av vårt resultat. Her diskuterer vi hva som kunne blitt gjort annerledes, resultatene og hvordan disse tilfredsstiller ønsket resultat.

Vi avslutter rapporten med kapittel 6 hvor vi kommer med en konklusjon, samt beskriver videre arbeid med MinJournal.

1.5 Litteraturstudie

Oppgaven vår består av en utviklingsdel og en teoretisk del. Begge disse har krevd mye forarbeid og består av mange forskjellige teknologier. Noen av teknologiene har vært velkjente mens andre har vært relativt nye for oss. Ved en beskrivelse av et nytt system som MinJournal, samt ved utvikling av skjemaer til et slikt system, er det viktig å ha en oppdatert forståelse og kunnskap om den relevante teknologien.

Ved denne litteraturstudien har vi for det meste brukt internett og søkemotorer som Google og Wikipedia. I motsetning til bøker er internett alltid oppdatert, men det finnes også mye feilinformasjon. Det er derfor viktig å være kritisk til artikler og stoff en finner på nettet. I utviklingen av skjemaene har vi brukt mest bokform for å lese oss opp om aktuell teknologi og for å søke etter løsninger på problemer.

1.6 Motivasjon

Vår motivasjon for denne oppgaven er at det er et nytt prosjekt med store mål. Prosjektet ved Evjeklinikken er helt i startfasen og vår oppgave vil være med å bidra til at MinJournal når de målene som er blitt satt for prosjektet.
Derfor anser vi oppgaven som viktig, spesielt for Evjeklinikken som bruker mye ressurser på oppfølging av pasienter.

Vårt arbeid vil sannsynligvis bli verdsatt og brukt av Evjeklinikken, og det igjen gjør at MinJournal vil få flere brukere. Ved at Evjeklinikken tar i bruk MinJournal gir en positiv effekt på andre helseinstitusjoner og -klinikker, som vil vurdere å selv ta i bruk løsningen. Videre er det en stor motivasjon for oss å vite at det vi gjør er relevant arbeid i forhold til en fremtidig jobbsituasjon, samt at produktet vårt kan ha stor nytte for flere mennesker.

2 Innføring og bakgrunn

I dette kapittelet vil vi ta for oss relevant lære vi mener er viktig både for gjennomføring av oppgaven, og for å få en god forståelse av det vi omtaler senere i rapporten.

I oppgavebeskrivelsen står det at vi skal utvikle skjemaer i XML. Det er da nødvendig for leser å ha litt bakgrunn i XML og hvordan det kan brukes. Vi gir derfor en grunnleggende innføring i den teknologien som trengs for utvikling av skjemaer og for å få en forståelse av hvordan disse fungerer.

Videre gjør vi rede for juridiske beskrankninger knyttet til håndtering av sensitive persondata i et internettbasert system. Vi går derfor nærmere inn på aktuelle lover og bestemmelser som er gjeldende, og som må tas i betraktning både ved implementeringen og bruk av et slikt system.

Vi går ikke i detalj i beskrivelsene, men prøver heller å gi leserne en grei og oversiktlig innføring av det vi mener er vesentlig. Derimot beskriver vi sikkerhetsløsningene på en litt mer detaljert måte, samt går i detalj ved noen angrepsscenarioer på de aktuelle sikkerhetsløsningene valgt av MinJournal.

2.1 Skjemautviklingen

Her følger en innføring av de viktigste begrepene og teknologiene for en grunnleggende forståelse av vårt arbeid ved utvikling av skjema til bruk i MinJournal.

2.1.1 HTML

HTML, Hyper Text Markup Language (3), brukes til Web-sider på internett og er en metode for å definere og tolke "tags" i henhold til SGML (Standard Generalized Markup Language (4)) regler. For å tolke og oversette HTML-kodene til et lesbart format bruker man en webleser, for eksempel Mozilla.

Et HTML dokument er et helt enkelt tekstdokument som inneholder skrift, tall og tegn. Ettersom HTML er tekstbasert kan hvem som helst lage et HTML-dokument ved å bruke en teksteditor som for eksempel Notepad. Et HTML-dokument er bygget opp av tagger som er rammet inn av spesielle tegn, ”<” og ”>”. Mellom start- og sluttaggene ligger informasjon til webleser om hvordan dokumentet skal se ut. I et HTML-dokument skriver man inn forskjellige kommandoer som forteller hvordan siden skal se ut.

Det finnes koder (elementer) for omtrent alt; Hvilken skrift man skal bruke, hvilken farge skriften skal ha, hvilken bakgrunn siden skal ha, om det skal være bilder på siden og så videre. I HTML er elementene låst til bestemte elementnavn som for eksempel: <h1>Overskrift</h1>, og overskrifter er ofte markert på denne måten i HTML. Dette kan en også se av Eksempel 1 under:

```
<html>
<head>
<title>Minimumskrav til hva et HTML dokument må inneholde</title>
</head>
<body>
<h1>Overskrift</h1>
Denne teksten vises på websiden
</body>
</html>
```

Eksempel 1: Minimumskrav HTML

2.1.2 XML

XML (Extensible Markup Language (5)) er en W3C-anbefaling for å strukturere eller beskrive data. XML ble introdusert for første gang i 1998 og ble raskt et populært og viktig format for utveksling av data på internett. Grunnen til at XML ble populært så raskt er at det er en enkel og allsidig standard. XML bruker Unicode-tegnsetting (6), som representerer alle tegnsystemer som brukes i dag. Et typisk XML-dokument er en tekstfil som bruker UTF-8 eller UTF-16, som er Unicode-basert tegnkoding.

I motsetning til i HTML kan man i XML definere egne elementer. Det vil si at det ikke er forhåndsbestemt hvilke elementer en må bruke, noe som gir mye større fleksibilitet. Å kunne definere egne elementer gjør at XML-formatet, i forhold til HTML, er lettere for utviklere å lese og forstå. XML er av den grunn kalt et selvbeskrivende format som beskriver struktur og datanavn i tillegg til dataverdiene.

For at et XML-dokument skal regnes for velformet og validert er det noen regler som må oppfylles. For det første har alle XML-dokument kun ett rotelement. Elementer som er såkalte ikke-tomme må ha en start- og slutt-tag med samme navn, mens tomme elementer kan angis med en lukket tag, <name />.

Videre må en huske at elementene er case-sensitiv, det vil si at en må ta hensyn til store og små bokstaver i elementene. En start-tag, for eksempel <name>, kan ikke avsluttes med en slutt-tag med feil "case", som for eksempel </Name>.
Siste relevante regel er at attributtverdier må settes i anførselstegn, og en må da bruke samme type anførselstegn på begynnelsen som på slutten av verdien. Dette kommer fram i Eksempel 2 under.

Ved å velge beskrivende elementnavn får dataene en mening, og strukturen blir lettere å lese. Det gjør dataene enklere for utenforstående å forstå, samtidig som de er like lesbare for datamaskiner og programmer. Dette kommer godt fram i Eksempel 2; et velformet XML dokument:

```
<?xml version="1.0" encoding="UTF-8"?>
<oppskrift navn="brød" forberedelsestid="5 minutter" totaltid="3 timer">
  <tittel>Vanlig brød</tittel>
  <ingrediens mengde="3" enhet="kopp">Hvetemel</ingrediens>
  <ingrediens mengde="7" enhet="ml">Gjær</ingrediens>
  <ingrediens mengde="1.5" enhet="kopp">Varmtvann</ingrediens>
  <ingrediens mengde="1" enhet="teskje">Salt</ingrediens>
  <fremgangsmåte>
    <trinn>Bland alle ingredienser og kna grundig.</trinn>
    <trinn>Dekk over med et klede og sett til heving i et varmt rom.</trinn>
    <trinn>Kna på nytt, legg i en form og stek ved 200 grader Celsius i 1
      time.</trinn>
  </fremgangsmåte>
</oppskrift>
```

Eksempel 2: Enkelt XML-dokument

"Et XML-dokument som er velformet og i tillegg oppfyller kravene i et tilknyttet XML Schema-dokument eller en DTD, kalles gyldig (engelsk: valid)." (7)

Som en ser av eksempelet er det XML 1.0 som brukes, og en ser også at slike attributtverdier må settes i anførselstegn. Den siste utgaven er 1.1, og ble lansert i februar 2004. Forskjellene på disse versjonene er ikke merkbare for den vanlige bruker og 1.1 trengs bare om du vil bruke Unicode i elementnavn. Versjon 1.0 tillater bare tegn, i element- og attributtnavn, som er lovlige i Unicode 2.0, mens versjon 1.1 bare har begrensninger i forhold til enkelte styretegn. I versjon 1.1 kan altså alle tegn brukes.

2.1.3 XHTML

XHTML (Extensible HyperText Markup Language (8)) er den siste versjonen av HTML. Istedenfor å lage en ny versjon av HTML, utviklet W3C (9) heller XHTML som også er kompatibel med XML. Det finnes to versjoner av XHTML, 1.0 og 1.1, hvor versjon 1.1 er mer krevende og tilbyr et rikere språk.
Nesten alle elementene og attributtene i XHTML er identiske til de i HTML, men det er noen forandringer, og ikke minst noen fordeler. Den største fordelen er at størrelsen på siden kan bli redusert og koden er lettere å lese.

2.1.4 XML Schema

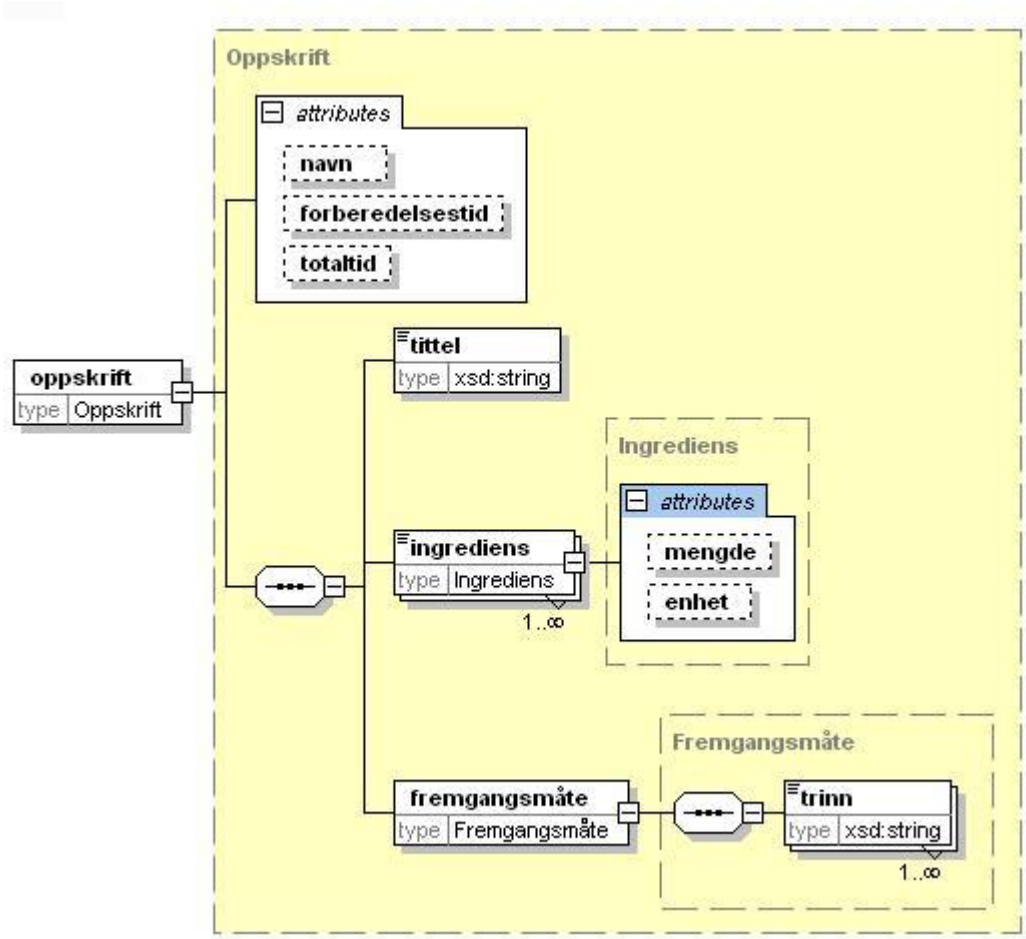
XML Schema (10) ble publisert i 2001 og ble det første XML skjemaspråk som ble anbefalt av W3C. XML Schema blir ofte kalt XML Schema Definition (XSD) og har filtypen *.xsd*.
Kort fortalt brukes XML Schema til å validere XML-dokumenter. Dokumentene blir da validert med hensyn på struktur og innholdsformater.

Det finnes flere XML skjemaspråk, for eksempel DTD (Document Type Definition (11)). DTD er det eldste skjemaspråket og kommer fra SGML. DTD er nå utdatert i forhold til XML Schema. Det er flere grunner til dette; Først og fremst har ikke DTD støtte for nye XML-egenskaper, som for eksempel navnerom.

XML Schema standarden er stor og omfattende, noe som kan gjøre den vanskelig å lese, samt å implementere. Uansett har XML Schema overtatt tronen som det beste og mest anvendte skjemaspråket. Nedenfor vises et enkelt og validert XML Schema, brukt til å validere Eksempel 2 om XML:

```
<?xml version="1.0" encoding="UTF-16"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified" attributeFormDefault="unqualified">
  <xsd:element name="oppskrift" type="Oppskrift"/>
  <xsd:complexType name="Oppskrift">
    <xsd:sequence>
      <xsd:element name="tittel" type="xsd:string"/>
      <xsd:element name="ingrediens" type="Ingrediens"
           maxOccurs="unbounded"/>
      <xsd:element name="fremgangsmåte" type="Fremgangsmåte"/>
    </xsd:sequence>
    <xsd:attribute name="navn" type="xsd:string"/>
    <xsd:attribute name="forberedelsestid" type="xsd:string"/>
    <xsd:attribute name="totaltid" type="xsd:string"/>
  </xsd:complexType>
  <xsd:complexType name="Ingrediens">
    <xsd:simpleContent>
      <xsd:extension base="xsd:string">
        <xsd:attribute name="mengde" type="xsd:decimal"/>
        <xsd:attribute name="enhet" type="xsd:string"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>
  <xsd:complexType name="Fremgangsmåte">
    <xsd:sequence>
      <xsd:element name="trinn" type="xsd:string" maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:schema>
```

Eksempel 3: Enkelt XML Schema dokument



Figur 1: Enkelt XML Schema vist i Altova XMLSpy

Figur 1 viser det samme skjemaet som i Eksempel 3. Det er vist i Schema-design, og ikke ren tekst. Til dette, og all skjemautforming, har vi brukt verktøyet Altova XMLSpy (12).

Ved å se skjemaet slik, ser en lettere strukturen på skjemaet, samt relasjonene mellom elementene.

2.1.5 XPath

XPath (13) er en standardisert måte å angi spesielle deler av et dokument på. Dette gjør at en dynamisk kan velge ut elementer fra et dokument i et stilark, for så å sette disse sammen i vilkårlig rekkefølge til ønsket resultatet.

Når en skriver XML vil en ofte at spesifikke deler av XML-dokumentet skal prosesseres på en bestemt måte. Et eksempel er om du publiserer grunnleggende opplysninger om ansatte på bedriftens interne nett. Da vil en sannsynligvis holde tilbake konfidensielle opplysninger om ansatte. Av dette eksemplet ser en viktigheten av å forstå teknologien som muliggjør å velge hvilke spesifikke deler av XML-dokumentet en vil prosessere. Xpath er designet akkurat for slike ting; Utvikleren skal kunne velge spesifikke deler av et XML-dokument.

XPath ble opprinnelig laget som en del av XSL (Extensible Stylesheet Language (14)), men ble generalisert som en egen anbefaling fordi den er nyttig for navigering i trær. Uttrykksformen for å orientere seg i en trestruktur kalles XPath.

Et XPath uttrykk kan bestå av inntil tre deler; Axis, nodetest og predicate. For eksempel: *"child::para[position()=1]",*
som angir "det første elementet av typen para som er barn av kontekstnoden".

child	axis angir hva slags relasjon vi ønsker i forhold til kontekstnoden
para	nodetest angir hva slags type node vi er interesserte i
position()=1	predicate plukker ut et utvalg av de nodene vi har kvalifisert ved axis og nodetest

Med kontekstnoden i oversikten nedenfor mener vi den noden vi "befinner oss på", altså den vi skal orientere oss i forhold til, i dokumenttreet.

XPath-uttrykket:	velger ut:
child::para	alle elementer av typen para som er barn av kontekstnoden
child::*	alle elementer som er barn av kontekstnoden
child::text()	alle tekstnoder som er barn av kontekstnoden
child::para[position()=1]	det første elementet av typen para som er barn av kontekstnoden

2.1.6 XForms

XForms (15) (16) er en XML-basert skjemateknologi spesifisert av W3C. XForms er XML-versjonen av HTML-forms og ble utviklet for å bli neste generasjon av HTML/XHTML-forms. Kort fortalt er XForms et standardisert sett med elementer (tagger) fra HTML-form som er laget for å bli integrert med andre internettbaserte standarder. Det vil si at XForms er en slags utvidelse av XHTML som definerer noen spesifikke tags. Disse tags kan ikke vises med en vanlig webleser, men må prosesseres med et verktøy før kompatibilitet mot en vanlig webleser.

XForms er et viktig verktøy for alle XML-utviklere, og skjemaer er en viktig del av internett. Skjemaer vil fortsette å være det primære hjelpemiddelet for å muliggjøre interaktive applikasjoner på internett. Internettapplikasjoner og løsninger for e-handel har ytret krav om bedre skjemaer og interaksjon på internett. XForms 1.0 er både et svar og en løsning på dette kravet.

XForms er et XML format for spesifiseringen av en dataprosessmodell for XML data og brukergrensesnitt for XML data, som for eksempel webskjema.

Dataene som er hentet inn fra et XForms dokument er velformet XML. En XForms-prosess har en XML Schema-prosess innebygget slik at det er muligheter for å validere opplysningene som brukeren oppgir opp mot et spesifisert XForms skjema.
Det første utkastet av XForm spesifikasjonen ble offentliggjort 6. april 2000, og har siden den gang blitt forbedret med en revidert utgave av versjon 1.0. Den reviderte versjonen kom i mars 2006. XForms 1.1 er det siste utkastet og ble publisert 22. februar 2007.

2.2 Juridiske aspekter ved internettbasert pasientjournal

Dette kapittelet tar for seg noen av de mest sentrale juridiske problemstillingene som dukker opp ved implementeringen av MinJournal på Evjeklinikken.

Ved innføring av internettbasert pasientjournal er det mange og store utfordringer i forhold til lovverket. Norsk helselovgivning er moderne og omfattende, og legger strenge rammer for hvordan helsepersonell og helseinstitusjoner skal drive virksomheten. Samtidig må en ikke glemme at også pasienter har klare og lovfestede rettigheter.

Mange ser på denne strenge lovgivningen som et stort problem ved etablering av IKT-løsninger i helsevesenet, og da særlig ved en internettbasert løsning. I mange tilfeller er dette synet på det norske lovverket feil, ettersom problemet ikke ligger i for strenge lover men derimot i for dårlige løsninger. Det kreves gode og avanserte løsninger for at en internettbasert pasientjournal skal ligge innenfor lovverket. Helselovgivningen er altså et rammeverk rundt all aktivitet innenfor helsevesenet, og setter grenser for hva som er tillatt av hvem, når og hvordan. I dette kapittelet går vi mer i detalj på enkelte lovregler som er sentrale ved etablering av en slik IKT-løsning i en helseinstitusjon.

2.2.1 Taushetsplikt, personvern og informasjonssikkerhet

Problemstillinger rundt taushetsplikt, personvern og informasjonssikkerhet er de mest sentrale i møtet mellom IKT og helse. Helselovgivningen har en kultur der så lite informasjon som mulig skal samles inn, og der så lite som mulig skal spres til så få parter som mulig. IKT og internett derimot har en helt motsatt kultur, og det er her de juridiske utfordringene ved en internettbasert pasientjournal ligger.

2.2.1.1 Taushetsplikt

Bestemmelsen om taushetsplikt finnes i Helsepersonelloven (17) kapittel fem og hovedregelen fremgår av lovens § 21:

§ 21. Hovedregel om taushetsplikt
"Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell."

I tillegg til denne er det en samsvarende paragraf i Pasientrettighetsloven (18). Denne loven tar utgangspunkt i pasientens ståsted og rettighetene til pasienter.

§ 3-6. Rett til vern mot spredning av opplysninger
"Opplysninger om legems- og sykdomsforhold samt andre personlige opplysninger skal behandles i samsvar med gjeldende bestemmelser om taushetsplikt. Opplysningene skal behandles med varsomhet og respekt for integriteten til den opplysningene gjelder.

Taushetsplikten faller bort i den utstrekning den som har krav på taushet, samtykker.

Dersom helsepersonell utleverer opplysninger som er undergitt lovbestemt opplysningsplikt, skal den opplysningene gjelder, så langt forholdene tilsier det informeres om at opplysningene er gitt og hvilke opplysninger det dreier seg om."

Som en ser av §§ 21 og 3-6 i henholdsvis helsepersonelloven og pasientrettighetsloven, er ikke bare taushetsplikten en plikt for helsepersonell men også en rett for pasienten. Taushetsplikt skal først og fremst verne om pasientens integritet og dermed skape tillit mellom pasient og helsepersonell. Et slikt tillitsforhold er helt avgjørende for at en eventuell behandling skal bli en suksess for begge parter. Taushetsplikt skal ikke beskytte helsepersonell, og helsepersonell kan heller ikke hindre en pasient i å opplyse andre om den behandling som er gitt. Det er også hensiktsmessig å informere at det kun er opplysninger en mottar i egenskap av å være helsepersonell som er taushetsbelagte etter helsepersonellovens bestemmelser. Opplysninger man får som privatperson er altså ikke underlagt bestemmelsene i helsepersonelloven, selv om de angår helseforhold. Det har oppstått grensetilfeller der det er tvil om opplysningene er gitt til behandleren i egenskap av helsepersonell eller som privatperson. Her står og faller det på helsepersonellets skjønn og etikk da det ikke er noen konkrete bestemmelser angående dette.

§ 21 i helsepersonelloven dikterer at "*Helsepersonell skal hindre at andre får adgang..*". En skal altså kun "*hindre*" at andre får adgang til opplysninger som er private og sensitive. I begrepet "*hindre"* er det både en aktiv plikt til å beskytte opplysningene og en passiv plikt til å passe på at opplysningene ikke spres til andre. Andre er definert som alle uten pasienten selv og det som kalles samarbeidende helsepersonell. I praksis vil dette si at en eventuell lege har taushetsplikt også mot samarbeidende helsepersonell, med mindre det foreligger særlige grunner til at disse skal involveres.

Den aktive og passive plikten til å bevare taushetsplikten ivaretas gjennom en kombinasjon av flere faktorer. Disse gjelder enten opplysningene er hentet inn gjennom MinJournal eller gjennom den ordinære ordningen med pasientkonsultasjoner. Sikkerhet og etikk er stikkord her, men også internkontrollsystemer og innarbeidete rutiner i organisasjon eller helseforetak er viktig.

2.2.1.2 Personvern

Ved innføring og bruk av IKT har det kommet mer fokus på problemstillinger knyttet til personvern og informasjonssikkerhet i helsevesenet. Problemstillingene knyttet til dette er blitt relevante på en helt ny måte etter innføringen og bruk av IKT. Det er allikevel viktig å presisere at personvern og informasjonssikkerhet angår all helseinformasjon i helsevesenet, uavhengig av hvilke teknologier som blir brukt.

Begrepet personvern er forholdsvis nytt i juridisk terminologi og er et sammensatt begrep. Det beskriver et vern eller hensyn som går langt tilbake i tid, men som også angår informasjon og opplysninger i helsevesenet. Kjernen av begrepet beskriver hensynet til individets interesse i å utøve kontroll med den informasjon som finnes. Personvern dreier seg altså om å verne individets personlige integritet samt respektere individets kontroll av opplysningene.

Personverninteressene kan være individuelle eller kollektive, men for MinJournal er det først og fremst de individuelle som er viktige og må ivaretas. Pasienter skal selvfølgelig ha vern mot at det hentes inn opplysninger om dem som ikke er relevante for en tjeneste eller behandling. De skal også vernes mot at uvedkommende får tilgang til disse opplysningene. Et eksempel på hvor det kan være hensiktsmessig å hente inn opplysninger om pasienter er ved forskningsprosjekter. Men også her vil det forekomme konflikter angående innsamling av helseopplysninger og personvernhensyn. Et annet eksempel er deling av pasientinformasjon i forbindelse med en konkret behandling. Her kan delingen gå på tvers av virksomheter eller bare innad i en virksomhet.

2.2.1.3 Utlevering, deling og tilgang

Det er i mange tilfeller nødvendig å dele pasientinformasjon mellom helsepersonell eller virksomheter i behandlingen av pasienten. Norsk helselovgivning tillater slik nødvendig deling av pasientinformasjon, og det finnes konkrete bestemmelser i lovverket for å formalisere slik utveksling av informasjon. De to mest sentrale bestemmelsene er §§ 25 og 45 i helsepersonelloven. Disse stiller et ubetinget krav om nødvendigheten av å utveksle informasjonen for at utveksling til samarbeidende helsepersonell, eller til andre som yter helsehjelp, skal gis. § 25 omhandler samarbeidende personell mens § 45 gjelder andre som yter helsehjelp. Disse paragrafene, samt lovens formål og hvem den gjelder, er gjengitt under slik at en får et overordnet syn på helsepersonelloven.

§ 1. Lovens formål.
"Lovens formål er å bidra til sikkerhet for pasienter og kvalitet i helsetjenesten samt tillit til helsepersonell og helsetjeneste."

§ 2. Lovens virkeområde.
"Loven gjelder helsepersonell og virksomheter som yter helsehjelp i riket. …"

§ 25. Opplysninger til samarbeidende personell.

"Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp. Taushetsplikt etter § 21 er heller ikke til hinder for at personell som bistår med elektronisk bearbeiding av opplysningene, eller som bistår med service og vedlikehold av utstyr, får tilgang til opplysninger når slik bistand er nødvendig for å oppfylle lovbestemte krav til dokumentasjon. Personell som nevnt i første og andre ledd har samme taushetsplikt som helsepersonell."

§ 45. Overføring, utlevering av og tilgang til journal og journalopplysninger.

"Med mindre pasienten motsetter seg det, skal helsepersonell som nevnt i § 39 gi journalen eller opplysninger i journalen til andre som yter helsehjelp etter denne lov, når dette er nødvendig for å kunne gi helsehjelp på forsvarlig måte. Det skal fremgå av journalen at annet helsepersonell er gitt tilgang til journalen etter første punktum.

Departementet kan i forskrift gi nærmere bestemmelser til utfylling av første ledd, og kan herunder bestemme at annet helsepersonell kan gis tilgang til journalen også i de tilfeller som faller utenfor første ledd."

Som en ser av §§ 25 og 45 skal deling kun skje om det er knyttet til en konkret behandlingssituasjon og at det skal være *nødvendig*. Dette betyr at det skal gjøres en faglig vurdering av hva slags opplysninger som skal gis, samt hva slags opplysninger det skal forespørres om. Uten en slik vurdering skal det ikke gis ut journal-opplysninger.

For Evjeklinikken er §§ 25 og 45 sentrale da de hos Evjeklinikken jobber med pasienter på flere nivåer. Psykisk og fysisk trening, ernæringsrådgivning og oppfølging krever at mange parter jobber sammen. Medisinsk, psykologisk, ernæringsfaglige - og fysikalske vurderinger koordineres i en samlet plan. Denne virksomheten har som et premiss at samarbeidende fagpersonell må dele relevante pasientopplysninger. Det er derfor helt nødvendige å tilgjengeliggjøre pasientens journal til alle involverte parter som har behov for denne for å kunne utføre sitt arbeid på en forsvarlig måte. Dette må ifølge loven avtales med pasienten det gjelder, og han eller hun kan motsette seg en slik utlevering av journalen. Ved Evjeklinikken avgir pasienten et skriftlig samtykke på at slik deling av informasjonen kan skje.

Ved prosjekter som MinJournal er det en pågående diskusjon vedrørende tilgang til helseregistre på tvers av virksomheter. Helseregisterloven (19) § 13 begrenser tilgang til helseregistre til den som arbeider under databehandlingsansvarliges eller databehandlers instruksjonsmyndighet. Dette begrenser og avskjærer muligheten for tilgang på tvers av virksomheter. Nedenfor vil vi se nærmere på relevante bestemmelser i helseregisterloven og helsepersonelloven.

Helseregisterlovens formål er beskrevet i § 1 som er gjengitt på neste side i rapporten. Formålsbestemmelsen i § 1 legger stor vekt på at behandlingen av helseopplysninger skal skje i samsvar med grunnleggende personvernhensyn. Disse personvernhensynene kan som tidligere nevnt deles opp i individuelle og kollektive interesser. Pasienter kan ha interesse av at andre pasienter deler sine helseopplysninger for å bedre kvaliteten på behandlingstilbudet, men pasienten kan samtidig ha interesse av å holde tilbake sine egne helseopplysninger på grunn av personvern.

Tiltak og reguleringer som skal ivareta pasientens interesser vil på mange områder også ivareta pasientens personverninteresse. En kan derfor si at den enkelte pasients pasientrettigheter og personvernrettigheter har samme interesser og i stor grad er sammenfallende.

§ 1. Lovens formål
"Formålet med denne lov 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. Gjennom forskning og statistikk skal loven bidra til informasjon og kunnskap om befolkningens helseforhold, årsaker til nedsatt helse og utvikling av sykdom for administrasjon, kvalitetssikring, planlegging og styring. Loven skal sikre at helseopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på helseopplysninger."

§ 13 *"Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon"* i helseregisterloven er sentral for Evjeklinikken. Loven sier at:
"Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt."

Det er altså kun de som arbeider for databehandler med selve registeret som skal og kan ha tilgang til informasjonen i registeret. For alle slike helseregistre er det et krav at databehandleransvarlig og databehandler skal sørge for tilfredsstillende informasjonssikkerhet. Informasjonssikkerhet i denne sammenhengen er konfidensialitet, integritet og tilgjengelighet ved behandling av helseopplysninger. Kort fortalt vil det si at helseopplysningene i helseregisteret er tilgjengelig bare for dem som er autorisert for bruk av disse opplysningene, og at de er tilgjengelig ved behov. Sist men ikke minst må opplysningene som ligger i registeret være korrekte og fullstendige.

Bestemmelser angående dette er gjengitt i § 16 *"Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet"*: *"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 gjennom planlagte og systematiske tiltak kan en bruke ulike verktøy. Risikoanalyse er et slikt verktøy, og gjennom systematisk bruk av risikoanalyse kan en vurdere krav, trusler og nødvendig sikkerhetsnivå. Disse vil selvsagt variere avhengig av informasjonssystem og type informasjon, og graden av sikring skal fastsettes ut fra konkrete analyser, bestemmelser i lover, forskrifter og internt regelverk.

Videre står det at for å oppnå tilfredsstillende informasjonssikkerhet må databehandler dokumentere informasjonssystemet og de sikkerhetstiltak som er gjort. Informasjonssystem er et system for behandling, lagring og overføring av informasjon. Denne dokumentasjonen gjøres både av hensyn til ansatte og brukere av informasjonssystemet, etterfølgende kontroller, og av hensyn til tilsynsmyndighetenes rett til denne dokumentasjonen. Dokumentasjonen skal altså være tilgjengelig for medarbeiderne hos den databehandlingsansvarlige, hos databehandleren, og tilgjengelig for tilsynsmyndighetene.

Databehandlingsansvarlig er den som bestemmer formålet med behandlingen av helseopplysningene, mens databehandler er den som behandler opplysningene på vegne av den databehandlingsansvarlige.

Ved Evjeklinikken er det etablert en databehandlingsansvarlig og databehandlere. Disse ansattes rolle og funksjon er definerte og det er gjennomført ROS-analyser (risiko- og sårbarhetsanalyse) i henhold til regelverket. Som en følge av implementeringen av MinJournal er det ved klinikken igangsatt revisjon av ROS-analysene, samt en redefinering av ansvarsområder knyttet til databehandling.

Vår tilgang til MinJournals testsystem berører ikke de beskrevne juridiske problemstillingene. Derimot gjelder bestemmelsene om taushetsplikt noe av dokumentasjonen vi har mottatt, ettersom dette er sensitive opplysninger som kan misbrukes av uvedkommende.

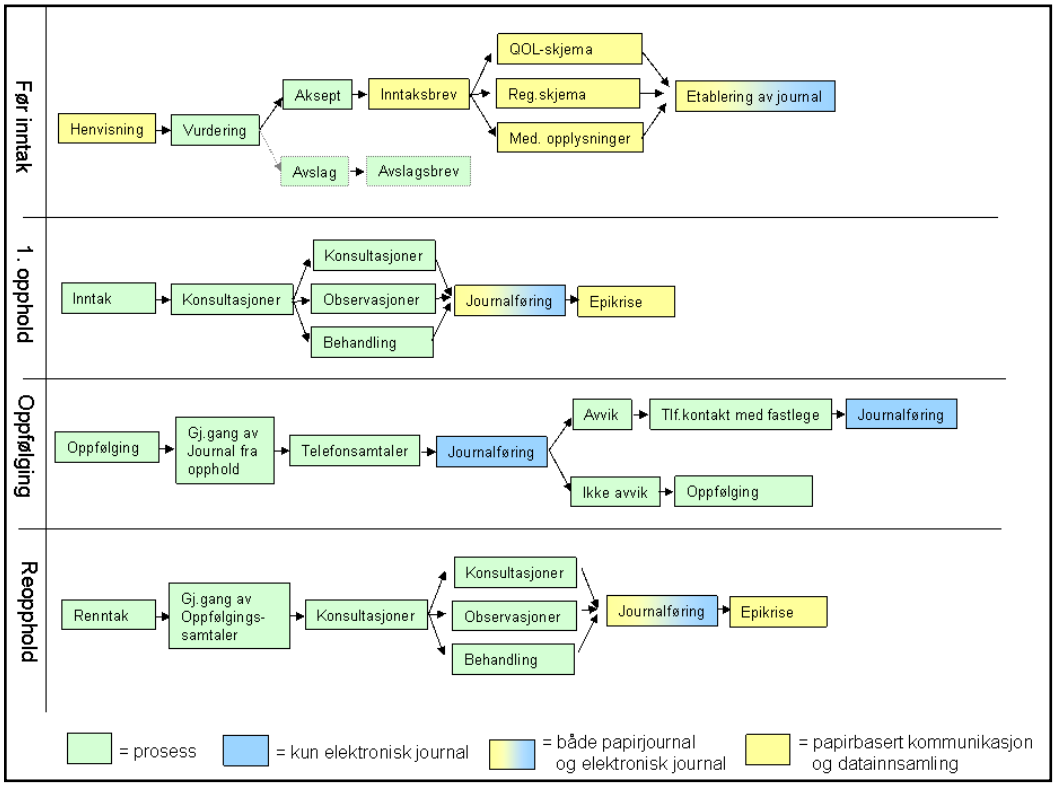
Vi har nå gått gjennom og beskrevet de mest sentrale juridiske problemstillingene og bestemmelsene som gjelder ved implementering og bruk av MinJournal på en helseinstitusjon. Videre skal vi beskrive aktuell sikkerhetsteknologi som sikrer at disse lovene og bestemmelsene kan bli oppfylt og tilfredstilt.

2.3 Prosess- og dokumentflyt ved Evjeklinikken

Vi går her kort gjennom prosess- og dokumentflyten på Evjeklinikken slik den er i dag. I kapittel fire beskrives det hvordan Evjeklinikken ønsker at prosess- og dokumentflyt skal foregå etter en implementering av MinJournal.

Som Figur 2 under viser, ender alle prosesser opp i en dokumentasjon i en papirbasert eller elektronisk journal. Papirbaserte dokumenter (henvisninger, pasientopplysninger, inntaksbrev, epikriser) skannes i utgangspunktet ikke, men legges tilgjengelig i den papirbaserte journalen. Viktige medisinske opplysninger (for eksempel allergier, anamnese, medikamentbruk, laboratoriesvar etc.) noteres også i den elektroniske journalen.

I dag fylles registreringsskjemaene ut (ernæring, aktivitet) og gjennomgås av fagpersonellet som forberedelser til konsultasjon. De arkiveres etter dette i pasientens papirjournal. Forskningsskjemaene påføres løpenummer (for anonymisering), lagres i permer og punches elektronisk for senere analyse (effektmåling og forskning).
Øvrige prosesser (for eksempel telefonoppfølging, konsultasjoner etc.) dokumenteres i den elektroniske journalen. Etter hvert opphold ved klinikken sendes det en papirbasert epikrise til pasientens fastlege. Kopi av epikrisen ligger i den elektroniske journalen.



Figur 2: Prosess- og dokumentflyt ved Evjeklinikken

2.4 Sikkerhet

I dette kapittelet beskrives aktuelle begreper og teknologier innen informasjonssikkerhet. Vi begynner med en gjennomgang av sentrale begreper og fordyper oss så i teknologier og forskjellige sikkerhetsløsninger som benyttes av MinJournal.

2.4.1 Internett og risiko ved bruk

Internett ble opprinnelig utviklet som et lukket testnettverk for militæret i USA, som ville bruke det til å koble sammen sine radarstasjoner. Joseph Carl Robnett Licklider, som stod bak prosjektet, forflyttet seg til MIT og utviklet det videre til det som etter hvert skulle bli til det vi i dag kjenner som internett.

Det var selvfølgelig begrenset hva dette nettverket kunne brukes til siden det ble utviklet på 1950-60-tallet. Utviklerne tenkte aldri over eventuelle problemer som kunne oppstå på grunn av det kommende verdensomspennende nettverket. Det fantes ikke, og finnes fortsatt ingen sikkerhetsmekanismer i selve nettet. Slike mekanismer, i tillegg til mer avansert funksjonalitet, må leveres av applikasjoner eller enheter i nettet som for eksempel servere og rutere.
Utviklingen av internettjenester eksploderte 1990 og utover, og det finnes en stor mengde tjenester i det moderne samfunnet i dag som er avhengige av internett for å fungere. Dette har gjort internettkriminalitet utbredt, og behovet for å sikre utvekslingen av informasjon er stort.

Mange er ikke klar over risikoen ved bruk av internett og hvor enkelt det er å stjele alt fra identiteter til bankkontoer, epost-passord og lignende. Dyktige hackere vil i mange tilfeller kunne avlytte forbindelsen mellom PC-en din og en server på nettet for å prøve å snappe opp passordet til for eksempel epost-kontoen din. Denne utnyttingen av forbindelser er ofte mulig å gjøre selv med all verdens sikring av både data og kommunikasjon. Poenget er å gjøre det så vanskelig eller så tidkrevende at ingen tar seg bryet å prøve, eller at informasjonen er utdatert før de klarer å få tak i og utnytte den.

Nettbanker er et eksempel hvor sikring av forbindelse er spesielt viktig. En slik forbindelse vil alltid overføre sensitive opplysninger, og må sikres mot eventuelle angrep. Her brukes derfor alltid en eller annen form for avansert sikring av forbindelsen mellom PC-en din og nettbankserveren. Det kreves ofte både personnummer/kontonummer, passord og en PIN-kode som enten er oppført på et engangskodekort eller genereres med en kodekalkulator. I tillegg sikres først overføringen av disse personlige opplysningene med kryptering (Se kapittel 2.5.3 om SSL). Dette gjør det vanskelig å stjele noe som helst ved avlytting.

Et annet eksempel er at ved overføring av høyst sensitive data som pasientjournaler og personopplysninger, slik som det blir gjort i MinJournal, kreves det enda strengere tiltak som stopper nesten alle former for tyveri og avlytting. Det brukes da et smartkort (kapittel 2.5.1), omtrent som de som brukes i GSM-telefoner, for å lagre en persons identitet i et såkalt PKI-sertifikat (nærmere beskrevet i kapittel 2.5.2 på side 23). Identiteten er dermed bundet til et smartkort som igjen er sikret med en personlig PIN-kode i likhet med et bankkort.

For å få en bedre forståelse for problemene rundt drift av systemer som MinJournal, er det flere begreper og teknologier innen informasjonssikkerhet som bør forklares. Disse tar vi for oss i de neste delkapitlene.

2.4.2 Introduksjon til informasjonssikkerhet

For å oppnå tilfredsstillende informasjonssikkerhet på data må konfidensialitet, integritet og tilgjengelighet være i fokus. Kravene til konfidensialitet, integritet og tilgjengelighet vil variere avhengig av informasjonssystem og type informasjon. For eksempel ved behandling av pasientopplysninger der det er viktig med konfidensialitet, skal dette kravet prioriteres fremfor hensyn til tilgjengelighet. Sammenhengen mellom disse tre begrepene er vist i Figur 3, der vi tenker oss at et gitt system plasseres som en prikk i trekanten. Man kan dermed ikke oppnå alle tre samtidig, men en kombinasjon der den ene går på bekostning av de to andre.

De fleste sikkerhetsløsninger i dag vil bestå av flere av disse begrepene og løsningene. For eksempel vil en PKI-løsning inneholde sertifikater for å sikre autentisering, og dermed integritet, og en form for kryptering for å sikre konfidensialitet. Vi kommer nærmere inn på dette i innføringen av disse begrepene.

Figur 3: Informasjonssikkerhets-trianglet

2.4.2.1 Konfidensialitet

Konfidensialitet vil si at en ressurs eller opplysning holdes hemmelig fordi det innebærer sensitive data eller ressurser som ikke alle skal ha tilgang til. I helsetjenesten gjelder dette for eksempel tilgang til pasientopplysninger. Om man jobber på et sykehus skal man ikke ha tilgang til alle pasientopplysningene. Denne tilgangen skal man kun ha dersom det er nødvendig eller at man har rett til det. Å sikre konfidensialitet inkluderer autentisering, autorisering og kryptering.

Autentisering vil si at man sikrer at brukeren er den han eller hun gir seg ut for å være. Slik autentisering er basert på tre prinsipper; noe du vet (passord), noe du har (smartkort), noe man er (fingeravtrykk). Sterkest autentisering oppnår man med en kombinasjon av disse prinsippene. MinJournal bruker en kombinasjon av noe du vet og noe du har, altså et smartkort du kan bruke med korrekt PIN-kode.

Autorisering vil si at man holder rede på hvilke ressurser og informasjon en bruker har tilgang til. Dette er en nødvendighet på lik linje med autentisering for at systemet skal kunne tildele de rettigheter den autentiserte brukeren skal ha. Disse rettighetene har administrator av systemet satt på bakgrunn av hvilke ressurser eller informasjon den enkelte bruker eller brukergruppe skal ha. Her gjelder need-to-know prinsippet som sier at man ikke skal ha tilgang til mer enn det som trengs for å gjøre den jobben man er ansatt for å gjøre.

Kryptering brukes for å kunne sende informasjon mellom systemet og bruker uten at uvedkommende skal få tilgang til informasjonen. Dette er spesielt viktig når informasjon skal sendes over internett, for eksempel når data hentes fra MinJournal og skal lagres internt på Evjeklinikken.

2.4.2.2 Integritet

Integritet viser til at informasjon eller ressurser er riktige og pålitelige. Det omhandler normalt at endringer som ikke er autoriserte og dermed kanskje feilaktige skal forhindres. Pålitelighet av informasjonen i MinJournal er viktig siden det skal være en pålitelig informasjonskilde for brukerne.

For å sikre integriteten er det to ting som er nødvendige. Det ene er at man må sikre at det kun er autoriserte personer som kan legge inn, oppdatere eller fjerne informasjon. Dette ble nevnt under innføringen av konfidensialitet, og skal gjøre at systemet er innbruddssikkert mot innlogging av uautoriserte personer samt hindre bakdørsangrep.
Det neste som må gjøres er å etablere en prosess der man har god kvalitetssikring av informasjonen som skal være tilgjengelig på MinJournal.

2.4.2.3 Tilgjengelighet

Tilgjengelighet omhandler aksess til informasjonen, eller ressurs når man har behov for det. Behov for tilgjengelighet vil variere fra system til system, men har man et system som ikke er tilgjengelig når det trengs kunne det like godt ikke eksistert.

For å oppnå tilfredsstillende tilgjengelighet må den tekniske løsningen være bra. Den må kunne håndtere trafikken på systemet, og ikke minst må systemet komme raskt på beina igjen etter eventuelle feil. Det vil være vanskelig for dem som designer og utvikler systemet å beregne trafikkbelastningen på systemet. Det er derfor viktig at løsningen lett lar seg utvide, slik at kapasiteten kan øke om man opplever større belastning på systemet enn forventet.

Om det av ulike grunner skulle oppstå feil er det nødvendig at det blir ført logger. På denne måten kan systemet varsle om feil. En form for sikkerhetskopiering må også være på plass for å sikre fullkommen tilgjengelighet.

Når man tenker tilgjengelighet drar man som oftest ikke paralleller til informasjonssikkerhet. Men det er mange angrep som går ut på å gjøre data eller ressurser utilgjengelige. Slike system er ofte bygd på en statistisk modell for å analysere forventede bruksmønstre. Disse mekanismene garanterer den tenkte tilgjengeligheten så lenge den statistiske modellen er riktig opp mot virkeligheten. Det angriperne kan utnytte med et slikt system er at de kan manipulere disse analyserte bruksmønstrene, slik at antakelsene bak den statistiske modellen ikke vil være gyldige lengre. Ved at analysen for det tenkte systemet er manipulert og feil, vil det kanskje gjøre at systemet vil arbeide under forhold det ikke var tiltenkt og dermed bli ustabilt.

Forsøk på å blokkere tilgjengeligheten, såkalte Denial of Service (DoS)-angrep (20), som innebærer å overbelaste sentrale enheter i nettverket slik at de ikke kan levere tjenester som normalt (og ofte slutte å fungere i det hele tatt), er vanskelige å oppdage. Man må analysere trafikken og se om de uvanlige bruksmønstrene og endring av trafikken har miljømessige årsaker, eller om det er et angrep. Et slikt angrep vil stjele så mye av ressursene i et nettverk at systemet vil bli ustabilt og i verste tilfelle slutte å fungere. Da vil det være forholdsvis lett for erfarne hackere å angripe et slikt sårbart system.

2.4.3 Helsenett

"Norsk Helsenett er et lukket nettverk for elektronisk kommunikasjon og samhandling i helse- og omsorgssektoren i Norge." (21)

Helsenettet tilbyr et tilfredsstillende sikkerhetsnivå slik at helsevesenet kan utveksle pasientsensitiv informasjon på et privat nett. Sikkerhetstiltakene innebærer integritet, konfidensialitet og tilgjengelighet.

Visjonen til Norsk Helsenett er å bidra til gode og sammenhengende tjenester innen helse og omsorg. Dette skal oppnås ved å være et sektornett for effektivt samarbeid mellom de ulike tjenesteleddene i sektoren.

Norsk helsenett skal bidra til en mer helhetlig tenkning, med mange nye muligheter og åpner for enklere samarbeid mellom flere klinikker. Arbeidsdeling, kompetanse og spesialisering er noen eksempler på gevinster en vil oppnå ved et standardisert helsenett.

Helsenettet er representert i alle regionene, og alle aktører i helse- og omsorgssektoren er helsenettets målgruppe. For småaktører er det ofte et spørsmål om økonomi angående tilknytning til helsenettet.

2.5 Teknologier for sikring av MinJournal

I denne delen vil vi gå mer i detalj på sikkerhetsløsningene som er brukt i MinJournal. Vi beskriver først og fremst begrepene fra et teknisk ståsted, men nevner også eventuelle sårbarheter i disse løsningene ved å beskrive konkrete eksempler eller scenarioer.

2.5.1 Smartkort

Rikshospitalet – Radiumhospitalet HF har valgt å bruke smartkort (22) for autentisering fordi det tilfredsstiller kravet for å kunne bruke sikkerhetsgradering ”personsikkerhet høy”. Dette er et krav for å kunne overføre sensitive personopplysninger og journaler over internett.

Rikshospitalet – Radiumhospitalet HF skriver i sin dokumentasjon av MinJournal (23):
”Noen offentlige tjenester krever elektronisk ID med sikkerhetsnivå standard, andre krever sikkerhetsnivå høyt. Det kreves ulike sikkerhetsnivåer fordi det er forskjell i kravet til sikkerhet ved de ulike offentlige tjenester du ønsker å benytte.Helseopplysninger krever nivå høyt.

Forskjellen på elektronisk ID med sikkerhetsnivå standard og høyt er:

- *Elektronisk ID med sikkerhetsnivå høyt får du kun med personlig fremmøte hos tilbyder. Elektronisk ID med sikkerhetsnivå høyt gir deg tilgang til flere offentlige tjenester enn elektronisk ID med sikkerhetsnivå standard.*
- *Elektronisk ID med sikkerhetsnivå standard kan du laste ned og installere på din PC, via Internett. Nedlastingen kan du gjøre fra tilbydere av elektronisk ID med sikkerhetsnivå standard.”*

En av fordelene med smartkort er at det personlige digitale sertifikatet er lagret på kortet, beskyttet med en PIN-kode. Et digitalt sertifikat kan sammenlignes med en digital utgave av et pass, og inneholder blant annet navn, personnummer, en offentlig og en privat krypteringsnøkkel, og et unikt sertifikatnummer.

2.5.1.1 Litt historie

Smartkortet ble utviklet og patentert på 1970-tallet. Det er usikkert hvem som er den virkelige oppfinneren av smartkortet. Det er uenighet om det er tyskeren Jürgen Dethloff, japaneren Kunitaka Arimura eller franskmannen Roland Moreno. Den første utbredte bruken av kortene var for betaling i franske telefonkiosker (Télécarte) fra 1983.

Michel Ugon fra Honeywell Bull utviklet det første mikroprosessorbaserte smartkortet i 1977. Idag har Honeywell Bull ca. 1200 patenter som er relatert til smartkort.

På 1990-tallet fikk smartkortet et ekstra løft når det smartkortbaserte SIM-kortet til GSM-telefoner ble utviklet. Den voldsomme produksjonen av telefoner som bruker disse kortene gjorde at smartkortene ble vanlige. I de senere år har det også blitt integrert smartkort i bank- og kredittkort, som for eksempel i VISA-kort.

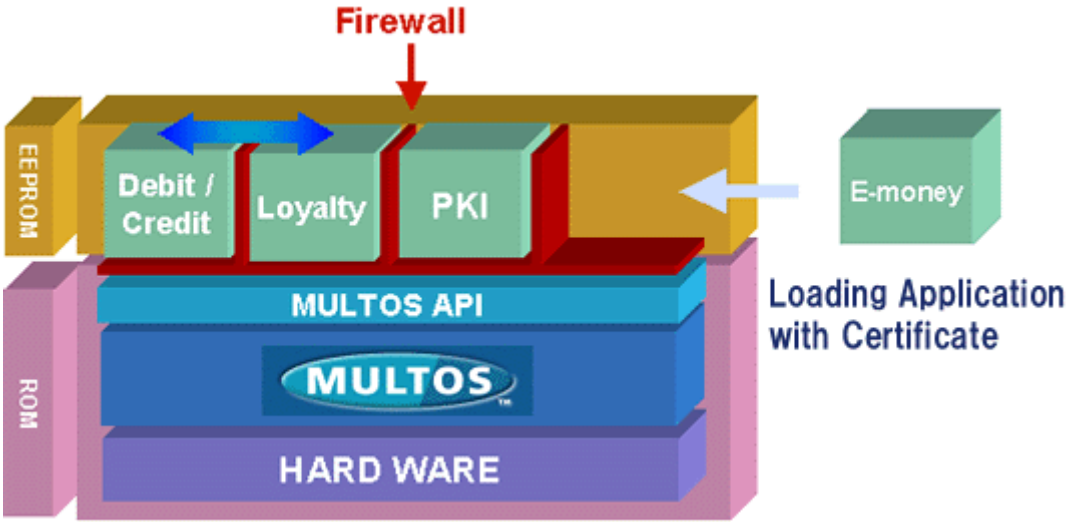
2.5.1.2 Kontaktbaserte smartkort

Dagens smartkort er på samme størrelse som bankkort. De har en gullbelagt chip som er omtrent 12 mm bred på den ene siden av kortet. Dette er koblingspunktet til kortleseren som muliggjør lesing og skriving av data på kortet.

Det finnes to standarder for smartkort; ISO/IEC 7816 (24) og ISO/IEC 7810 (25). (BuyPass-kortet følger ISO 7810)

Disse standardene definerer:

- Fysisk utforming og materialbruk
- Posisjon og utforming av elektriske tilkoblingspunkter
- Elektrisk karakteristikk
- Kommunikasjonsprotokoller
- Formatet på kommandoer sendt til og fra kortet
- Funksjonaliteten til kortet



Figur 4: Hitachis smartkortarkitektur med MULTOS (26)

Figur 4 viser arkitekturen til smartkortet som brukes for autentisering mot MinJournal. Det er et Hitachi-kort med MULTOS (27) operativsystem.
Vi ser at ROM (Read Only Memory (28), kun lesbart ikke skrivbart) inneholder operativsystemet i kortet. EEPROM (Electronically Erasable Programmable ROM (29)) kan programmeres og slettes etter ønske. Det er her informasjonen om brukeridentitet, sertifikater og kontoopplysninger osv. lagres.

Vi går ikke mer i detalj om dette, men viser bildet for å sette litt perspektiv på hvor mye teknologi som er presset inn i den lille chip-en.

2.5.1.3 Kontaktløse smartkort

Smartkort uten elektriske kontaktpunkter er også utbredt. De bruker RFID (30) for kommunikasjon mot baser. De kan fungere innen cirka 10 – 50 cm fra en antenne, avhengig av korttype. Disse kortene er mye brukt i enkle betalingstjenester som tog- og t-banestasjoner og lignende. De fleste skisenter bruker også et kontaktløst smartkortsystem for tilgang til skiheiser.

2.5.1.4 Oppsummering

Smartkort lages som regel i plast og er derfor lette å bøye. Når de fleste også oppbevarer smartkortet i lommer, lommebok eller veske, kan de lett bli ødelagte. Jo større en chip er, desto lettere knekker den eller blir skadet. I systemer med mange brukere, som for eksempel banker, utgjør kostnadene for skader på smartkort allikevel mye mindre enn hva de sparer inn på en nedgang i antall svindler. Utenom fysiske problemer er smartkortene altså svært sikre. Det er nærmest umulig å få noe ut av dem uten den riktige PIN-koden. Man må også tenke på at helseforetak som tar i bruk MinJournal ikke har noe valg. Smartkort er det eneste valget når man må følge norsk lovverk på dette området. På den annen side er det dessverre ikke nok med bare smartkortet. Man trenger en større infrastruktur av servere og teknologier for å levere tjenester

som kryptert forbindelse og overføring av data. PKI og SSL er to sentrale teknologier vi skal forklare nærmere i de neste delkapitlene.

2.5.2 Public Key Infrastructure (PKI)

2.5.2.1 Hva er PKI?

PKI (31) er, som navnet tilsier, en samling eller infrastruktur av teknologier, prosesser og organisatoriske sikkerhetspolitikker. PKI støtter bruken av "public key cryptography" (32) og måter å verifisere ektheten av offentlige nøkler på.

Digitale sertifikater gir en kobling mellom systemer/servere, eller personer og deres offentlige nøkler. Disse sertifikatene signeres av såkalte Certificate Authorities (CA) (33). En CA er en offisiell sertifikatutsteder som deler ut sertifikater til sine kunder. Det finnes en rekke å velge mellom, og de fleste internettlesere inneholder en liste over hvilke toppnivå-CA-er man kan stole på.

Hvis man stoler på en CA så stoler man også på at sertifikatets medfølgende nøkkelpar (privat og offentlig krypteringsnøkkel) er ekte.

2.5.2.2 Hva menes med infrastruktur?

For at PKI i praksis skal fungere slik det er ment, må en kunne forsikre seg om at sertifikater/nøkler er ekte og nøklene tilhører at det sertifikatet det står at de gjør. Nøklene må heller ikke være merket som ugyldige. Figur 5 viser en oversikt over PKI- arkitekturen og hvordan de forskjellige partene henger sammen.

2.5.2.3 Hva brukes PKI til?

Alle som handler på nettet kommer borti PKI i en eller annen form. Når sensitive personlige opplysninger, som for eksempel kredittkortopplysninger, overføres via internett brukes PKI for å sikre forbindelsen mot avlytting.

2.5.2.4 Hvorfor PKI?

PKI er utviklet for å gi forbedret sikkerhet på internett. Det er et forsøk på å gjøre internett så sikkert at man kan utføre hverdagslige ting, som å betale regninger via en internettbasert bank-portal, istedenfor å møte opp personlig i banken. Det blir også mulig å handle i såkalte web-shopper, som er butikker på nettet.

2.5.2.5 Hvordan fungerer PKI?

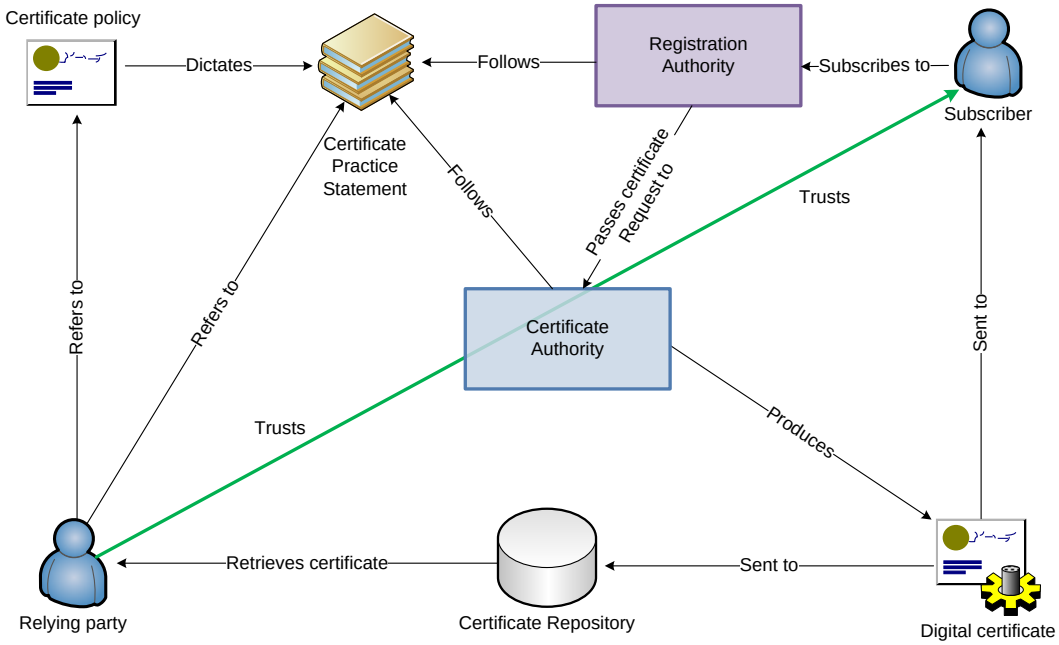
Det kan være vanskelig å få oversikt over hvordan PKI fungerer i praksis, og det er mange involverte elementer. Figur 5 viser et oversiktsbilde av hele PKI-arkitekturen. Forklaring til elementene følger.

"Certificate policy" er bedriftens interne sikkerhetspolitikk med hensyn til digitale sertifikater som igjen dikterer hvordan reglene og praksisen skal være ("Certificate practice statement").

"Registration Authority" (Registreringmyndighet) kan være en bedrift, som for eksempel Buypass. De produserer smartkort med innebygde PKI-sertifikater med signatur fra en CA ("Certificate Authority").

Når Buypass får inn en bestilling på et smartkort registreres brukeren i deres system og kortet produseres. En søknad sendes til en CA som gir kunden et sertifikat som lagres på smartkortet, som igjen er beskyttet med en PIN-kode. Sertifikatet lagres i en webserver kalt "Certificate Repository" slik at sertifikatet kan valideres mot denne ved bruk på internett.

"Relying party" er en bruker eller server som stoler på en CA, og "Subscriber" er sertifikatets eier.



Figur 5: Oversikt over PKI (34)

2.5.2.6 Teknologier i PKI

PKI er som nevnt en sammensetning av teknologier, prosesser og sikkerhetspolitikker. Teknologiene, og da spesielt sikkerhetsprotokollene som er brukt i PKI, er interessante for oss i dette prosjektet. En av de viktigste teknologiene som er brukt er SSL. En omfattende innføring følger.

2.5.3 Secure Socket Layer (SSL)

SSL (35) er en protokoll for sikring av overføringen av data på internett. MinJournal benytter SSL 3.0, som er siste versjon.

Etter en innføring i protokollen kommer det en mer teknisk del som også inneholder en beskrivelse av et velkjent angrep for å knekke protokollen.

2.5.3.1 Beskrivelse

SSL-protokollen lar applikasjoner kommunisere over internett på en måte som motvirker avlytting, endring og forfalskning av meldinger. Protokollen tilbyr autentisering og personvern over internett ved hjelp av kryptografi.

Vanligvis er det kun serveren som blir autentisert slik at klienten (internettleseren) vet at den kommuniserer med den rette. For at begge parter skal kunne autentisere hverandre må det benyttes PKI som beskrevet over.
SSL involverer tre steg:

- Utveksling av støttede algoritmer mellom parter som skal kommunisere.
- ”Public key”-basert utveksling og sertifikat-basert autentisering.
- ”Symmetric cipher”-basert (36) trafikk-kryptering.

2.5.3.2 ”Public key cipher”

”Public key”-basert kryptografi er enkelt forklart kryptografi basert på bruk av en privat nøkkel og en offentlig nøkkel. Den private nøkkelen er det bare du som kjenner, mens den offentlige er tilgjengelig for ”hvem som helst”.

Meldinger som krypteres med den private nøkkelen kan kun dekrypteres med den offentlige nøkkelen. Dermed kan meldingens opphav påvises.

I motsatt tilfelle, der meldingen krypteres med den offentlige nøkkelen, er det bare eieren av den private nøkkelen som kan dekryptere innholdet. Dermed er meldingen sikret slik at ingen andre enn akkurat eieren kan åpne den.

2.5.3.3 "Symmetric key cipher"

"Symmetric cipher" er et prinsipp som betyr at to parter som kommuniserer deler på en "hemmelighet" i form av en felles krypteringsnøkkel. Denne brukes for kryptering av meldinger som utveksles. Nøklene er som regel like, men det vil i noen tilfeller være en triviell forskjell som kun innebærer en enkel transformering av nøkkelen.

Det finnes flere forskjellige krypteringsalgoritmer som kan brukes ifølge SSL-protokollen. De varierer i styrke og effektivitet alt etter hva bruksområdet er. Dette er ofte forvalgt av serveren, slik at klienten eller brukeren ikke trenger å gjøre slike avanserte valg.

2.5.3.4 SSL i praksis

Sikker kommunikasjon med en SSL-aktivert server er i praksis enkelt for en bruker. Se Figur 6.

Punkt 1: Et firma må be om å få utstedt sertifikater til sine servere. Det blir da registrert nødvendig informasjon som navn, adresse, kontaktinformasjon osv.
De fleste seriøse CA-er sjekker også om opplysningene stemmer og at firmaet er seriøst. I tillegg til dette genereres det krypteringsnøkler til bruk for sikker kommunikasjon.

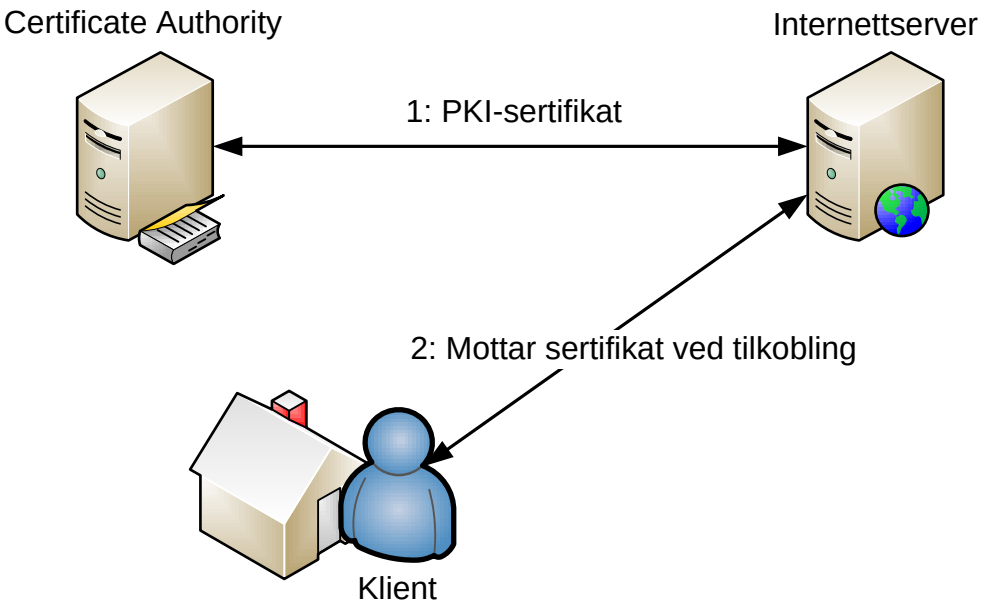
Punkt 2: Brukeren/klienten prøver å koble til internettserveren. Klienten får da beskjed om at det kreves en sikker tilkobling og vil motta et sikkerhetssertifikat fra serveren. Man kan da velge å stole på utsteder og serveren eller ikke. Hvis man velger å stole på sertifikatets ekthet settes forbindelsen opp, og kommunikasjonen mellom partene kan foregå som en hvilken som helst server-klient-forbindelse. Forskjellen fra"normalt" er da at forbindelsen sikres med ("symmetric key") kryptering.

2.5.4 SSL og MinJournal

MinJournal bruker som nevnt SSL 3.0. For nøkkelutveksling og autentisering brukes krypteringsnøklene i sertifikatet til serveren og klienten. MinJournal-serveren har et 2048-bits nøkkelpar, mens Buypass-smartkortet har et par på 1024 bits. Dataforbindelsen krypteres med en 128 bits "symmetric key".

2.5.5 SSL angrepsscenario

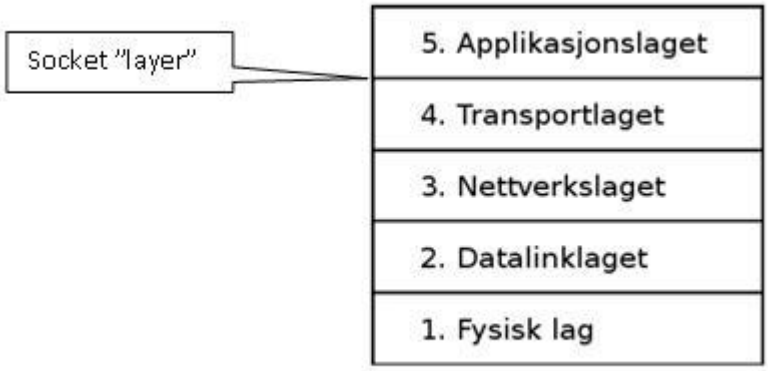
Vi vil prøve å beskrive en metode for å "knekke" SSL-protokollen slik at forbindelser kan avlyttes og meldinger forfalskes, eller rett og slett fjernes. Først går vi litt mer i detalj i protokollen for at angrepet skal kunne forstås. Dette delkapittelet er mer teknisk detaljert og anbefales for de som har tilstrekkelig teknisk innsikt.



Figur 6: SSL i praksis

2.5.5.1 Teknisk beskrivelse av SSL

SSL opererer på "socket-laget" som ligger mellom applikasjonslaget og transportlaget i TCP/IP-stakken (Transmission Control Protocol (37)/ Internet Protocol (38)). Dette kommer fram på figuren under.



Figur 7: Socket laget i TCP/IP-stakken

2.5.5.2 SSL forbindelse

Nedenfor går vi gjennom en litt forenklet SSL forbindelse mellom to parter, Alice og Bob.

Vi bruker disse forkortelsene i meldingene mellom partene:

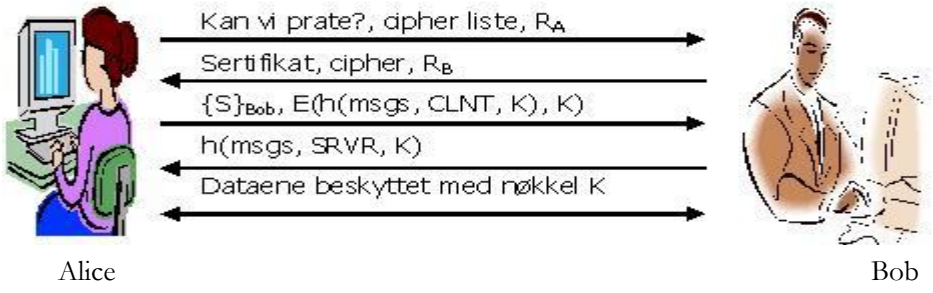
- S = "pre-master hemmelighet"
- K = h(S, R_A, R_B), hvor h er hash funksjonen
- msgs = alle tidligere meldinger
- CLNT = nøyaktig streng
- SRVR = nøyaktig streng

I den første meldingen sier Alice at hun vil opprette en SSL-forbindelse, og sender en cipher-liste som Alice har støtte for, samt en nonce (39) R_A. Nonce står for "number used once" og er en utfordring som bare kan bli brukt én gang. En nonce er altså en unik utfordring som sikrer at responsen er "fersk", noe som forhindrer et såkalt replay attack. Ufordringen her er fra Alice til Bob, og responsen fra Bob er en respons som kun Bob kan lage og som Alice kan verifisere.

I neste melding, fra Bob til Alice, svarer Bob med hans sertifikat. Han velger et cipher fra cipher listen Alice sendte, og sender en utfordring, R_B, tilbake til Alice.

I den tredje meldingen sender Alice "pre-master hemmelighet" S som hun genererte, sammen med en hash som er kryptert med en nøkkel K. Denne hashen inkluderer msgs, som er alle tidligere beskjeder, og CLNT som er en nøyaktig streng. Hashen blir brukt for å verifisere at alle tidligere beskjeder har blitt mottatt korrekt. Bob svarer med en lignende hash i den fjerde meldingen. Alice kan da bekrefte at Bob har mottatt beskjedene korrekt og ikke minst kan Alice autentisere Bob, siden han er den eneste som kan ha dekryptert S. Dekryptering av S er påkrevd for å generere nøkkelen K.

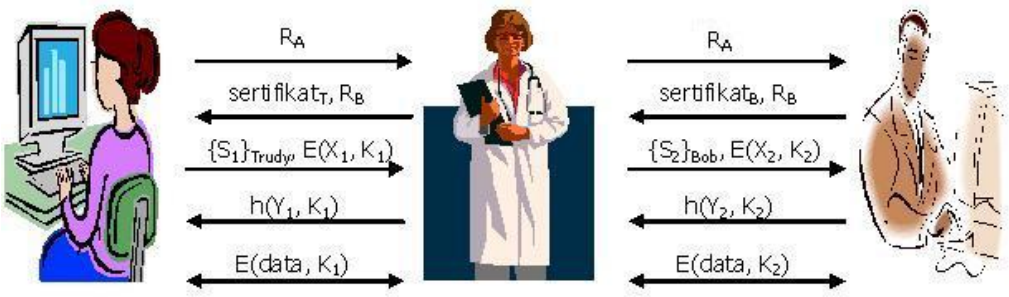
Etter disse fire meldingene har Alice autentisert Bob og de har en felles symmetrisk nøkkel K. Denne nøkkelen kan de bruke til å kryptere og sikre integriteten på kommende meldinger dem imellom.



Figur 8: SSL forbindelse

2.5.5.3 Angrepsmetoden

SSL er utsatt for Man-in-the-Middle-attack (40), selv om SSL er designet for å beskytte mot slike angrep. Poenget her er, som navnet tilsier, at angriperen skal være en mellommann som sitter og mottar og videresender meldingene mellom de to opprinnelige partene. Figur 9 illustrerer angrepet. Trudy lurer Alice til å tro at hun er Bob, og Bob til å tro at hun er Alice. Dette gjøres ved å sende dem forfalskede sertifikater.



Figur 9: "Man-in-the-Middle"-angrep

Ved at Bob sitt sertifikat blir signert av en CA, som for eksempel VeriSign (41), er han sikret mot slike angrep. Da kan ikke Trudy autentisere seg selv som Bob, og om Trudy sender sitt eget sertifikat vil angrepet mislykkes når Alice prøver å verifisere signaturen på sertifikatet.

Men når SSL brukes mellom server og webleser (klient), noe som er vanlig, vil det bare komme en meldingsboks med en advarsel i Alices webleser. Og hva gjør Alice og den vanlige bruker da? Jo, de aller fleste vil ignorere denne advarselen, og da er angrepet til Trudy vellykket.

2.5.6 Oppsummering

Internett er et usikkert medium og internettkriminalitet blir stadig mer utbredt. Det er derfor viktig og nødvendig å ha en tilfredsstillende sikkerhet tilknyttet internettløsninger som MinJournal. MinJournal har innebygget sikkerhetsteknologi som skal sikre konfidensialitet, integritet og tilgjengelighet. Dette har de gjort ved å bruke flere løsninger; Buypass-smartkort med PIN-kode for å logge seg på, samt at all kommunikasjon er kryptert ved bruk av SSL. Vi har gjennomgått disse forskjellige teknologiene, og beskrevet sårbarheter ved disse, for at leseren skal få et innblikk i begrepene og forstå at ingen løsninger er uten sårbarheter.

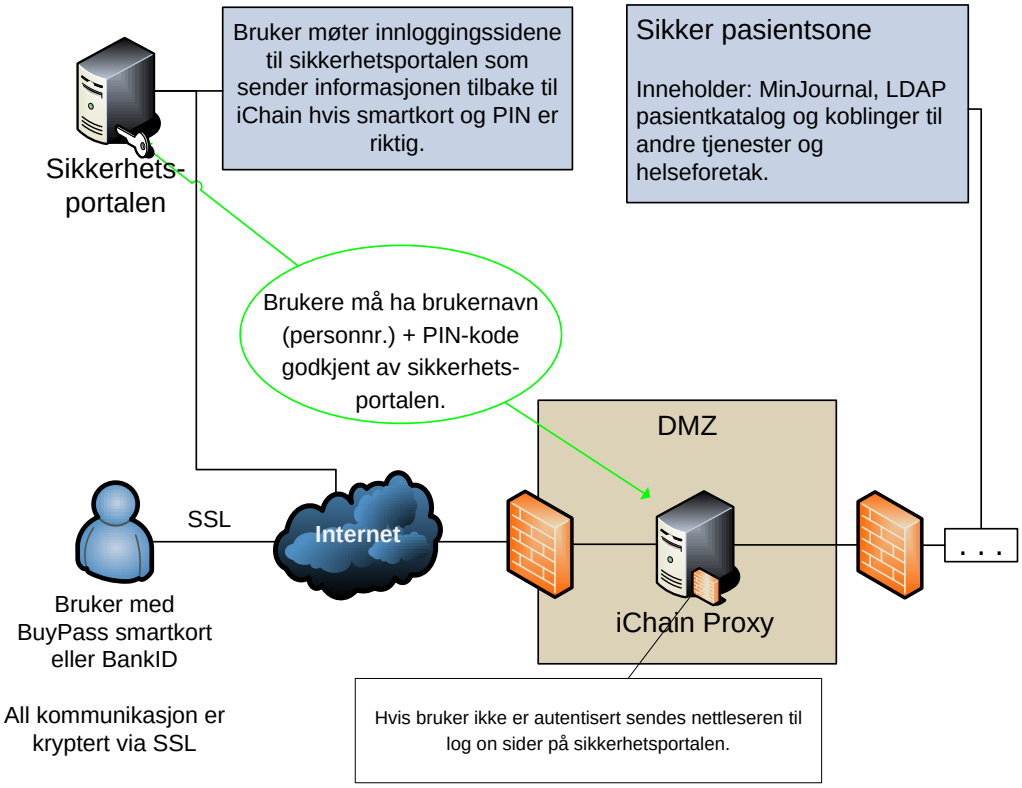
3 Relevant arbeid

Vårt prosjekt er å bistå i implementeringen av MinJournal, og det er da først og fremst hensiktsmessig å sette seg inn i hvordan MinJournal har blitt implementert i andre helseinstitusjoner. Vi har også sett på et lignende system, "minTRSSIDe", som har blitt utviklet for Sunnaas og implementert for Sunnaas TRS.

Til slutt settes minTRSSIDe opp mot MinJournal og fordeler og ulemper ved begge løsningene beskrives.

3.1 MinJournal

I dette kapittelet beskrives innholdet og tjenestene i MinJournal.



Figur 10: Teknisk oversikt over strukturen rundt MinJournal (42)

Figur 10, over, viser en litt forenklet oversikt over strukturen rundt MinJournal. LDAP (Lighweight Directory Access Protocol (43)) er en protokoll for kommunikasjon med katalogtjenester (Directory services (44)). I dette tilfellet brukes den til å hente informasjon om pasienter fra pasientkatalogen. Informasjonen passerer gjennom DMZ (De-Militarized Zone (45)), som brukes for å lage et sikkert skille mellom det interne nettverket og internett.

3.1.1 Sikkerhetsnivåer

MinJournal er delt i to soner/sikkerhetsnivåer; Åpen og PKI-beskyttet.
De åpne sidene er tilgjengelige for alle og er uten noen form for beskyttelse. Sidene har samme utforming som de PKI-beskyttede, men viser ingen personlig informasjon.

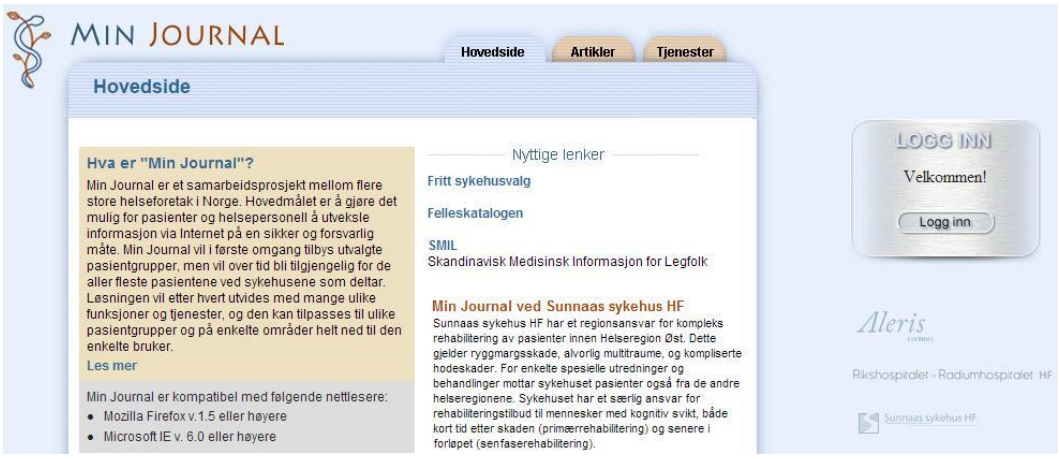
De PKI-beskyttede sidene krever at man logger inn med et smartkort fra Buypass (med sterk autentisering/personsikkerhet høy-gradering). PKI-sertifikatet på smartkortet inneholder en 1024 bits public key.

Gruppetilgang

"Det finnes 2 typer grupper i MinJournal:

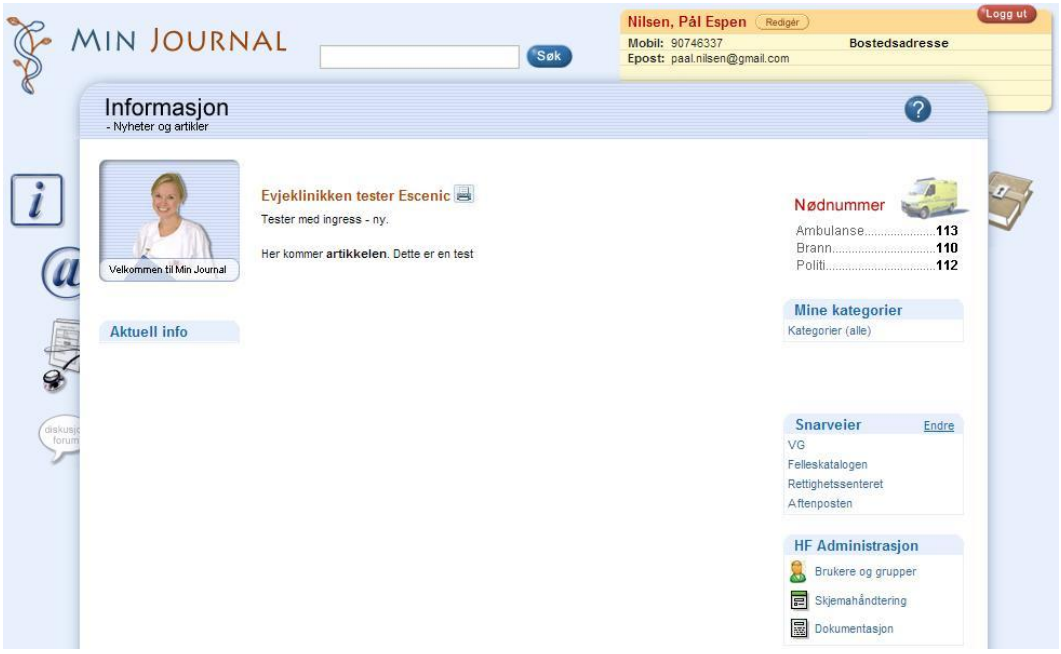
> ***HF** – grupperer flere pasienter og helsepersonell innenfor en helsefaglig enhet. Gruppene kan ha flere funksjoner slik som adgangskontroll, e-postgrupper, abonnement på interesseområde med flere. Gruppen defineres av en administrator tilknyttet det enkelte HF.*
>
> ***MR** – grupperer flere pasienter og helsepersonell på tvers av HF'ene. Gruppene navngis med MR_gruppenavn. Gruppene vises som seksjoner i Escenic for de innholdsadministratorene som er medlem av gruppen - på tvers av HF'ene (Samme innhold kan vises til brukere av MinJournal på tvers av HF)."* (46)

3.1.2 Forside



Figur 11: MinJournal forside (ikke innlogget)

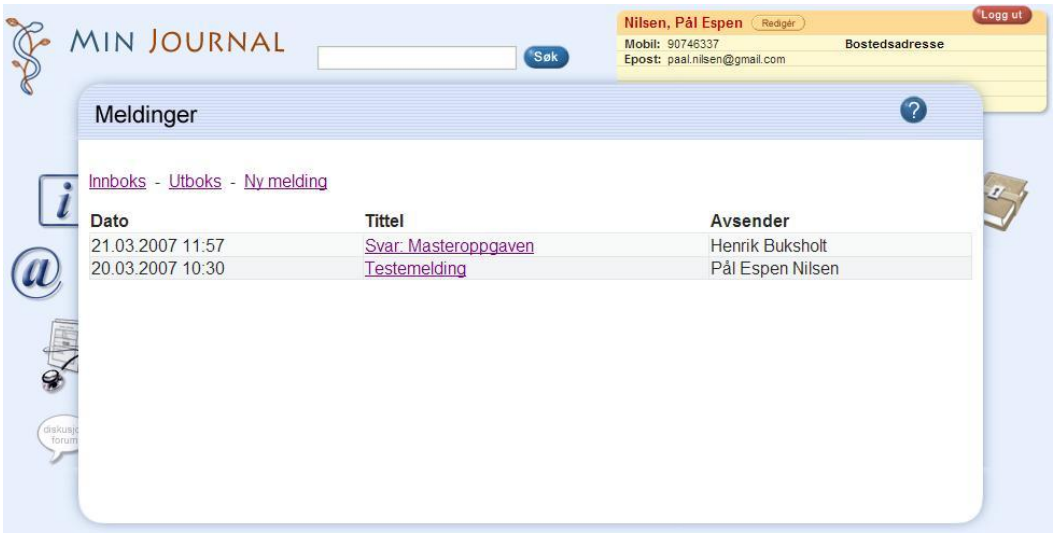
Figur 11 viser forsiden til MinJournal før innlogging. Det vises kun offentlig informasjon om prosjektet og noen relevante artikler som er publisert. Til høyre vises knappen for innlogging.



Figur 12: MinJournal forside (innlogget)

Figur 12 viser forsiden etter innlogging. Navn og registrerte personalia vises øverst til høyre, og menyen til venstre. Nede til høyre ser man de tre kategoriene under HF Administrasjon som skiller superbrukere fra vanlige brukere. Dagboken er representert med et bok-ikon til høyre.

3.1.3 Meldinger



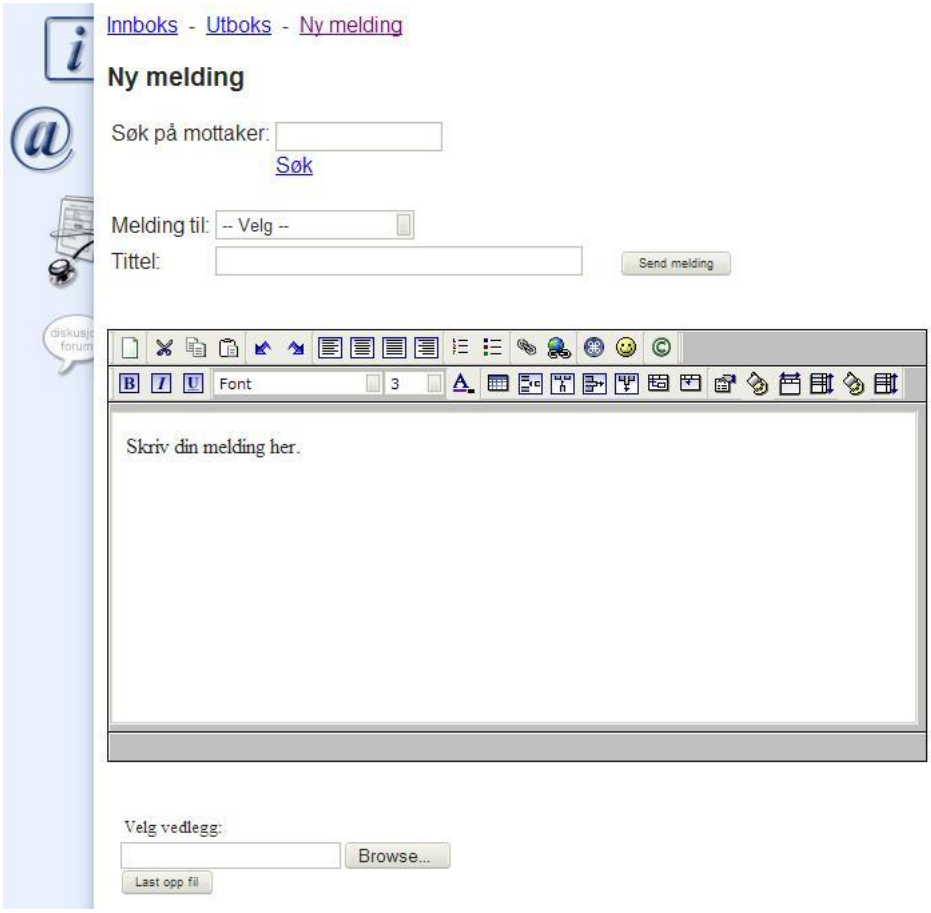
Figur 13: Meldingstjenesten

Figur 13 viser den innebygde meldingstjenesten. Her vises innboksen med et par meldinger. Det hele fungerer som et forenklet e-post-program.

Tjenesten baserer seg på grupper. Pasienter kan sende meldinger kun til spesifiserte mottakere. Dette avgjøres av hvilken tilgangsgruppe pasienten er medlem av. Administrator kan legge til flere mottakere.

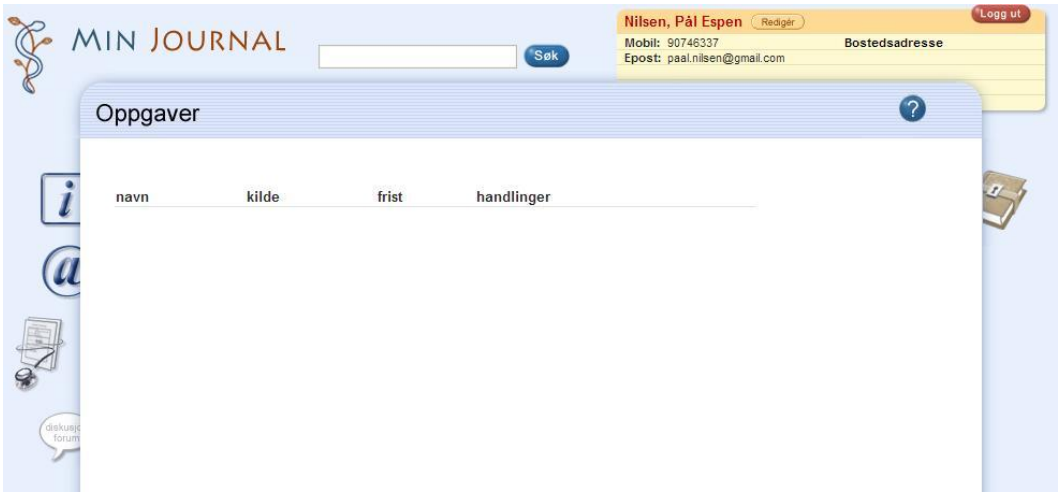
Helsepersonell kan sende meldinger til alt av helsepersonell og pasienter som er medlem i deres tilgangsgruppe.

Tekstredigereren for meldinger har i tillegg de mest nødvendige funksjoner for formatering av tekst og tabeller etc. (Se Figur 14.)



Figur 14: Meldingstjenesten, ny melding

3.1.4 Elektroniske skjema

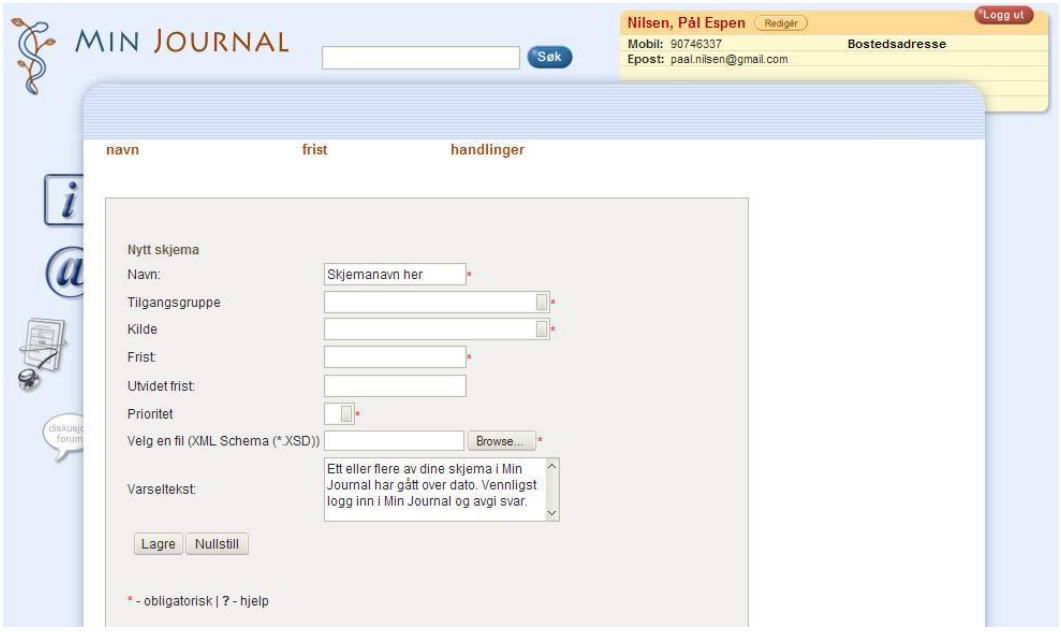


Figur 15: Oppgaver

Figur 15 viser en oversikt over gjeldende oppgaver. Her ligger skjemaene som helsepersonell laster opp. Det registreres en frist ved opplasting av disse skjemaene (se Figur 16). Det betyr at skjemaene må fylles ut innen den datoen (frist i Figur 15).

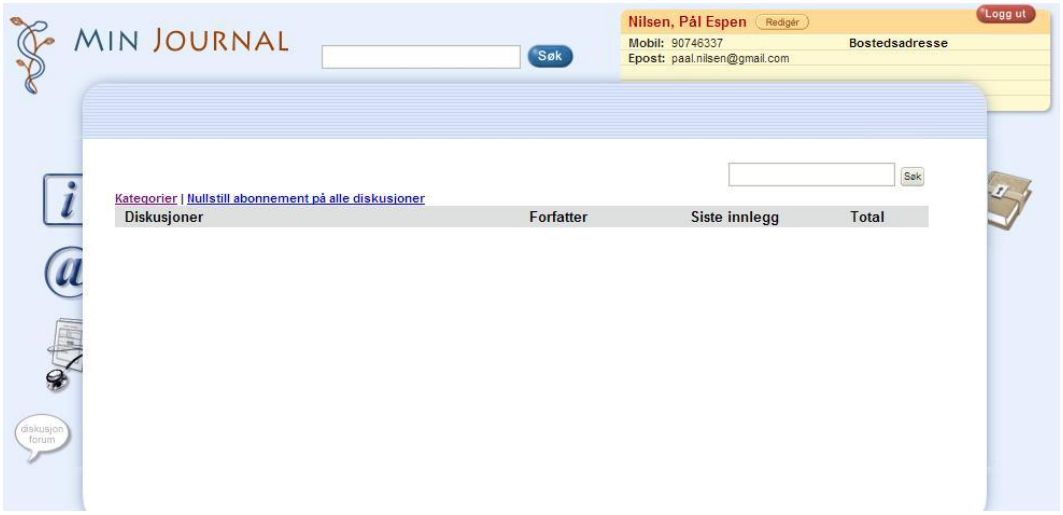
Hvis en trykker på "Se innleverte skjema" kommer det opp en liste over skjemaer som er levert tidligere, med dato og tidspunkt for levering, og en kan trykke på linken for å se på dem.

Under (Figur 16) vises opplastningssiden for skjemaer. Denne er det kun administratorer og helsepersonell med tilstrekkelige rettigheter som kan benytte.



Figur 16: Skjemahåndtering

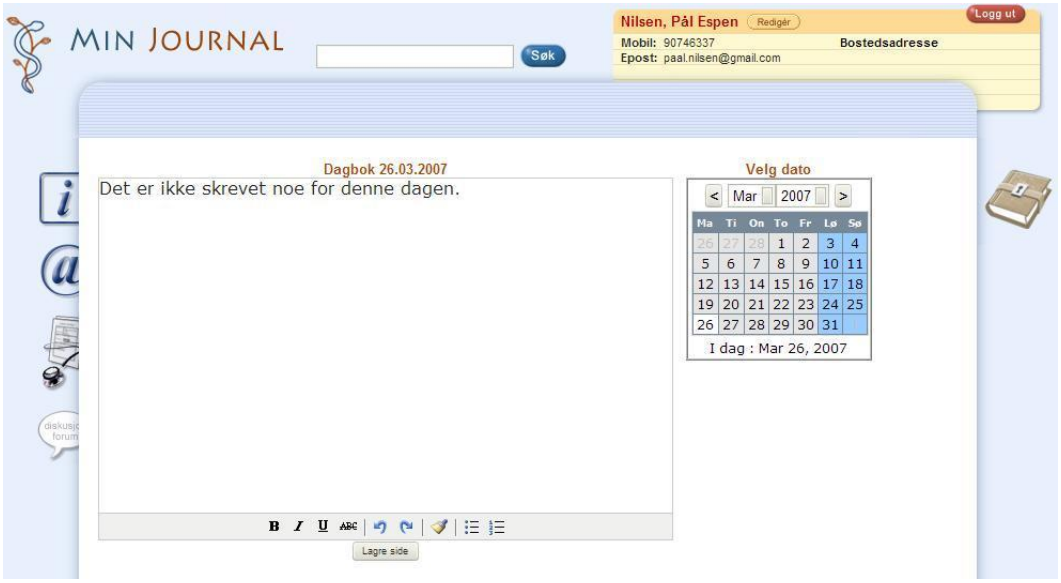
3.1.5 Diskusjonsforum



Figur 17: Diskusjonsforum

Figur 17 viser det innebygde diskusjonsforumet. Her kan både helsepersonell og pasienter opprette og besvare tråder og innlegg. Forumet er i skrivende stund ikke operativt.

3.1.6 Dagbok



Figur 18: Dagbok

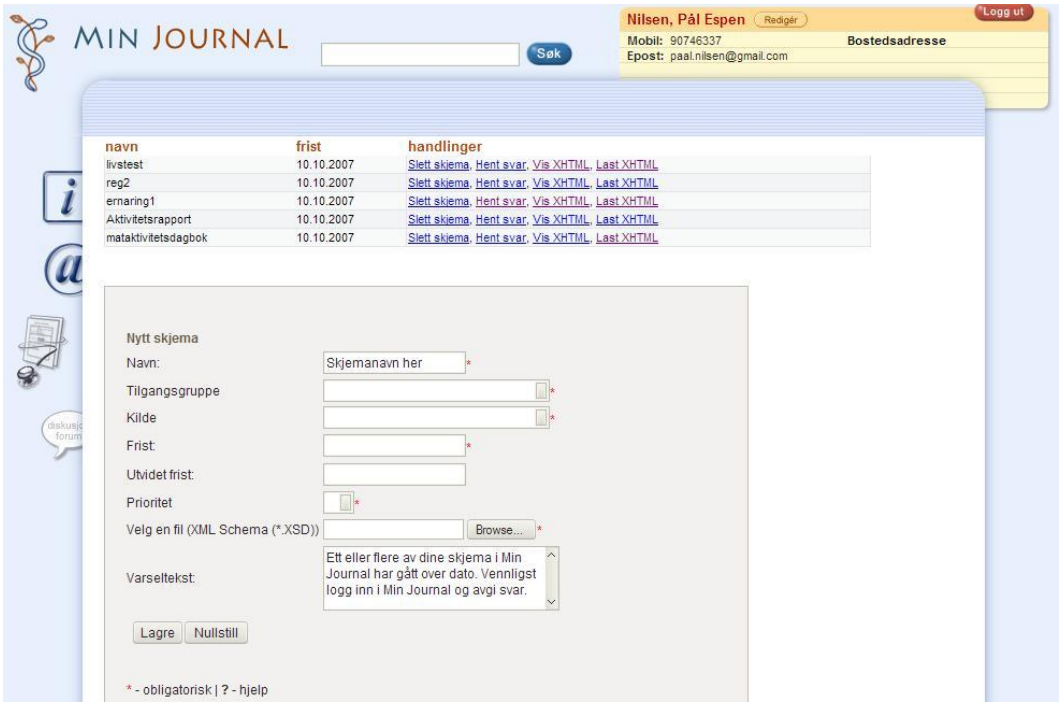
MinJournal har en enkel dagbokfunksjon der man enkelt skriver inn teksten man vil og trykker "lagre side". Teksten lagres i portalen og vises på kalenderen med uthevet/fet skrift.

3.1.7 Snarveier

Det kan opprettes snarveier på forsiden (innlogget) (se Figur 12) av MinJournal. Pasienter kan opprette sine egne snarveier, mens helsepersonell kan opprette snarveier etter tilgangsgruppe eller kategorigruppe. Disse kan vises som standard, være obligatoriske (vises alltid) eller være valgfrie slik at pasienten selv velger om de skal vises eller ikke.

3.1.8 Administrasjon

Administratorer for klinikker har muligheten til å opprette brukere og grupper. De kan sette gruppetilhørighet for brukere innad i klinikken, samt laste opp og redigere skjemaer for brukerne.



Figur 19: Skjemaadministrering

Figur 19 viser det samme som Figur 16, men med noen av våre test-skjemaer (livstest, reg2, ernaring1 …) opplastet i tillegg. Som vist på bildet ser man at man kan slette skjemaet, vise innleverte skjemaer fra brukere (”hent svar”), vise XHTML, eller laste opp redigert XHTML.

Prosessen fra man laster opp skjemaet (.xsd-filen) til det ferdige skjemaet vises, som klinikken ønsker, er forklart nærmere under kapittel 4.

3.2 MinTRSSIDe

I denne delen gjennomgås relevant arbeid med hensyn til eksisterende elektroniske pasientjournal-løsninger. Dette vil omhandle Sunnaas sykehus TRS' web-portal minTRSSIDe. Vi går ikke i detalj om systemet, men prøver å gi en innføring i hva som er gjort og hvordan systemet fungerer.

3.2.1 Om Sunnaas TRS

"TRS er et landsdekkende kompetansesenter for syv sjeldne, medfødte diagnosegrupper. Senteret er en del av Sunnaas sykehus HF i Helse Øst RHF og ligger på Nesodden utenfor Oslo. …" (47)

3.2.2 Om minTRSSIDe

minTRSSIDe er Sunnaas TRS sin nye webportal. Den ble utviklet i samarbeid med ITVerket AS.

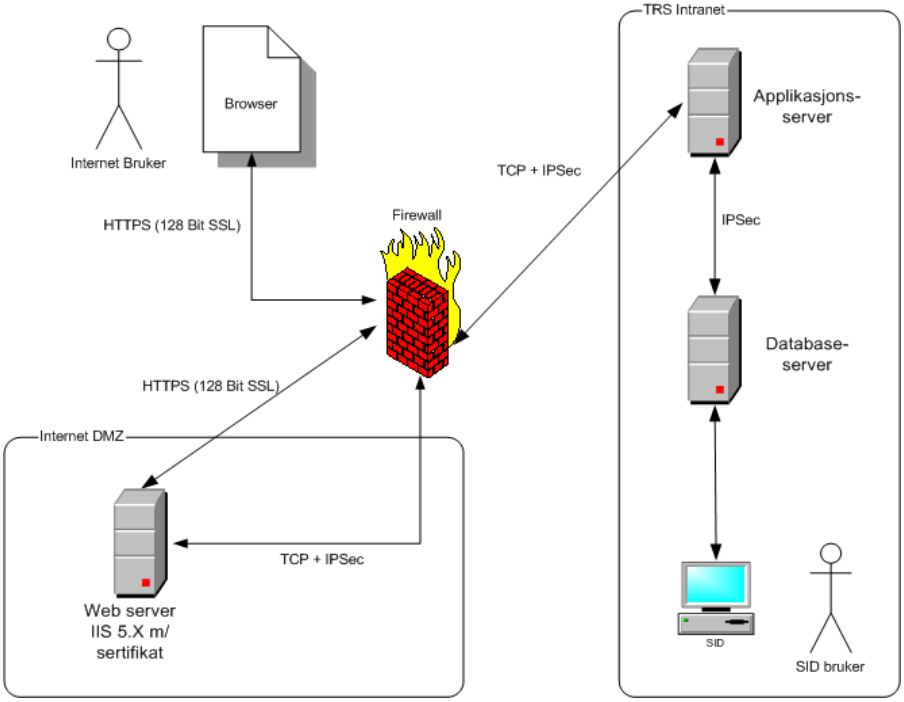
"… Den gjør det mulig for registrerte brukere å kommunisere effektivt med TRS via sikker e-post, lese egne journalopplysninger og oppdatere egne personalia på siden.

Webportalen er en unik løsning utviklet for TRS kompetansesenter. minTRSSIDe gjør det mulig å kommunisere elektronisk med fagpersoner på TRS på en trygg måte om sensitive forhold knyttet til egen helse. ..." (48)

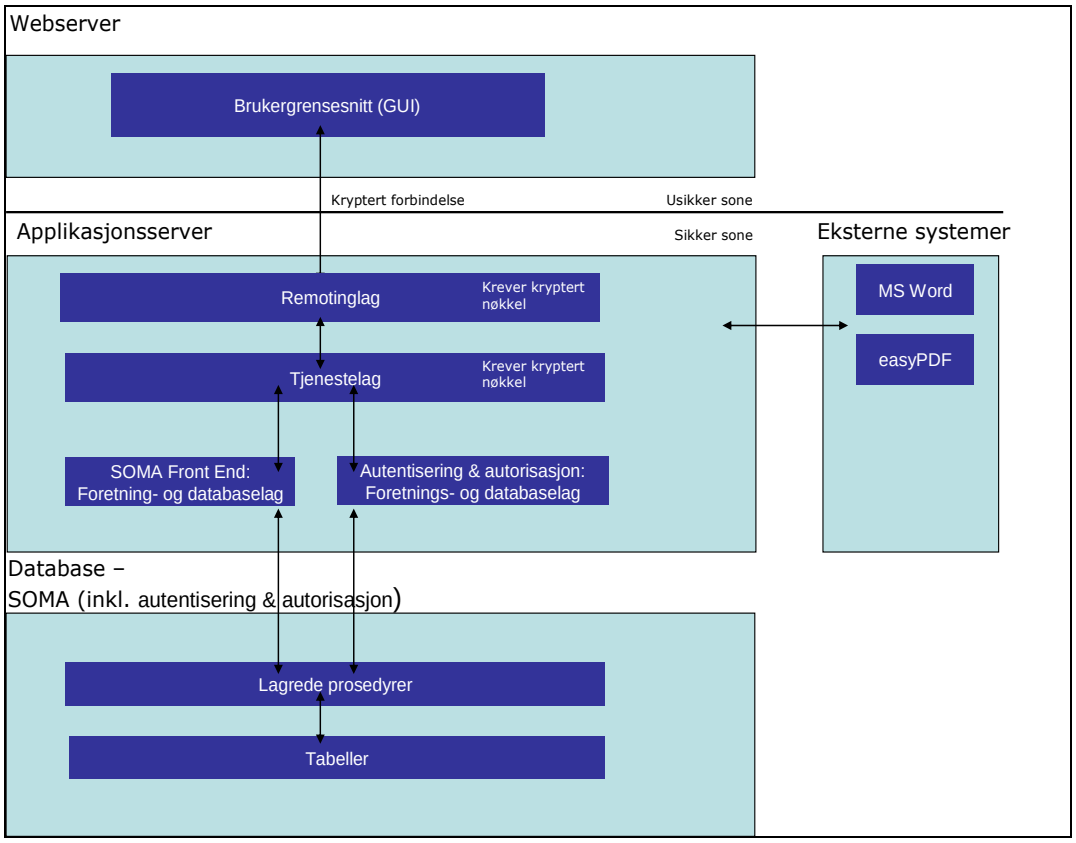
De ansatte ved Sunnaas TRS bruker et program som heter SID for å få tilgang til lesing og skriving i databasen. Dette inkluderer pasientjournaler og administrasjon av hva den enkelte skal få se av informasjon på sin minTRSSIDe.

3.2.3 Teknisk oversikt

Følgende to figurer (Figur 20 og Figur 21) viser hvordan systemet er lagt opp med hensyn til nettverk og applikasjoner. Her ser vi at IPSec brukes mellom de forskjellige serverne. IPSec (Internet Protocol Security (49)) brukes for å opprette en kryptert forbindelse som er svært sikker.



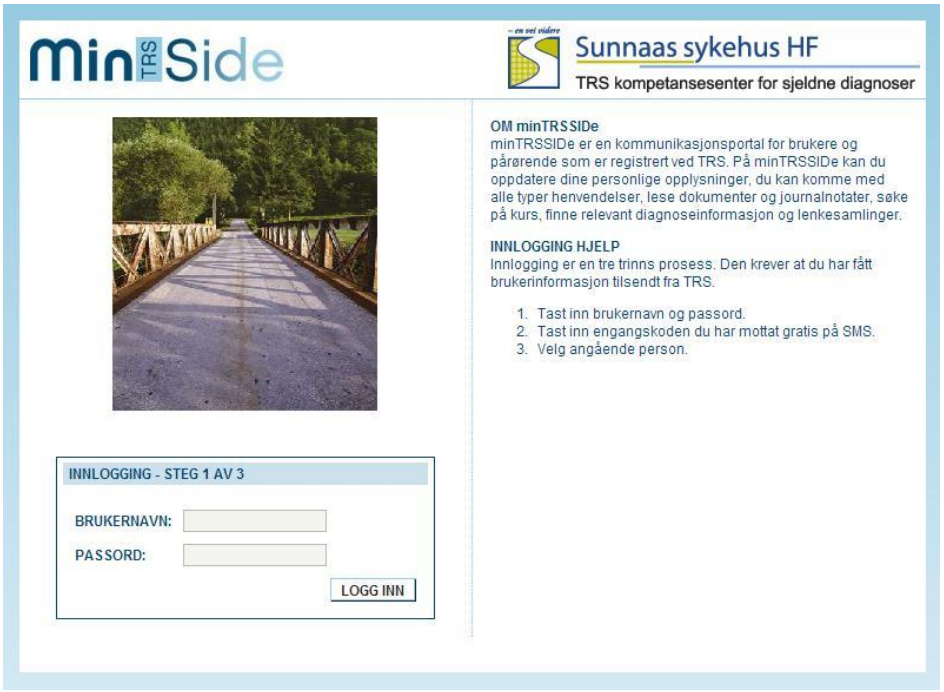
Figur 20: Overordnet nettverksarkitektur (50)



Figur 21: Overordnet applikasjonsarkitektur (50)

3.2.4 Web-portal

Web-portalen er det pasienten, eller den såkalte kunden, forholder seg til. Figur 22 viser hvordan innloggingssiden ser ut. Kundene må først registreres med et brukernavn, passord og personalia inkludert mobiltelefonnummer. Når de så logger seg inn med brukernavn og passord blir det sendt en engangskode til det registrerte mobilnummeret. Dette er for å sikre at ikke uvedkommende får tilgang til den personlige websiden. Mer om dette under "Sikkerhetsmekanismer"(kapittel 3.2.5).



Figur 22: minTRSSIDe, innloggingsside

Figur 23 viser hvordan forsiden ser ut. Øverste linje i vinduet viser navnet på personen som er logget inn og hvem siden angår ("angående:"). Menyen til venstre brukes for å navigere på websiden.

Figur 23: minTRSSIDe, webportalens forside (51)

Beskrivelse av menyelementer i Figur 23:

- "Personalia" brukes for å se hvilke opplysninger som er registrert på deg og for å endre disse.
- "Sikker e-post" brukes for å kommunisere med Sunnaas TRS personell.
- "Dokumenter" viser dokumenter som er tilgjengelig for gjennomsyn.
- "Kurs" viser deg hvilke kurs som er tilgjengelige og gir deg mulighetene for å sende en søknad fra websiden.
- "Logg" viser alle hendelsene i portalen.
- "Tilgang" lar deg administrere hvem og hva det skal gis tilgang til i portalen.

3.2.5 Sikkerhetsmekanismer

ITVerket AS og Sunnaas sykehus TRS har vært i dialog med Datatilsynet for å klare å lage et brukervennlig system og lovlig system. Dette systemet må følge alle gjeldende lover og regler med hensyn til behandling av sensitiv informasjon. Man må ta hensyn til både lagring og overføring av journaler/opplysninger mellom ansatte, samt overføringen av personopplysninger over usikre medier, som internett.

Det første som skjer er at kundene må registreres med full personalia, inkludert gyldig personlig mobilnummer og et brukernavn og passord.

3.2.6 Sikring av innlogging til web-portalen

Når kunden åpner innloggingssiden til minTRSSIDe sikres forbindelsen med SSL og en 128 bits krypteringsnøkkel. Man logger videre inn med brukernavn og passord. minTRSSIDe-systemet sender så en sms med en engangskode som er gyldig i ti minutter. Denne må tastes inn for å få tilgang til den personlige siden.

3.2.7 Sikring av underliggende nettverk og applikasjoner

Det brukes flere forskjellige mekanismer for å sikre systemet:

- SSL-sertifikat
- Kryptert TCP forbindelse
- Caching
- Autentisering og autorisasjon (beskrevet over)
- Uleselig kode

Mellom bruker/webleser og webserver brukes det et SSL-sertifikat med 128 bits krypteringsnøkkel. Dette autentiserer serveren slik at brukeren er sikker på at han kobler til korrekt server. Webserveren kommuniserer videre med applikasjonsserveren via en kryptert TCP-forbindelse for å sikre mot nettverksavlytting.

Alle websider inneholder kode som deaktiverer caching (mellomlagring) slik at navigasjonstastene (frem og tilbake) i webleseren ikke vil fungere.

For å unngå utnytting av dette brukes teknikker for å gjøre koden svært vanskelig å lese.

Disse tiltakene for sikring av webportal og underliggende systemer og applikasjoner, er gjort i forsøk på å følge Datatilsynets anbefalinger og samtidig gjøre systemet brukervennlig nok for sine kunder. Ifølge prosjektleder for MinJournal og sikkerhetsrådgiver ved Rikshospitalet – Radiumhospitalet HF, er disse tiltakene kanskje ikke nok for å tilfredsstille gjeldende lovverk. Vi vil ikke konkludere med noe i hverken den ene eller den andre retningen i denne rapporten.

3.3 Sammenligning av MinJournal og minTRSSIDe

I dette kapittelet ser vi på fordeler og ulemper med begge løsningene, og sammenligner dem til den grad det er mulig.

3.3.1 Innloggingsløsning

minTRSSIDe ble utviklet med tanke på at noen av kundene har konsentrasjonsproblemer, og derfor trenger en enkel løsning for innlogging og informasjonsflyt. Innloggingsløsningen til minTRSSIDe er relativt enkel. Den har den fordelen at den ikke krever noen installasjon, kun en personlig mobiltelefon for mottak av engangskode. Vi fikk kommentarer fra Sunnaas TRS om at den i noen tilfeller allikevel ikke var enkel nok. Noen av kundene hadde problemer med å skrive inn koden de mottok i SMS-meldingen.

MinJournals løsning er mer omfattende å installere, ettersom man må ha en kortleser og tilhørende drivere og programvare før man kan ta i bruk smartkortet. Sertifikatet må importeres til internettleseren, men dette gjøres bare første gang. Dette vil man kunne guide brukeren til å gjøre, for eksempel over telefon, eller man kan få en tekniker til å gjøre det for vedkommende. Etter installasjonen er gjennomført er det bare å åpne http://www.minjournal.no, trykke på logg inn og taste inn den personlige PIN-koden i vinduet som kommer opp på skjermen.

Løsningene er altså i bunn og grunn forskjellige. Fra pasientens ståsted kan derimot løsningene oppleves like i praksis, ettersom man i begge tilfeller må skrive inn en kode for å logge inn. Om den ene eller den andre løsningen har en fordel eller ikke er vanskelig å si. Det er tross alt stor forskjell på brukerne av løsningene. En innloggingsløsning som ikke krever noen form for kode eller passord ville i de fleste tilfeller være å foretrekke.

Man kunne implementert en løsning med fingeravtrykkleser eller lignende, men det vil igjen medføre enda høyere utgifter til både utstyr og brukerstøtte. Kompatibilitet med eksisterende programvare etc. kan også være et potensielt problem.

Fordelen med minTRSSIDe på dette området er at en som regel har mobiltelefonen tilgjengelig hvor enn en går, og derfor kan bruke løsningen der det finnes en PC med internettilkobling.

Dette er vanskeligere med MinJournal ettersom det mest sannsynlig ikke finnes en smartkortleser installert på den samme tilfeldige PC-en med internettkobling.

Hvis vi på den annen side skal konkludere på bakgrunn av informasjonssikkerheten, er MinJournal den løsningen som oppfyller kravene til sikring av forbindelser for overføring av pasientopplysninger (personsikkerhet høy). minTRSSIDe oppfyller kanskje ikke disse kravene.

3.3.2 Sikring av innlogging og dataoverføring

Det er visse krav til å overføre pasientopplysninger over internett. Forbindelsen må krypteres og innlogging/autentisering må være på nivå "personsikkerhet høy".

Antakeligvis oppfyller ikke minTRSSIDe kravene til innloggingsløsningen, men bruker i likhet med MinJournal SSL for sikring og kryptering av forbindelsen.

MinJournal-serveren benytter et PKI-sertifikat med et 2048 bits nøkkelpar, mens Buypass-smartkortet som brukerne benytter inneholder et 1024 bits nøkkelpar. Forbindelsen mellom klient og server sikres med RC4 krypteringsalgoritme (52) med en 128 bits nøkkel.

Til gjengjeld bruker minTRSSIDe kun 128 bits nøkler i sertifikat på serveren og ikke noen personlige klientsertifikater, mens forbindelsen sikres med RC2 algoritme (53) med 64 bits nøkkellengde. Denne løsningen er ikke dårlig, og er kanskje også tilstrekkelig, men sikringen av informasjonen legger seg på et nivå som er vesentlig lavere enn MinJournal's.

Drøfting av sikkerhetsløsningene i MinJournal finnes i kapittel 5.7.

3.3.3 Grafisk grensesnitt og brukervennlighet

En av de første tingene vi fikk beskjed om fra Rikshospitalet – Radiumhospitalet HF var at utseendet til MinJournal har lavere prioritet enn selve system– og funksjonsutviklingen. Løsningen er fortsatt under utvikling, så det grafiske grensesnittet fungerer derfor ikke helt optimalt. Brukervennligheten er i skrivende stund ikke bedre enn absolutt nødvendig. Menyene er lite gjennomførte og trenger en oppussing. Spesielt med tanke på å gjøre det klarere hvilke ikoner som fører til hva. Det skal dog nevnes at løsningen fortsatt er under utvikling.

På det samme området er minTRSSIDe mye bedre, men dette er en ferdig utviklet løsning. En del av filosofien til Sunnaas TRS, når de skulle utvikle løsningen, var at brukeren står i sentrum. Etter vår mening kan sidene til tider virke litt kaotiske og overfylte med informasjon. En gjennomsnittsbruker vil kanskje ha problemer med å navigere, men tilbakemeldingene fra brukerne har, ifølge Sunnaas, vært gode.

3.3.4 Integrasjon med andre løsninger

MinJournal er foreløpig et frittstående system uten noen integrasjon med andre løsninger. Det finnes ingen muligheter for å lese eller skrive informasjon til/fra pasientjournaler, slik som de fleste klinikker (inkludert Evjeklinikken) bruker på sitt interne nettverk.

Det finnes allikevel en måte å gjøre dette på, men i en forenklet form; Innsendte svar fra skjemaer lagres som .xml-filer, og kan tolkes eller "oversettes" slik at dataene automatisk kan legges inn i journalene til Evjeklinikken. Dette er heller ikke implementert ennå.

Til sammenligning er minTRSSIDe 100 % integrert med journalsystemet (SID) hos Sunnaas TRS. Det betyr at alle data som vises på minTRSSIDe hentes fra den enkelte pasients journal, og dataene som endres ved hjelp av minTRSSIDe lagres i journalen. Dette er en stor fordel i Sunnaas TRS' favør.

4 Vårt arbeid og resultater

I dette kapitlet skal vi gå gjennom prosessen vår og det arbeidet vi har gjort med oppgaven. Dette innebærer blant annet å vise resultater fra skjemautvikling og meldingstjeneste samt beskrive prosess- og dokumentflyten ved Evjeklinikken etter implementering.

4.1 Introduksjon til utviklingen

Ved all skjemautvikling har vi brukt verktøyet Altova XMLSpy 2007. Dette er et verktøy som innehar alle egenskapene vi så som nødvendige, samt at det er brukervennlig. Vi har også brukt XMLSpy 2007 til å redigere den genererte XHTML-koden.

For å få et tilfredsstillende utseende på skjemaene har vi brukt verktøyet Macromedia Dreamweaver 8. Dreamweaver har vi brukt til å redigere det opprinnelige stilarket på MinJournal ved å legge inn nye stilklasser for Evjeklinikken. Vi får ikke vist det endelige skjemaet i MinJournal ettersom det ikke er mulighet til å bruke egne stilark i systemet. Det vi derimot har gjort er å vise skjemaet i MinJournal frem til og med redigert XHTML-utgave. Det endelige skjemaet viser vi som en vanlig HTML-side, men utseende på skjemaet vil være identisk til hvordan det vil bli i MinJournal med eget stilark knyttet til skjema.

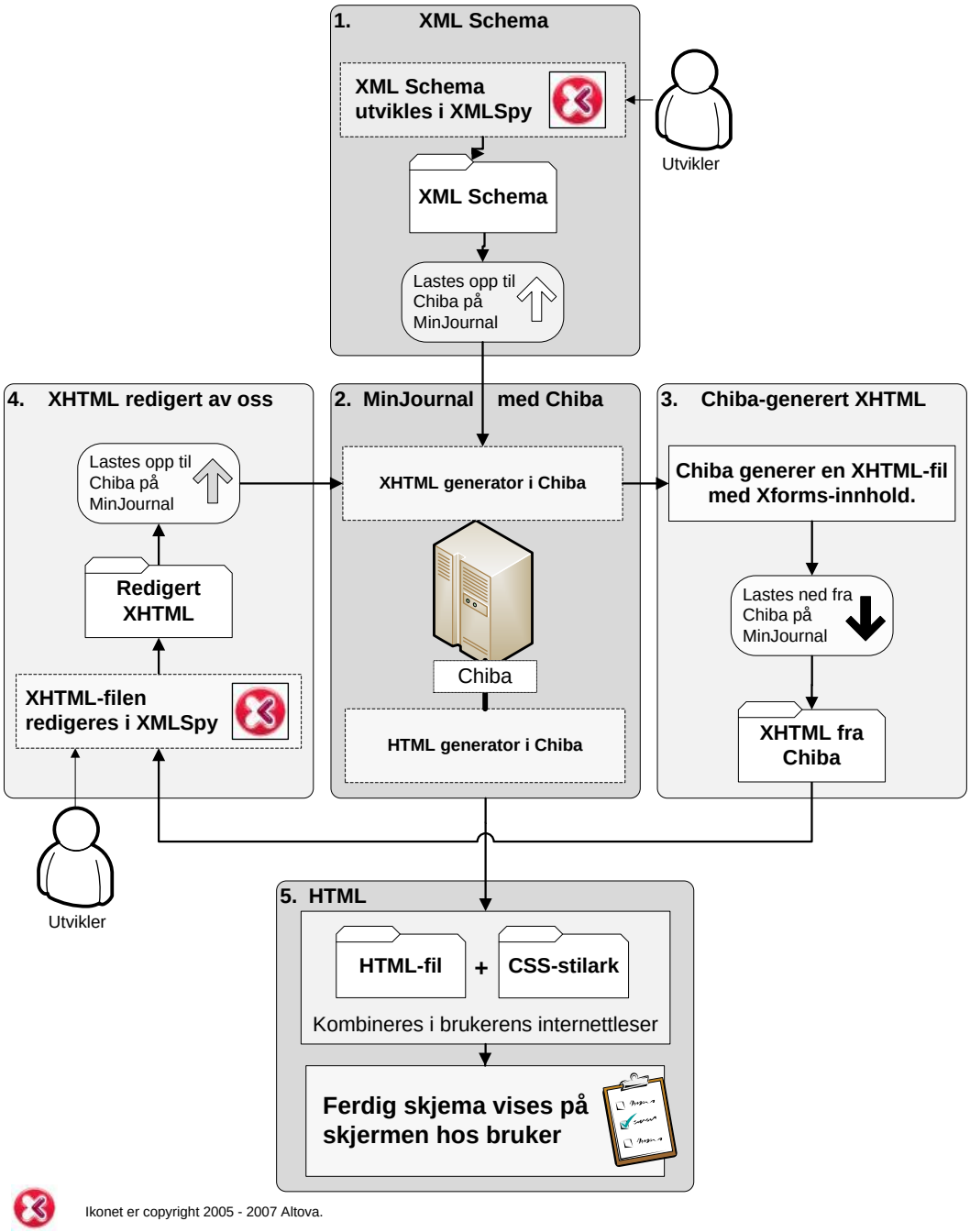
4.1.1 Skjemaprosessen

Her beskriver vi prosessen fra vi begynner å utvikle skjemaene frem til den ferdige utgaven av dem. Vi går grundig gjennom de sentrale punktene i neste delkapittel, hvor vi viser til det ferdige resultatet av ett av de fem skjemaene vi har utviklet.

4.1.1.1 Steg i prosessen (se Figur 24 under):

- Utvikle XML Schema (.xsd) i Altova XMLSpy 2007, må være validert og velformet
- Laste opp .xsd i MinJournal
    - Chiba (54) genererer et XHTML-dokument, basert på XForms, fra opplastet .xsd
- Laste ned XHTML og redigere denne for ønsket utseende
    - Redigere stilark og knytte det til XHTML.
- Laste opp ny XHTML til opplastet skjema
    - Chiba genererer HTML av opplastet XHTML
- Skjema er ferdig redigert og publisert

Det er ønskelig å fjerne punkt 3 og 4 i Figur 24, fordi det skaper merarbeid i prosessen. Punktene er i tillegg unødvendige siden det kun er et spørsmål om å utvikle et bedre stilark som fungerer for alle skjemaer, og inkludere støtte for XML Schema-filer som inneholder æ, ø og å.



Figur 24: Skjemaprosessen

4.1.1.2 Kort forklaring til prosessen

Når en laster opp .xsd i MinJournal blir dette generert til et filformat som støttes av webleser. MinJournal bruker verktøyet Chiba for å generere XHTML (basert på XForms) og HMTL fra opplastet .xsd.

Chiba er en "åpen kildekode Java implementering" av XForms standarden til W3C og leverer XForms funksjoner til weblesere. Chiba gjør det mulig å prosessere XForms til mange forskjellige plattformer og arkitekturer, inkludert MinJournal.

4.1.2 Utvikling

Vi går her gjennom prosessen med utvikling og testing av ett av de skjemaene vi har utviklet. Skjemaet er et registreringsskjema som er brukt ved registrering av pasienter ved Evjeklinikken. Dette registreringsskjemaet er i bruk ved Evjeklinikken i dag, men da i papirform. Det er et relativt omfattende skjema som skal samle inn mye informasjon om pasientene før oppholdet på Evjeklinikken.

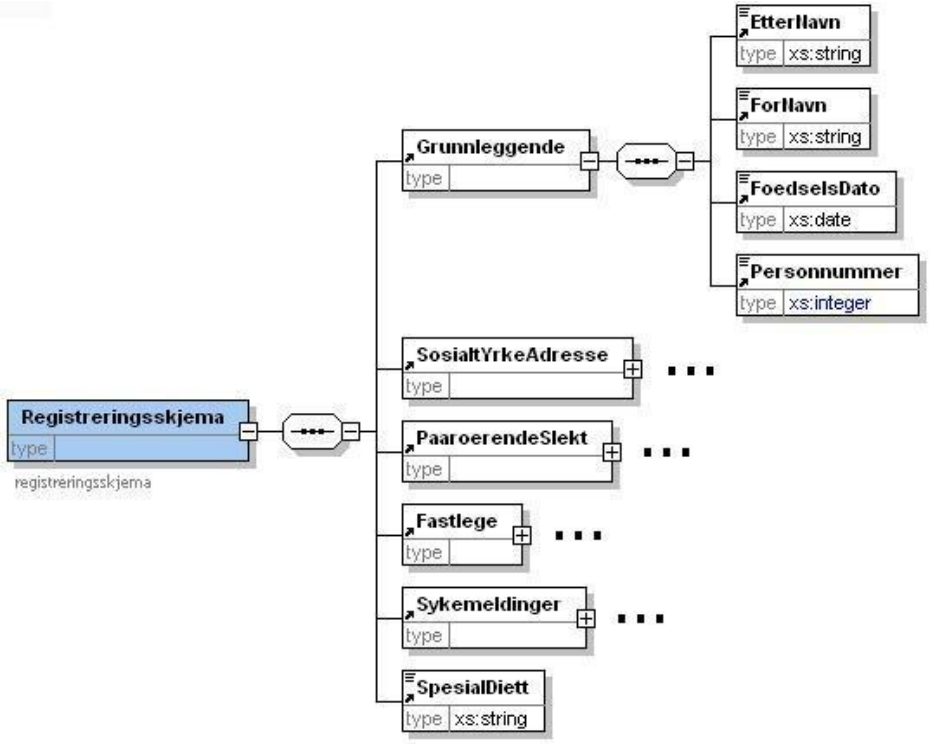
Alle skjemaene vi har utviklet finnes i papirform, og vi har utviklet dem for å bli tilsvarende de eksisterende skjemaene med hensyn til utseendet.

Ved utvikling av skjemaene brukte vi Altova XMLSpy 2007 og baserte oss på et eksempelskjema vi fikk fra Rikshospitalet – Radiumhospitalet HF. Skjemaet vi fikk tilsendt er ikke så omfattende, men er en grei mal å bruke ettersom skjemaet allerede er brukt og fungerer i MinJournal.

Figur 25 nedenfor viser et utdrag av koden til registreringsskjemaet. Her kan en se hvilken versjon og encoding som er brukt. Videre kan en se navn på elementene vi har brukt, men dette kommer bedre frem i Figur 26 hvor vi viser skjemaet i en skjemaoversikt fremfor ren tekst.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- edited with XMLSpy v2007 sp2 (http://www.altova.com) by Henrik Buksholt -->
<xs:schema xmlns="http://my-company.com/namespace"
xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://my-
company.com/namespace" elementFormDefault="qualified" attributeFormDefault="unqualified">
	<xs:element name="Registreringsskjema">
		<xs:annotation>
			<xs:documentation>registreringsskjema</xs:documentation>
		</xs:annotation>
		<xs:complexType>
			<xs:sequence>
				<xs:element ref="Grunnleggende"/>
				<xs:element ref="SosialtYrkeAdresse"/>
				<xs:element ref="PaaroerendeSlekt"/>
				<xs:element ref="Fastlege"/>
				<xs:element ref="Sykemeldinger"/>
				<xs:element ref="SpesialDiett"/>
			</xs:sequence>
		</xs:complexType>
	</xs:element>
```

Figur 25: Utdrag fra koden til registreringsskjema.xsd

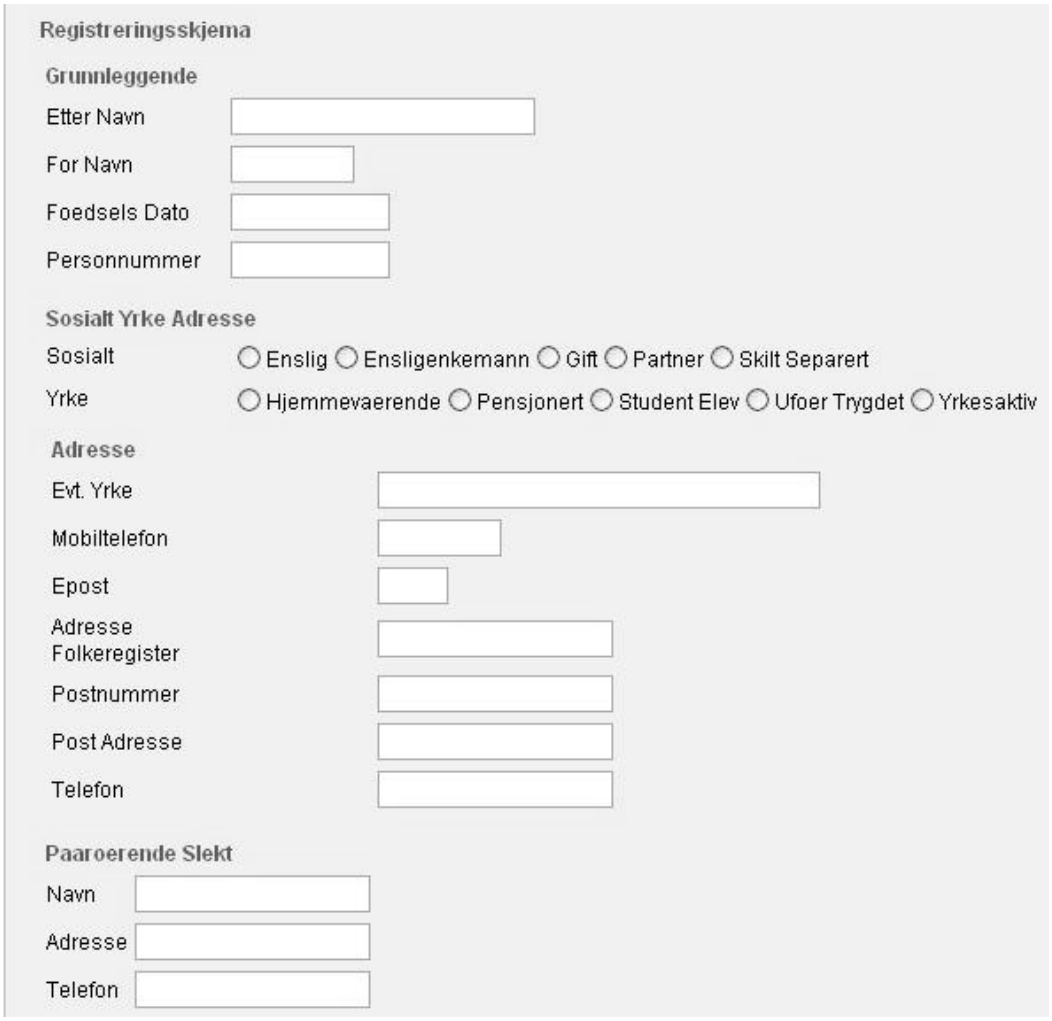


Figur 26: Registreringsskjema vist ved skjemaoversikt

Skjemaet ble etter noe testing og forandring validert og fikk status som velformet av utviklingsverktøyet. Dette viste seg ikke å være nok for at det skulle bli godtatt av MinJournal. Som en ser av elementnavnene har vi utelatt å bruke norske tegn (æ, ø, å). Ved første utkast av skjemaet brukte vi derimot norsk tegnsetting, men fikk da feilmeldinger ved opplasting av skjemaet til MinJournal. Etter flere henvendelser til Rikshospitalet – Radiumhospitalet HF og mye testing viste det seg at Chiba foreløpig ikke støtter norsk tegnsetting. Vi gikk så gjennom skjemaet og skiftet ut alle norske tegn og klarte dermed å laste opp vårt første skjema til MinJournal. Resultatet vises i Figur 27.

Ved å se på Figur 26 og det publiserte skjemaet på Figur 27 vil en kjenne igjen mange av navnene på elementene, for eksempel ser en ”Grunnleggende” med underliggende informasjon på begge figurene. Vi påpeker at figurene kun viser et utdrag av skjemaet, derfor vil mengden informasjon som vises variere i forhold til det endelige produktet. De fullstendige skjemaene er vedlagt (vedlegg A: Registreringsskjema, og resten ligger på CD i vedlegg B).

Skjemaet slik det fremgår av Figur 27 ser uferdig ut og har blant annet ikke norsk tegnsetting. Man kan også se at størrelsen på tekstfeltene varierer og ikke har noen sammenheng, samt at det har rotete og kjedelig design. Det gjenstår mye arbeid før skjemaet er slik vi ønsker at det skal fremstå for brukere av MinJournal. Når vi skulle forandre på dette skjemaet måtte vi laste ned den genererte XHTML-koden til skjemaet og forandre på denne.



Figur 27: Registreringsskjema direkte fra .xsd

Det er begrenset hva slags forandringer en kan gjøre ved å redigere koden i dette XHTML-dokumentet. For å legge inn bilde la vi til en referanse til det (nettadresse) like under <html:body> i koden.

```
<html:body>
<html:div class="evje">
  <img src="http://home.hia.no/~penils01/eklogo.gif" alt="Evjeklinikken"
longdesc="Evjeklinikken" />
```

Videre kan vi forandre den genererte koden slik at den viser norsk tegnsetting. Dette gjøres ved å redigere den "labell"-en som er feil. Nedenfor er det vist et eksempel med opprinnelig generert kode hvor det ikke er norsk tegnsetting og hvordan den ser ut etter redigering. En kan også se at det er XForms kode ("tag"-er) i det genererte XHTML-dokumentet.

Opprinnelig kode:

```
<xforms:label xforms:id="label_4">Foedsels Dato</xforms:label>
```

Redigert kode:

```
<xforms:label xforms:id="label_4">Fødselsdato</xforms:label>
```

Etter de ønskelige og mulige forandringene er gjort kan en laste opp ny XHTML og publisere skjemaet på nytt. Vi forandret på det vi hadde mulighet til og resultatet er vist i Figur 28 under.

Som en ser av skjemaet nedenfor (Figur 28), er det satt inn et bilde og teksten er forandret til å inneholde norsk tegnsetting. Vi kan derimot ikke forandre på størrelsen på tekstfeltene eller forandre på plasseringen av bildet. Altså, det som er mulig å forandre av utseende ved å redigere generert XHTML er blitt gjort på skjemaet over.

Grunnen til at vi ikke kan gjøre redigeringer utover dette, er at dette må skje ved å endre stilarket som er lagret på serveren til MinJournal. Det er foreløpig kun utviklerne som har mulighet for å endre denne filen. Det vi derimot kan gjøre er laste ned det opprinnelige stilarket og legge til egendefinerte stiler. Vi kan naturligvis ikke bruke MinJournal til å vise skjemaene våre basert på disse stilene, og må dermed vise disse som vanlige HTML-dokumenter i en lokal nettleser. Det vil på sikt bli mulig å bruke egne stiler på MinJournal, i form av enten en link eller egendefinerte stiler i MinJournal's opprinnelige stilark.

Figur 28: Registreringsskjema etter vår redigering av XHTML-dokumentet

4.1.3 Redigering av stilark

MinJournal baserer seg på stilark av typen CSS (Cascading StyleSheet) for å angi teksttype, farger, plasseringer av elementer etc. på websidene (HTML-filene). På MinJournal ligger det et standard-stilark som brukes på alle skjemaer. I denne fasen av prosessen er det designet av skjemaene som er aktuelt, og for å få ønsket utseende må vi redigere det opprinnelige stilarket.

Vi har som nevnt ikke mulighet for å påvirke det opprinnelige stilarket på MinJournal, så vi må lage nye klasser for å angi design som kun angår våre skjemaer. Klassene plasseres i en ny .css-fil og en link til denne plasseres i standard-skjemaet på MinJournal. I XHTML-filen til skjemaet angir vi hvilken stilklasse skjemaet skal følge.

Vi vil her vise noen utdrag fra CSS-filen. Fullstendig CSS-fil er ligger på CD-en i vedlegg B.

Det er viktig å skille skjema-klasse fra element-klasse;

Skjemaklasse angis i <*div class="skjemaklasse"*> mens elementklasse angis for eksempel slik:
<td id="group_1-label" colspan="2" class="full-group-label">Rapport</td>

4.1.3.1 Eksempel 4: Styling av elementklasse 'full-group-label'

I standardstilarket som ligger på MinJournal ser stilklassen slik ut:

```
.full-group-label {
   color:#685D47;
   font-size:12px;
   font-weight:bold;
   border:none;
   padding-top:5px;
  }
```

For å endre stilen til å passe våre skjemaer med skjemaklasse 'evje', satt vi inn følgende stil i tillegg:

```
.evje.full-group-label {
   color:#000000;
   font-size:13px;
   font-weight:bold;
   padding-top:10px;
   padding-bottom: 10px
  }
```

'.evje' er den teksten som gjør at stilen angis på elementer med elementklasse 'full-group-label' i skjemaer med skjemaklasse 'evje'.

Eksempel 4: Styling av elementklasse 'full-group-label'

4.1.3.2 Eksempel 5: Styling av element etter id

Elementer har en id i tillegg til klasse. Denne id er unik i dokumentet og kan derfor brukes til å endre stil til individuelle elementer uavhengig av klasse.
Syntaksen for å gjøre dette er som følger:

```
.evje_livstest #select1_16-label {
        width:200px;
        padding-right:20px;
        padding-top:10px;
        }
```

Der '.evje_livstest' er skjemaklassen og '#select1_16-label' angir at det er elementet med id 'select1_16-label' som skal "styles".

Eksempel 5: Styling av elementer etter id

4.1.3.3 Eksempel 6: Styling etter "tag"

Det kan angis felles stil for tag-er i HTML-dokumenter.
Hvis man eksempelvis vil endre stil på celler i en tabell, brukes følgende:

```
td {
  height: 20px;
  }
```

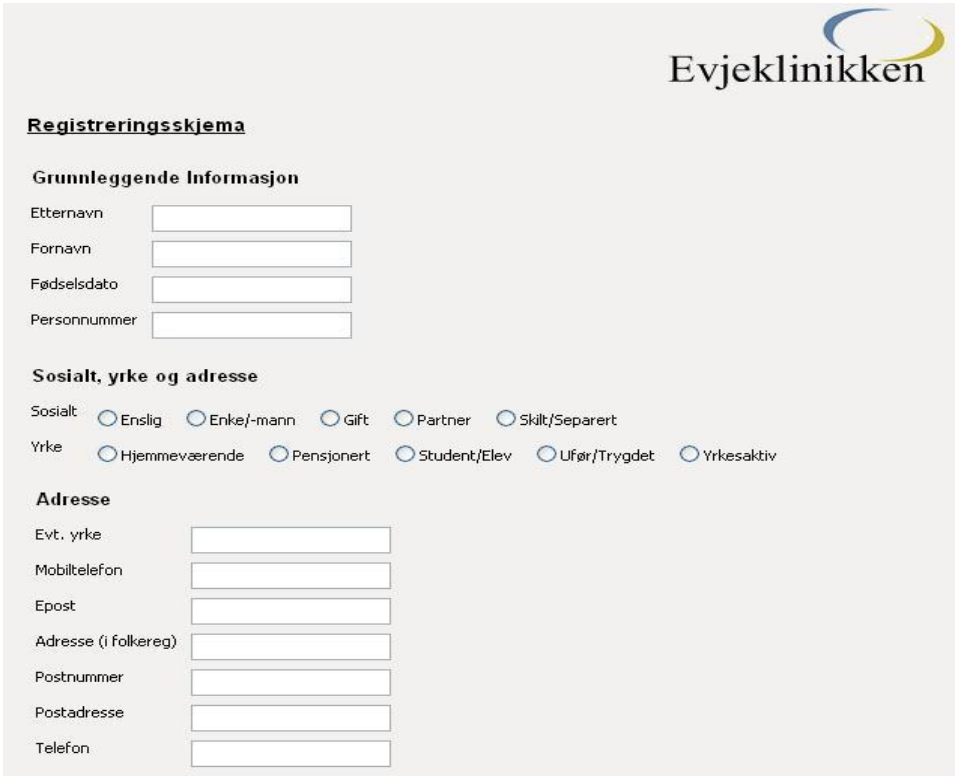
Eksempel 6: Styling etter "tag"

Det gjør at alle celler i tabeller vil ha en høyde på 20 piksler.

4.1.4 Resultat

Nedenfor vises det endelige resultat av Registreringsskjemaet. Resultatet ble et oversiktlig og funksjonelt skjema (Figur 29):

Som nevnt har vi utviklet alle våre skjemaer med papirformskjemaet som mal for utseendet. Under vises det opprinnelige skjemaet i papirform (Figur 30). Vi viser dette slik at en kan sammenligne disse to skjemaene og dermed selv vurdere om resultatet er tilfredsstillende. Minner igjen om at figurene av skjemaet som er vist i dette kapittelet bare er et utdrag av hele skjemaet. Det fullstendige skjemaet, samt de andre skjemaene, er vedlagt som henholdsvis vedlegg A og B.


Evjeklinikken

Registreringsskjema

Grunnleggende Informasjon

Etternavn
Fornavn
Fødselsdato
Personnummer

Sosialt, yrke og adresse

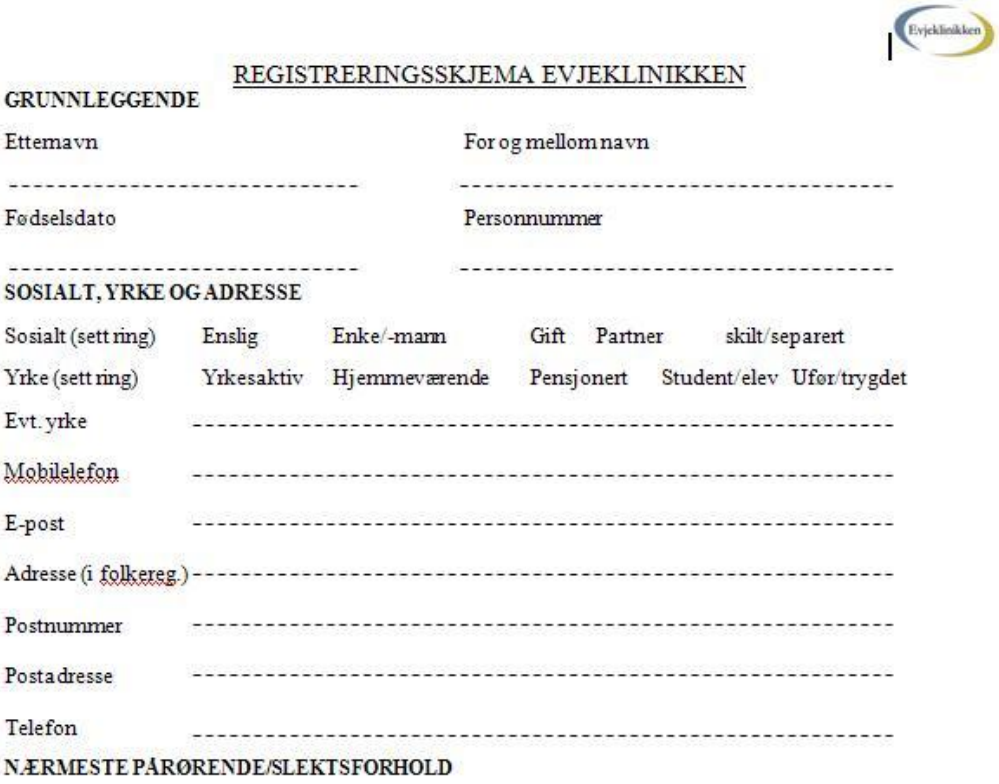
Sosialt ○ Enslig ○ Enke/-mann ○ Gift ○ Partner ○ Skilt/Separert

Yrke ○ Hjemmeværende ○ Pensjonert ○ Student/Elev ○ Ufør/Trygdet ○ Yrkesaktiv

Adresse

Evt. yrke
Mobiltelefon
Epost
Adresse (i folkereg)
Postnummer
Postadresse
Telefon

Figur 29: Endelig utgave av registreringsskjema


REGISTRERINGSSKJEMA EVJEKLINIKKEN

GRUNNLEGGENDE

Etternavn For og mellomnavn

Fødselsdato Personnummer

SOSIALT, YRKE OG ADRESSE

Sosialt (sett ring) Enslig Enke/-mann Gift Partner skilt/separert

Yrke (sett ring) Yrkesaktiv Hjemmeværende Pensjonert Student/elev Ufør/trygdet

Evt. yrke ----------

Mobilelefon ----------

E-post ----------

Adresse (i folkereg.) ----------

Postnummer ----------

Postadresse ----------

Telefon ----------

NÆRMESTE PÅRØRENDE/SLEKTSFORHOLD

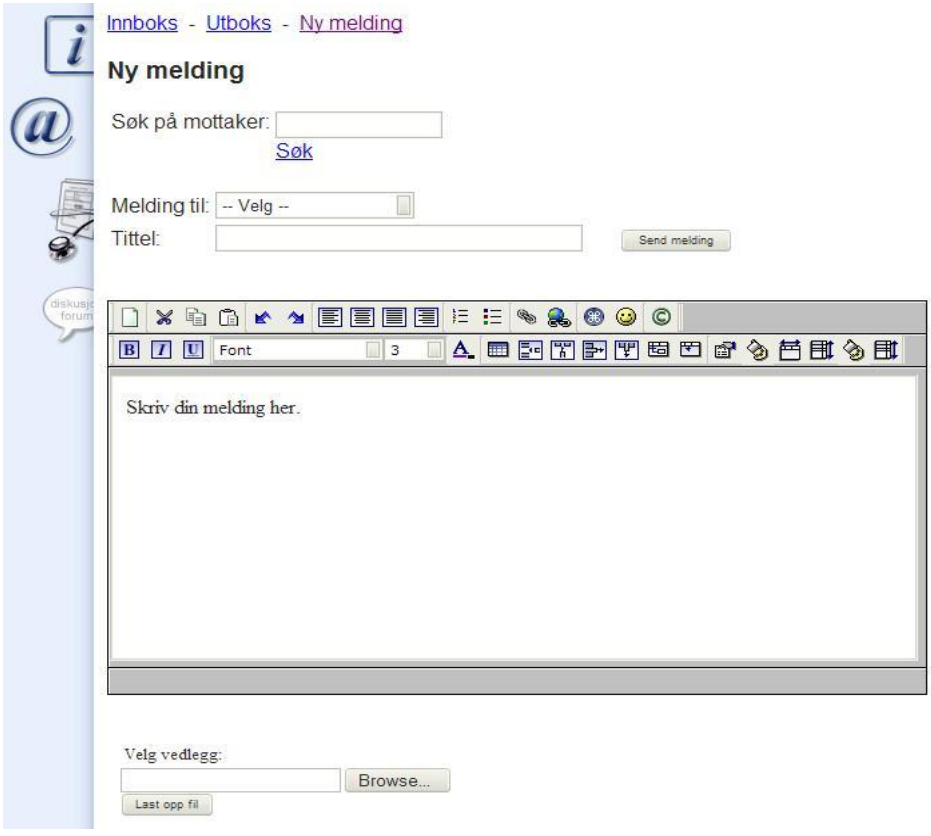
Figur 30: Registreringsskjema i papirform

4.2 Meldingstjeneste

I oppgavebeskrivelsen står det at vi skal tilpasse en meldingstjeneste i MinJournal som Evjeklinikken vil bruke til kommunikasjon mellom ansatte og pasienter. Da vi skrev oppgavebeskrivelsen hadde vi fått inntrykk av at dette ville la seg gjøre, men faktum er at meldingstjenesten er låst på MinJournal og ingen redigering er foreløpig mulig.

Det vi derimot kan gjøre med meldingstjenesten er å bistå Evjeklinikken i oppretting av grupper og brukere til denne tjenesten. Det som må gjøres er at Evjeklinikken opplyser om deres behov og om hvem som skal tilhøre de forskjellige tilgangsgrupperne.
Opprinnelig er det tenkt at pasienten kan sende melding til alt helsepersonell som er medlem av pasientens tilgangsgrupper, og disse vil pasienten kunne se i mottakerlisten i meldingstjenesten. Helsepersonell skal kunne sende melding til alle pasienter og alt helsepersonell som er medlem av egne tilgangsgrupper. Dette er det administrator som spesifiserer og det er derfor viktig at Evjeklinikken har klart for seg de ulike behovene hos pasientene og helsepersonellet.

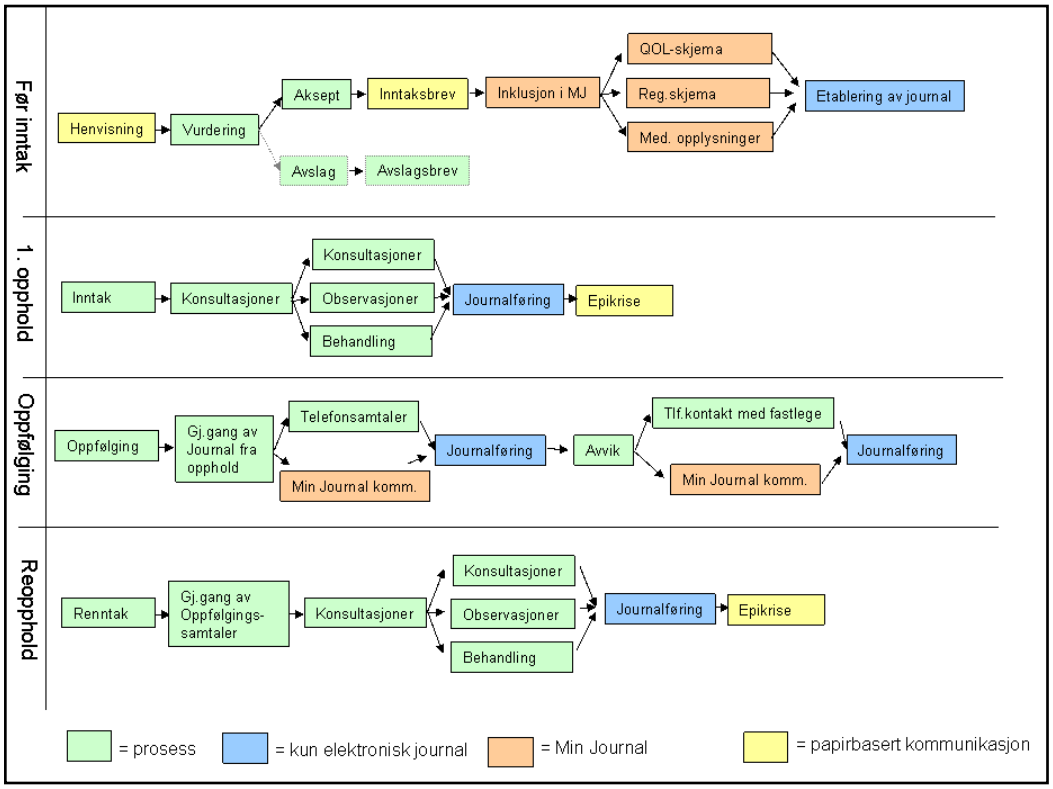
Evjeklinikken får den eksisterende meldingstjenesten i MinJournal. Denne er tilfredsstillende i bruk men mangler noen hensiktsmessige tjenester samt at utseendet er litt kjedelig. Den eksisterende meldingstjenesten, vist i Figur 31.



Figur 31: Meldingstjenesten

4.3 Prosess- og dokumentflyt etter implementering

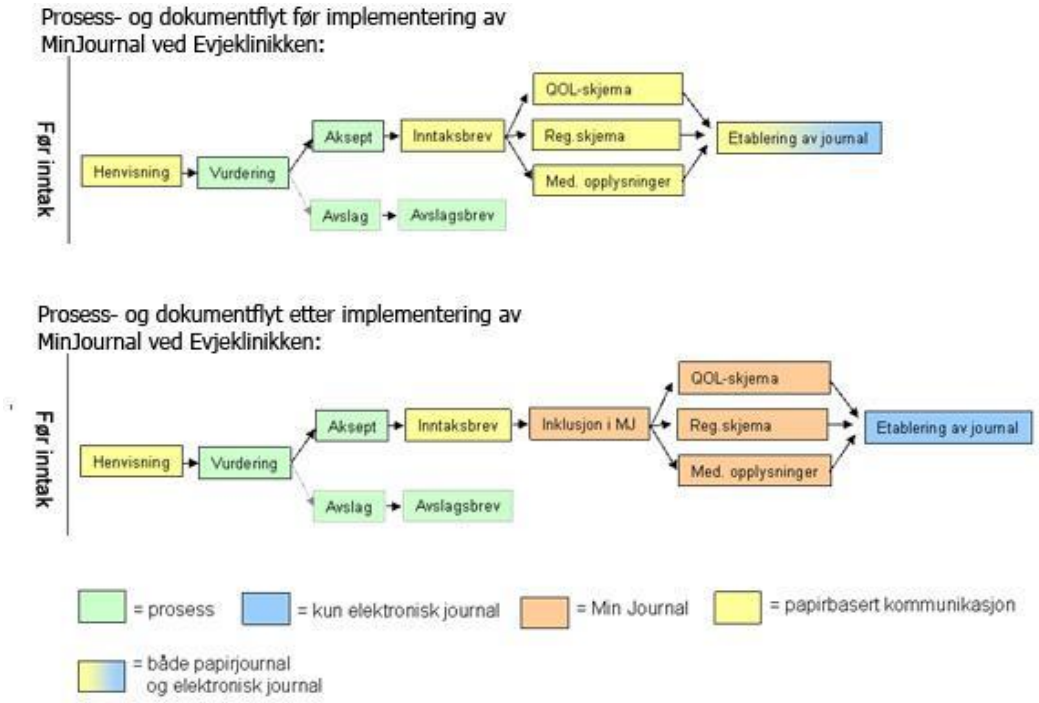
En full implementering av MinJournal ved Evjeklinikken vil endre dokumentflyten slik det er angitt i Figur 32 under. For en komplett sammenligning med dokumentflyten *før* implementering henviser vi til Figur 2 side 16.



Figur 32: Prosess- og dokumentflyt etter implementering av MinJournal

Som Figur 32 viser, vil pasientene benytte meldingstjenesten i sin kommunikasjon med klinikken og klinikkens ansatte.

En full innføring av MinJournal ved Evjeklinikken impliserer en overgang fra en dobbel journalføring til kun elektronisk journalføring. Dette fordi den papirbaserte datainnsamlingen fra pasientene vil kunne erstattes med bruk av MinJournal-skjema og utfylling via internett. Dette kommer bedre frem i sammenligningen på Figur 33 hvor vi viser utdrag fra prosess- og dokumentflyt før og etter en implementering.



Figur 33: Sammenligning av prosess- og dokumentflyt før og etter implementering

Figur 33 viser prosess- og dokumentflyt, før inntak av pasienter, *før* og *etter* en implementering av MinJournal ved Evjeklinikken. En ser av prosess- og dokumentflyten at det *før* implementering av MinJournal kun brukes papirbasert kommunikasjon frem til etablering av pasientjournal. Journalføringen ved dette tilfellet foregår i papirform og elektronisk.

Etter en full implementering av MinJournal vil mye av kommunikasjonen foregå elektronisk, samt at etableringen av journal og journalføring kun vil foregå elektronisk.

I startfasen etter implementering av MinJournal vil det være noen mangler, blant annet enn full automatisering for innhenting av data. For å oppnå ønsket effekt av MinJournal må en full automatisering av denne prosessen være på plass. Når det gjelder dette må Evjeklinikken avvente videre utvikling fra MinJournal-prosjektet.

Ved den midlertidige løsningen for innsamling av skjema har Evjeklinikken vurdert å kjøpe en skanner og programvare for lesing og klargjøring til analyse.

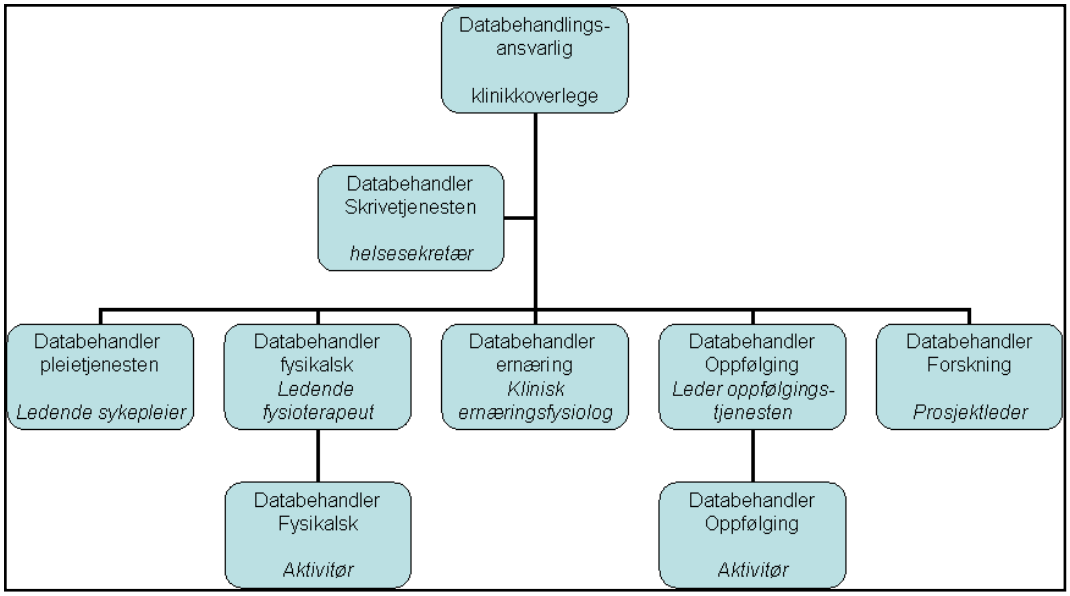
4.4 Juridiske beskrankninger ved Evjeklinikken

Som nevnt er det mange juridiske spørsmål og bestemmelser knyttet til implementering av en internettbasert pasientjournal.

Ved de juridiske problemstillingene knyttet til en implementering på Evjeklinikken er det helsepersonelloven og helseregisterloven som er relevante. Helsepersonellovens formål *"er å bidra til sikkerhet for pasienter og kvalitet i helsetjenesten samt tillit til helsepersonell og helsetjeneste"*. Formålsbestemmelsen i helseregisterloven legger stor vekt på at behandlingen av helseopplysninger skal skje i samsvar med grunnleggende personvernhensyn.

De sentrale problemstillingene ved en slik implementering omhandler overføring, utlevering av og tilgang til journaler, samt en definisjon av hvem samarbeidende personell, databehandlingsansvarlig og databehandler er. Ved overføring og utlevering av journaler blir sikkerheten ivaretatt av MinJournal. Hvem som skal ha tilgang til disse journalene, samt hvem som er databehandlingsansvarlig og databehandler ved Evjeklinikken blir bestemt av Evjeklinikken selv. Gjeldende bestemmelser ved "*overføring, utlevering av og tilgang til journaler og journalopplysninger*" samt bestemmelse om "*opplysninger til samarbeidende personell*" finnes i henholdsvis §§ 45 og 25 i helsepersonelloven.

Ved Evjeklinikken er det etablert en databehandlingsansvarlig og databehandlere. Nedenfor følger en oversikt over autoritetsstrukturen på Evjeklinikken hvor en kan se hvem som er databehandlingsansvarlig og databehandlere. Det følger av Helseregisterloven at det skal foreligge en slik autoritetsstruktur for databehandling av helseregistre. Bakgrunnen for dette er at ikke utenforstående skal få tilgang til registeropplysningene.



Figur 34: Autoritetsstruktur IT Evjeklinikken

Disse ansattes rolle og funksjon er definerte og det er gjennomført ROS-analyser (risiko- og sårbarhetsanalyse) i henhold til regelverket. Som en følge av implementeringen av MinJournal er

det ved klinikken igangsatt revisjon av ROS-analysen sammen med en redefinering av ansvarsområder knyttet til databehandling.
Evjeklinikken jobber med pasienter på flere nivåer, og har som premiss at samarbeidende fagpersonell må dele relevante pasientopplysninger. Det er derfor helt nødvendig å tilgjengliggjøre pasientens journal til alle involverte parter som har behov for denne. Dette må ifølge loven avtales med pasienten, hvor han eller hun kan motsette seg en slik utlevering av journalopplysninger. Dette er løst ved at pasienter ved Evjeklinikken avgir skriftlig samtykke på at deling av journalopplysninger kan skje til samarbeidende fagpersonell.

4.5 Brukerhåndbok

Som en tilleggsoppgave har vi på eget initiativ spurt etter behovet for en enkel brukerhåndbok av MinJournal ved Evjeklinikken. Denne forespørselen ble godt mottatt og var noe Evjeklinikken virkelig kunne ha bruk for. Både fagpersonell og pasienter vil ha stor nytte av en slik veiledning. Brukerhåndboken vil for det meste være en samling av bilder fra systemet hvor vi beskriver kort hva en skal, kan eller må gjøre ved de forskjellige menyene og valgene en møter i portalen. Eksempel på dette vises i Figur 35 under.

Forklaring til Figur 35:

Punkt 1: Her vil en kunne føre inn informasjon om seg selv; navn, mobilnummer, e-post- og bostedsadresse.

Punkt 2: Ved å trykke på bildet vil en kunne navigere seg tilbake til forsiden av MinJournal. En kan se at bildet er lenger ut til venstre i forhold til bildene under, og dette er fordi en allerede er på forsiden av MinJournal.

Punkt 3: Trykker en på dette bildet vil det føre en til meldingstjenesten i MinJournal. Herfra vil en kunne sende og motta meldinger til og fra fagpersonell og pasienter etter behov.

Punkt 4: Dette bildet indikerer skjema. Ved å trykke på dette bildet vil en komme til oversikten over egne skjemaer. Her kan en fylle ut publiserte skjema (for eksempel registreringsskjema) og se på allerede utfylte skjema.

Punkt 5: Dette er diskusjonsforumet i MinJournal. Her kan en delta i de diskusjoner en vil, samt følge med på andre aktuelle diskusjoner (en må ha tilgang til disse).

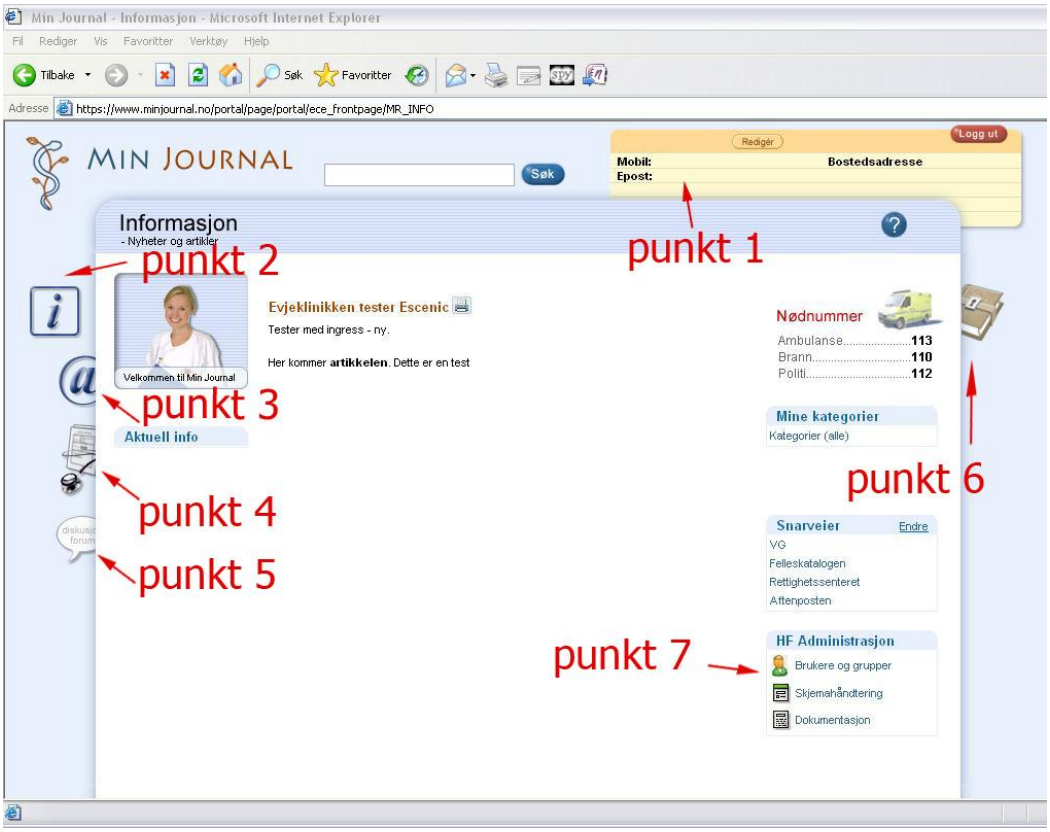
Punkt 6: Dagbok; Ved å trykke på dagboken vil en komme til sin personlige dagbok. Her kan en føre dagbok, dag for dag, og denne er det bare en selv som har tilgang til. Dager hvor en har skrevet noe vil i kalenderen markeres med uthevet skrift.

Punkt 7: Dette punktet er kun for de med administratorrettigheter. Pasienter og fagpersonell som ikke har behov for disse rettighetene vil ikke se denne menyen.

Administrative oppgaver som kan utføres her er: bruker- og gruppehåndtering, skjemahåndtering og dokumentasjonshåndtering.

Videre på denne forsiden finner man nødnumre, aktuell informasjon, hjelpfunksjon og sine egne snarveier til andre nettsteder.

Viser til vedlegg B for fullstendig brukerhåndbok.



Figur 35: Brukerhåndbok

5 Drøfting

I dette kapitlet drøfter vi vårt arbeid med oppgaven og våre resultater fra samtlige delproblemer. Vi belyser hvorvidt vi har nådd målene som ble satt eller ikke. Det innebærer om resultatene våre er tilfredsstillende og hva som eventuelt kunne vært bedre.

5.1 Vårt arbeid med oppgaven

Prosjektoppgaven ble gitt av Evjeklinikken som et samarbeid med Rikshospitalet – Radiumhospitalet HF's IT-avdeling i Oslo. Evjeklinikkens IT-ansvarlig Vidar Mortensen startet arbeidet med MinJournal tidlig, og satte seg godt inn i prosjektet og utviklingen.

Vi var usikre på hva masteroppgaven helt konkret innebar til å begynne med, og kontaktet derfor Evjeklinikken og Rikshospitalet – Radiumhospitalet HFs IT-avdeling for å sette opp mulige konkrete problemstillinger. Begge parter var opptatte med flere prosjekter, og e-post-utvekslingen gikk sent i starten. Dette forsinket oss en del, men vi klarte å få til et produktivt telefonmøte der vi satte opp flere problemstillinger som vi jobbet videre med. Etter diskusjoner oss to studenter i mellom, definerte vi et utkast av oppgavebeskrivelsen i samarbeid med veileder ved HiA.

I etterkant av dette fikk vi en melding fra studiekoordinator ved HiA om at Evjeklinikken var usikre på om de kunne gjennomføre prosjektet. Begrunnelsen var at deres IT-ansvarlig, og foregangsmann for MinJournal-prosjektet, hadde byttet jobb. De hadde derfor ikke kompetanse til å kunne veilede oss på det tekniske området. Vi diskuterte problemet med veilederen vår og studiekoordinator ved HiA, og besluttet å be om hjelp fra Rikshospitalet – Radiumhospitalet HF.

MinJournal-prosjektet ledes av IT-avdelingen ved Rikshospitalet – Radiumhospitalet HF i Oslo. Det var derfor naturlig å prøve få en kontaktperson der for teknisk veiledning. Sikkerhetsrådgiver Ivar Olav Berge gikk med på å være vår kontakt og veileder. Dette i samarbeid med konsulent Rune Engh, som kunne ta seg av tekniske spørsmål. Prosjektleder ved Evjeklinikken, Tor-Ivar Karlsen, samtykket i å veilede oss innen alt som angikk Evjeklinikken, samt innenfor aktuelt lovverk.

Vi hadde et møte med veilederne på IT-avdelingen ved Rikshospitalet – Radiumhospitalet HF den 24. januar 2007. Der fikk vi en innføring i prosjektet, og diskuterte aktuelle problemstillinger.

I etterkant arbeidet vi med oppgavebeskrivelsen. Denne ble godkjent og endret etter ønske fra oppdragsgiver før vi leverte den til studiekoordinator ved HiA den 7. februar 2007.

Vi begynte deretter å skrive på rapporten, samtidig som vi studerte litteratur og satte oss inn i aktuelt stoff. Dette innebar også en del spørsmål som ble stilt til våre veiledere på Rikshospitalet – Radiumhospitalet HF. IT-avdelingen der er omfangsrik og har mange prosjekter gående

samtidig. Våre to veiledere var derfor ofte opptatte, og e-poster og forsøk på å ta kontakt med dem var derfor ofte mer tidkrevende enn ønsket. Dette førte til at vårt planlagte arbeid med skjemautviklingen til dels ble forsinket.

På tross av forsinkelsen i utviklingen satte vi oss inn i relevant teknologi som ligger til grunn for MinJournal, lovverket som gjelder ved et slikt system, og informasjon om XML og skjemautvikling. Internett ble flittig brukt, men de mest sentrale og relevante kildene var Rikshospitalet – Radiumhospitalet HF i form av tilsendt dokumentasjon om MinJournal og et eksempelskjema til MinJournal. Selv om informasjonsflyten gikk seint mellom oss og veilederne, fikk vi utnyttet tiden til å skrive de delene av rapporten vi kunne.

For å kunne utvikle skjemaene måtte vi ha tilgang til MinJournal i form av et testsystem hvor vi kunne laste opp og teste de forskjellige utviklede skjemaene. En uheldig kommunikasjonssvikt mellom prosjektleder for MinJournal og Buypass førte til at det tok vesentlig lenger tid enn forventet før vi mottok smartkortet vårt. Det viste seg også at kommunikasjonssvikten hadde bredd seg til IT-driftsavdelingen ved Rikshospitalet – Radiumhospitalet HF, slik at smartkortene våre ikke var riktig registrert i deres system. Denne feilen ble rettet opp etter et møte med prosjektleder og våre veiledere i Oslo.

Etter sistnevnte møte var vi på Sunnaas sykehus TRS og fikk en demonstrasjon av deres system, minTRSSIDe, samt en fyldig dokumentasjon av arbeidet. Det var interessant å se en ferdig løsning, og det gav oss en viktig og økt forståelse for internettbaserte journalløsninger. I tillegg fikk vi se hva som har blitt gjort av relevant arbeid innenfor dette feltet.

For å hjelpe oss med de delene av rapporten som angår Evjeklinikkens behandling av data og juridiske beskrankninger, har vi fått utlevert relevante dokumenter av prosjektleder ved Evjeklinikken. Under en ”Workshop” på Evjeklinikken, i regi av Rikshospitalet – Radiumhospitalet HF angående implementering av MinJournal, deltok vi og fikk en bedre forståelse for eventuelle problemer og problemstillinger som må vurderes ved en slik implementering. Workshop-en hjalp oss godt på vei videre i rapportskrivingen og skjemautviklingen.

5.2 Hva vi kunne ha gjort annerledes

I etterkant av arbeidet med oppgaven ser vi at det er noen ting vi kunne eller burde gjort annerledes. Vi ble, som nevnt, noe forsinket i forhold til planen. Dette var blant annet på grunn av forsinkelser ved mottak av informasjon fra veilederne våre ved Rikshospitalet – Radiumhospitalet HF. Med hensyn til vår håndtering av disse forsinkelsene ser vi at vi burde vært mer pågående og bestemte for å få tak i informasjonen vi trengte. Vi avtalte ingen plan for når og hvor ofte veilederne skulle sette av tid til oss, noe vi helt klart hadde hatt stort utbytte av i forhold til at en del problemer kunne blitt løst på et tidligere tidspunkt.
I startfasen, under arbeidet med oppgavebeskrivelsen, burde vi ha anskaffet mer informasjon om MinJournal og muligheter for tilpasninger. En del av den informasjonen vi baserte oss på kom frem muntlig på vårt første møte med veilederne på Rikshospitalet – Radiumhospitalet HF.

Vi påpeker at informasjonen ikke var feil, men vi misforstod noen punkter. Det førte til at oppgavebeskrivelsen ble unøyaktig når det gjelder meldingstjenesten, som vi som nevnt ikke kan tilpasse på det nivået vi først ønsket. Resultatet vi kom frem til er skissert slik *vi* ønsker at skjemaene skal se ut. For å vise hvordan vi ønsker at det endelige resultatet av skjemaene skal være, har vi benyttet en ekstern webside for testing og publisering. Vi presiserer at våre endelige skjemaer ikke samsvarer med hvordan de ville sett ut i dagens MinJournal-løsningen.

5.3 Skjemautvikling og -prosess

Skjemaet vist i kapittel 4.1.4 ble, med tanke på utseende, lik den eksisterende papirformen som er oversiktlig og pen. Prosjektleder ved Evjeklinikken er godt fornøyd med skjemaet, og de andre skjemaene vi har utviklet, både med tanke på utseendet og funksjonalitet. Han har heller ingen betenkeligheter med å ta dette i bruk ved MinJournal på Evjeklinikken.

Vi hadde noen problemer under redigeringen av utseende på skjemaet. Disse var først og fremst relatert til at det opprinnelige stilarket på MinJournal-serveren ikke kunne forandres. Per dags dato finnes det ikke muligheter for å laste opp egendefinerte stilark til MinJournal-serveren. Løsningen vår ble da å vise til det endelige skjemaet på en webside hvor vi kunne bruke vårt eget stilark, tilpasset de utviklede skjemaene, for ønsket utseende.

For å oppnå optimalt resultat i det praktiske arbeidet hadde det vært ønskelig med større fleksibilitet når det gjelder tilpasning av utseende på skjemaer, meldingstjenesten og MinJournal totalt sett. Stilarket til skjemaene burde vært mulig å laste ned, redigere og laste opp på nytt. Det burde være mulighet for å laste opp flere stilark slik at hvert skjema kunne hatt sitt eget stilark med eget utseende. Dette ville ikke være nødvendig ved alle skjemaer men like fullt svært ønskelig.

Skjemaprosessen (illustrert med Figur 24 på side 45) synes vi er for omfattende til praktisk bruk i en helseklinikk. Det trengs en forståelse for XML og XHTML slik som løsningen fungerer på nåværende tidspunkt. Det er ikke en optimal løsning å måtte redigere XHTML-filene og stilarket for at skjemaene skal få ønsket utseende. Helsepersonellet vil i de fleste tilfeller ha ferdig utviklede skjemaer som lastes opp ved behov. Det vil da bli for tidkrevende å måtte gjøre disse ekstra modifikasjonene hver gang et skjema skal lastes opp.

Man ser ofte at helsepersonell i tillegg har bakgrunn innen IT. Ansatte med slik bakgrunn bidrar til å forenkle implementeringen av MinJournal i nåværende form. Det er uansett unødvendig å måtte gi personalet opplæring i noe mer enn et program for å opprette et XML Schema-dokument. Dette er en løsning hvor den delen av skjemaprosessen som gjelder redigering av XHTML, og eventuelt også stilarket, bør fjernes. Som nevnt tidligere innebærer dette å legge til støtte for spesielle tegn som æ, ø og å, i tillegg til et stilark som fungerer til alle skjemaer. Dette antar vi at allerede er med i planene for den videre utviklingen av MinJournal, ettersom det er et stort hinder for brukervennligheten i systemet.

5.4 Meldingstjenesten

Evjeklinikken får en funksjonell og operativ meldingstjeneste som fungerer tilfredsstillende. Ved den nåværende meldingstjenesten kan kommunikasjonen foreløpig bare gå mellom ansatte ved Evjeklinikken, og mellom pasienter og helsepersonell.

Det var ønskelig med mulighet for kommunikasjon til samarbeidende helsepersonell (for eksempel fastlege), men MinJournal inneholder i dag ingen støtte for dette. Dette er for øvrig svært aktuelt i den videre prosessen med MinJournal, så sannsynligvis vil det komme støtte for inklusjon av samarbeidende helsepersonell i nær fremtid. Teknologien er allerede på plass for en slik tjeneste, og utfordringen vil være å få dette gjennomført slik at det tilfredsstiller lovverket.

Noe annet som hadde vært hensiktsmessig hadde vært muligheter for å kunne sende en kopi av meldingen til for eksempel samarbeidende personell. Dette hadde gjort det enklere for helsepersonell å være oppdatert på pasientene, da helsepersonell kunne fulgt meldingsflyten fra pasient til annet helsepersonell.

Videre ønsket Evjeklinikken et personlig preg på meldingstjenesten. Dette lot seg heller ikke gjøre da meldingstjenesten ikke er mulig å redigere. Dette er per dags dato noe som må gjøres av utviklerne til MinJournal.

Det som må gjøres før meldingstjenesten er operativ ved Evjeklinikken er å opprette brukere og brukergrupper og hvem som skal tilhøre de forskjellige tilgangsgruppene.
Når dette er avgjort må tilgangsgruppene bli lastet opp i MinJournal, enten ved å laste opp en XML fil eller ved å legge disse inn i systemet direkte på serveren.

5.5 Prosess- og dokumentflyten ved Evjeklinikken

Ved en full implementering av MinJournal vil opprettelse av alle journaler foregå elektronisk. Kommunikasjon med Evjeklinikken vil, i tillegg til de opprinnelige telefonsamtalene, skje ved hjelp av meldingstjenesten i MinJournal.

En slik endring i prosess- og dokumentflyten vil gi de ønskede gevinstene for Evjeklinikken. Journaler vil bli elektroniske og oppfølgingen av pasientene vil bli bedre og enklere med meldingstjenesten. Dette vil redusere belastningen på oppfølgingssenteret, da en del av oppfølgingen kan skje via denne. Når det oppdages avvik fra forventet progresjon vil oppfølgingssenteret kunne benytte MinJournal, i tillegg til telefonsamtaler, for en dialog med pasienten. Per dags dato er det oppfølgingssenteret som oppdager avvik, men dette er noe som kan automatiseres ved automatiske analyser av innsamlet data fra MinJournal. Om tenkt progresjon ikke er oppnådd kunne det vært ønskelig med full automatikk slik at oppfølgingssenteret får en melding om dette. Da kan oppfølgingssenteret ta kontakt med den aktuelle pasienten for å høre hva avviket skyldes og hvordan en skal jobbe for at slikt ikke skal skje igjen.

En implementering av MinJournal vil i første omgang ikke oppfylle alle de ønskelige gevinstene med tanke på prosess- og dokumentflyten. Foreløpig er det slik at datainnsamlingen er begrenset. Registreringsskjemaene fylles ut av pasientene, og det respektive fagpersonellet (ernæringsfysiolog, fysioterapeut, lege og sykepleier) bruker dataene i videre tilrettelegging.

Det er ønskelig med en full automatisering av datainnsamling fra skjemaene på MinJournal. Etter hvert som MinJournal blir bedre utbygget vil dette støttes og dataene kunne legges inn i en database for både forsknings- og utviklingsformål. Forskningsskjemaene (WRSM, OWLQOL) vil på samme måte fylles ut av definerte pasientgrupper på fastsatte tidspunkt. Når disse blir lagt i en database, vil de kunne hentes ut og analyseres ved behov, blant annet til forskning.

5.6 Håndtering av de juridiske problemstillingene

For å tilfredsstille lovverket har Evjeklinikken etablert en databehandlingsansvarlig og databehandlere. Det foreligger også en autoritetsstruktur for databehandling av helseregistre i samsvar med helseregisterloven. Videre er det gjennomført ROS-analyser i henhold til regelverket, og det er nå satt i gang en revisjon av disse som en følge av implementeringen av MinJournal.

For at samarbeidende fagpersonell skal få tilgang til pasientjournaler krever lovverket at dette må avtales med pasienten, og at han/hun må gi samtykke. Dette er løst ved at samtlige pasienter ved Evjeklinikken må avgi skriftlig erklæring på at journaler skal være tilgjengelige for samarbeidende fagpersonell.

Evjeklinikken imøtekommer, på en tifredsstillende måte, de juridiske problemstillingene en implementering av en internettbasert pasientjournal reiser. Det kommer godt frem at de juridiske beskrankningene blir tatt alvorlig og at Evjeklinikken legger arbeid i å imøtekomme disse.

5.7 Sikkerhetsløsninger i MinJournal

MinJournal baserer seg på PKI-sertifikater for å sikre informasjonsflyten over internett. Sertifikatene inneholder en privat og en offentlig nøkkel. De offentlige nøklene utveksles mellom server og klient for å sikre utvekslingen av en felles krypteringsnøkkel.

Ved at det benyttes PKI-sertifikater både på server- og klientsiden, Økes sikkerheten drastisk. ”Man-in-the-middle”-angrep blir vanskeligere å utføre når begge parter autentiserer hverandre med sertifikater som er utstedt av godkjente CA-er. Brukersertifikatene er i tillegg knyttet til personlig identitet (personnummer), slik at MinJournal-serveren sjekker smartkortnummer mot sin interne database over brukere.

Vi vil også påpeke at serversertifikatet inneholder et 2048 bits nøkkelpar, og brukersertifikatet inneholder et nøkkelpar på 1024 bits. Grunnen til at nøklene er så store er for å unngå såkalte "Brute force attacks" (55).

Den kritiske fasen i enhver krypteringsløsning er ofte når partene skal autentisere hverandre og forbindelsen settes opp. Vi har tidligere beskrevet "Man-in-the-middle"-angrep (kapittel 2.5.5.3 på side 29), som er et vanlig angrep i denne fasen av kommunikasjonen. Det er derimot også mulig å snappe opp informasjon etter at initieringen av forbindelsen er gjennomført, og den krypterte forbindelsen er satt opp. Man må da finne krypteringsnøkkelen som er i bruk.

MinJournal benytter en symmetrisk sesjonsnøkkel ("symmetric key") for å sikre overføringen av data. Algoritmen som benyttes her er RC4 med en nøkkellengde på 128 bits. Denne RC4-nøkkelen kan virke liten i forhold til nøkkelparet som er lagret i PKI-sertifikatet, men her må man passe på å ikke se seg blind på nøkkellengden, og tenke mer praktisk funksjon.

For det første er dette en sesjonsnøkkel, som betyr at det blir generert en ny nøkkel for hver gang man logger inn på MinJournal. Hver bruker vil nok ikke være innlogget mer enn ca. én time og etter utlogging merkes nøkkelen som ugyldig.

For det andre kreves det en enorm regnekraft for å knekke en 128 bits nøkkel. Det er snakk om milliarder, om ikke billioner av år, for å finne en slik nøkkel med dagens teknologi.

VeriSign skriver følgende på sine nettsider (41):
"High-level encryption, at 128 bits, can calculate 288 times as many combinations as 40-bit encryption. That's over a trillion times a trillion times stronger. A hacker with the time, tools, and motivation to crack 40-bit encryption would require a trillion years to break into a session protected by an SGC-enabled certificate."

Dette leser vi litt kritisk siden det er argumenter for å selge en sikkerhetsløsning, men VeriSign er også en av verdens største leverandører av sikkerhetsløsninger så det må være noe sant i det. Det de sannsynligvis snakker om, er å knekke krypteringsnøkkelen med "brute force attack", altså rå regnekraft.

Det er ikke hensiktsmessig å snakke om å "knekke" krypteringsnøkler på den måten, siden det som oftest ikke er lønnsomt og/eller tar for lang tid. Det er bedre å prøve å utnytte hull eller sårbarheter i en algoritme.

RC4 har noen kjente sårbarheter som kan utnyttes, men som er så godt dokumenterte og kjente at det er gjort tilstrekkelig mottiltak for å stoppe utnytting av dem. På Wikipedia, i innledningen til artikkelen om RC4 (52), leser vi at det er den mest brukte "stream cipher" algoritmen. Dette på tross av at den ikke oppfyller kravene til moderne krypteringsalgoritmer. Det anbefales heller ikke at den brukes i nyere applikasjoner, selv om den i mange tilfeller er sikker nok for praktisk bruk.

For å prøve å sette sikkerheten i perspektiv trekker vi inn WEP (Wired Equivalent Privacy (56)), som benytter RC4 for kryptering av trådløse forbindelser. WEP ble kritisert for å være

usedvanlig usikkert. En gjennomsnittlig datakyndig person kan nå enkelt laste ned verktøy som knekker krypteringsnøkkelen på noen få timer kun ved hjelp av en vanlig hjemme-PC. Dette er en løsning som er et bevis på feil bruk av RC4. SSL 3.0 implementeringen av RC4 har ingen slike "lettvinte" sårbarheter så vidt vi kjenner til.

5.8 Resultatet av implementeringen

En full innføring av MinJournal ved Evjeklinikken vil gi mange gevinster for både ansatte og pasienter. I løpet av workshop-en på Evje nevnte de ansatte flere ønskelige gevinster ved bruk av MinJournal. Disse var:

- Bedre resultat av behandlingen
- Pasientene føler seg møtt
- Bedre service
- Bedre oppfølgingstjeneste
- Styrke samarbeid med annet helsepersonell

Bedre resultat av behandlingen vil være et resultat av alle gevinstene ved et slikt system. Pasienter vil føle seg møtt ettersom en slik tjeneste vil være nyttig for pasientene, samt at det har vært en etterspurt tjeneste. Evjeklinikken vil yte bedre service ved at de vil være tilgjengelige gjennom meldinger på meldingstjenesten. Et slikt system vil også lette mye av arbeidet de har i dag med innsamling av data og skjemaer, slik at de har bedre tid til pasientene.

Pasientene vil ha stor nytte av MinJournal da en implementering av dette systemet vil gjøre kommunikasjonen mellom pasient og fagpersonell ved Evjeklinikken bedre. Oppfølgingstjenesten i dag skjer på faste tidspunkt, og over telefon, mens ved bruk av MinJournal kan pasienter skrive til fagpersonell når de vil og få respons innen en gitt tidsramme.

På sikt vil MinJournal høyst sannsynlig ha støtte for inklusjon av samarbeidende helsepersonell. Dette vil helt klart styrke samarbeidet mellom helsepersonell og igjen bidra til en bedre behandling av pasienter.

6 Konklusjon

Vi har basert arbeidet vårt på eksisterende MinJournal ved Rikshospitalet – Radiumhospitalet HF. Vi har fått dokumentasjon og en innføring i MinJournal-løsningen, og i tillegg har vi fått et eksempelskjema til bruk i MinJournal.

Vi har utviklet fem skjemaer som Evjeklinikken skal ta i bruk når MinJournal er implementert og operativt ved klinikken. Samtlige skjemaer ble vurdert og godkjent av prosjektleder ved Evjeklinikken, som var godt fornøyd med resultatet.

En implementering av MinJournal reiser mange juridiske spørsmål og vi har belyst de mest relevante bestemmelsene som gjelder ved en slik internettbasert pasientjournal. Evjeklinikken har gjort nødvendige tiltak, og tilfredsstiller samtlige bestemmelser i lovverket som er gjeldende ved implementering av MinJournal-løsningen.

Videre har vi beskrevet den implementerte sikkerheten som anvendes av MinJournal. Sikkerheten er allerede implementert og dermed ikke vårt hovedfokus. Det er likevel hensiktsmessig å beskrive dette godt slik at en ser viktigheten av en bunnsolid sikkerhet og sikring av data ved et slikt system. Det kommer godt frem at utviklerne av MinJournal-løsningen har hatt fokus på sikkerheten, og ser viktigheten av solide sikkerhetsløsninger ved en slik internettbasert journal. Vi har, med tanke på informasjonssikkerheten, ikke funnet noen svakheter i MinJournal-løsningen.

En implementering av MinJournal ved Evjeklinikken vil bidra til et bedre og bredere behandlingstilbud til pasientene, blant annet ved hjelp av meldingstjenesten. Ettersom MinJournal fortsatt er under utvikling, og tjenestene mangler tilpasningsmuligheter, fikk vi ikke gjort ønskede endringer i meldingstjenesten. Slik den fremstår i dag, er den fullt operativ men ikke tilpasset Evjeklinikken slik det var ønsket.

For de ansatte vil en implementering lette flere arbeidsoppgaver, blant annet journalføringen. Dette fører til at de ansatte vil få mer tid til andre arbeidsoppgaver, som igjen vil bidra til et bedre behandlingstilbud.

For å oppnå ønsket gevinst av implementeringen må Evjeklinikken gå til anskaffelse av et verktøy som automatiserer innsamling av data. Ved en full automatisering er innsamlet data lettere tilgjengelig for bruk til blant annet forskning og analysering.

Videre er det hensiktsmessig med større frihet ved tilpasning av MinJournal. Dette er noe som må gjøres av utviklerne av MinJournal. Systemet er fullt operativt per dags dato men mye arbeid gjenstår før MinJournal fremstår slik det er tenkt. Mange av tjenestene som tilbys er fortsatt mangelfulle. Vi mener oppgaven vår beskriver de aktuelle problemstillingene som oppstår ved implementering av et internettbasert pasientjournalsystem, samt belyser mangler og nødvendig videre arbeid.

7 Referanser

1. **Evjeklinikken AS.** Evjeklinikken. [Internett] [Sitert: 10 05 2007.] http://www.evjeklinikken.no/.
2. **Rikshospitalet - Radiumhospitalet HF, IT-avdelingen.** *MinJournal.* [Internett] [Sitert: 11 05 2007.] http://www.minjournal.no.
3. **World Wide Web Consortium (W3C).** *HTML 4.01 Specification.* [Se http://www.w3.org/TR/html401/]
4. —. Overview of SGML Resources. *W3C.* [Internett] [Sitert: 14 05 2007.] http://www.w3.org/MarkUp/SGML/.
5. **World Wide Web Consotrium (W3C).** *Extensible Markup Language (XML).* [Se http://www.w3.org/XML/]
6. **Unicode Inc.** Unicode Home Page. [Internett] [Sitert: 14 05 2007.] http://unicode.org/.
7. **Wikipedia.org.** XML. *no.Wikipedia.org.* [Internett] [Sitert: 15 05 2007.] http://no.wikipedia.org/wiki/XML.
8. **World Wide Web Consortium (W3C).** *XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition).* [Se http://www.w3.org/TR/xhtml1/]
9. —. *W3C.* [Internett] [Sitert: 14 05 2007.] http://www.w3.org.
10. —. *XML Schema.* [Se http://www.w3.org/XML/Schema]
11. —. Guide to the W3C XML Specification ("XMLspec") DTD, Version 2.1. *W3C.* [Internett] [Sitert: 14 05 2007.] http://www.w3.org/XML/1998/06/xmlspec-report-v21.htm.
12. **Altova.** XML Spy. *Altova.* [Internett] [Sitert: 14 05 2007.] http://www.altova.com/products/xmlspy/xml_editor.html.
13. **World Wide Web Consortium (W3C).** *XML Path Language (XPath) Version 1.0.* [Se http://www.w3.org/TR/xpath]
14. —. *The Extensible Stylesheet Language Family (XSL).* [Se http://www.w3.org/Style/XSL/]
15. —. *XForms 1.1.* [Se http://www.w3.org/TR/xforms11/]
16. **Wikipedia.org.** XForms. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Xform.
17. **Helse- og omsorgsdepartementet.** *Lov om helsepersonell.* [Lovdata.no (http://www.lovdata.no/all/nl-19990702-064.html)]
18. —. *Lov om pasientrettigheter.* [Lovdata.no (http://www.lovdata.no/all/nl-19990702-063.html)]
19. —. *Lov om helseregistre og behandling av helseopplysninger.* [Lovdata.no (http://www.lovdata.no/all/nl-20010518-024.html)]
20. **Wikipedia.org.** Denial-of-service attack. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Denial-of-service_attack.
21. **Norsk Helsenett AS.** *Norsk Helsenett.* [Internett] [Sitert: 14 05 2007.] http://www.nhn.no/om-norsk-helsenett/about.
22. **Wikipedia.org.** Smart card. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Smart_card.
23. **Rikshospitalet - Radiumhospitalet HF.** *Systemforvaltning "MinJournal".* Oslo : RR HF IT-avdelingen, 2006.
24. **Wikipedia.org.** ISO 7816. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/ISO_7816.

25. —. ISO 7810. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/ISO_7810.
26. **Hitachi.** MULTOS. *Hitachi Smart Card System Solutions.* [Internett] [Sitert: 14 05 2007.]
http://www.hitachi.co.jp/Div/smartcard/english/multos.html.
27. **MULTOS Consortium.** *MULTOS Consortium.* [Internett] [Sitert: 14 05 2007.]
http://www.multos.com/.
28. **Wikipedia.org.** Read only memory. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Read-only_memory.
29. —. EEPROM. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/EEPROM.
30. —. RFID. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/RFID.
31. **Kevin Shorter.** PKI - what is it and do I want one? *BCS.org.* [Internett] [Sitert: 17 04 2007.]
http://www.bcs.org/server.php?show=conMediaFile.1462.
32. **Wikipedia.org.** Public key cryptography. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Public-key_cryptography.
33. —. Certificate Authority. *Wikipedia.* [Internett] [Sitert: 15 04 2007.]
http://en.wikipedia.org/wiki/Certificate_authority.
34. **Kevin Shorter.** *BCS.org.* [Internett] [Sitert: 15 04 2007.]
http://www.bcs.org/server.php?show=ConWebDoc.2964.
35. **Wikipedia.org.** Transport Layer Security (TLS) / Secure Sockets Layer (SSL). *Wikipedia.*
[Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Transport_Layer_Security.
36. —. Symmetric key cryptography. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Symmetric_key.
37. **Defense Advanced Research Projects Agency.** *RFC 793 Transmission Control Protocol.* [Se
http://www.faqs.org/rfcs/rfc793.html]
38. —. *RFC 791 Internet Protocol.* [Se http://www.faqs.org/rfcs/rfc791.html]
39. **Wikipedia.org.** Cryptographic nonce. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Cryptographic_nonce.
40. —. Man-in-the-middle attack. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Man_in_the_middle.
41. **VeriSign.** *VeriSign.* [Internett] [Sitert: 14 05 2007.] http://www.verisign.com/.
42. **Rikshospitalet - Radiumhospitalet HF, IT-avdelingen.** *Sikkerhetsarkitektur.* Oslo : s.n., 2006.
43. **K. Zeilenga, OpenLDAP Foundation.** *RFC 4510: Lightweight Directory Access Protocol.* [Se
http://tools.ietf.org/html/rfc4510]
44. **Wikipedia.org.** Directory services. *Wikipedia.* [Internett] [Sitert: 14 05 2007.]
http://en.wikipedia.org/wiki/Directory_service.
45. **Wkipedia.org.** DMZ. [Internett] [Sitert: 11 05 2007.]
http://en.wikipedia.org/wiki/Demilitarized_zone_%28computing%29.
46. **Rikshospitalet - Radiumhospitalet HF.** *Min Journal - Funksjonalitetsbeskrivelse.* Oslo : RR HF - IT avdelingen, 2006.
47. **Sunnaas sykehus TRS.** Hva er TRS? [Internett] [Sitert: 23 mars 2007.]
http://trs.sunnaas.no/.
48. —. Om minTRSSIDe. [Internett] [Sitert: 23 mars 2007.]
http://trs.sunnaas.no/modules/module_123/proxy.asp?D=2&C=226&I=4344&mids=a643a.

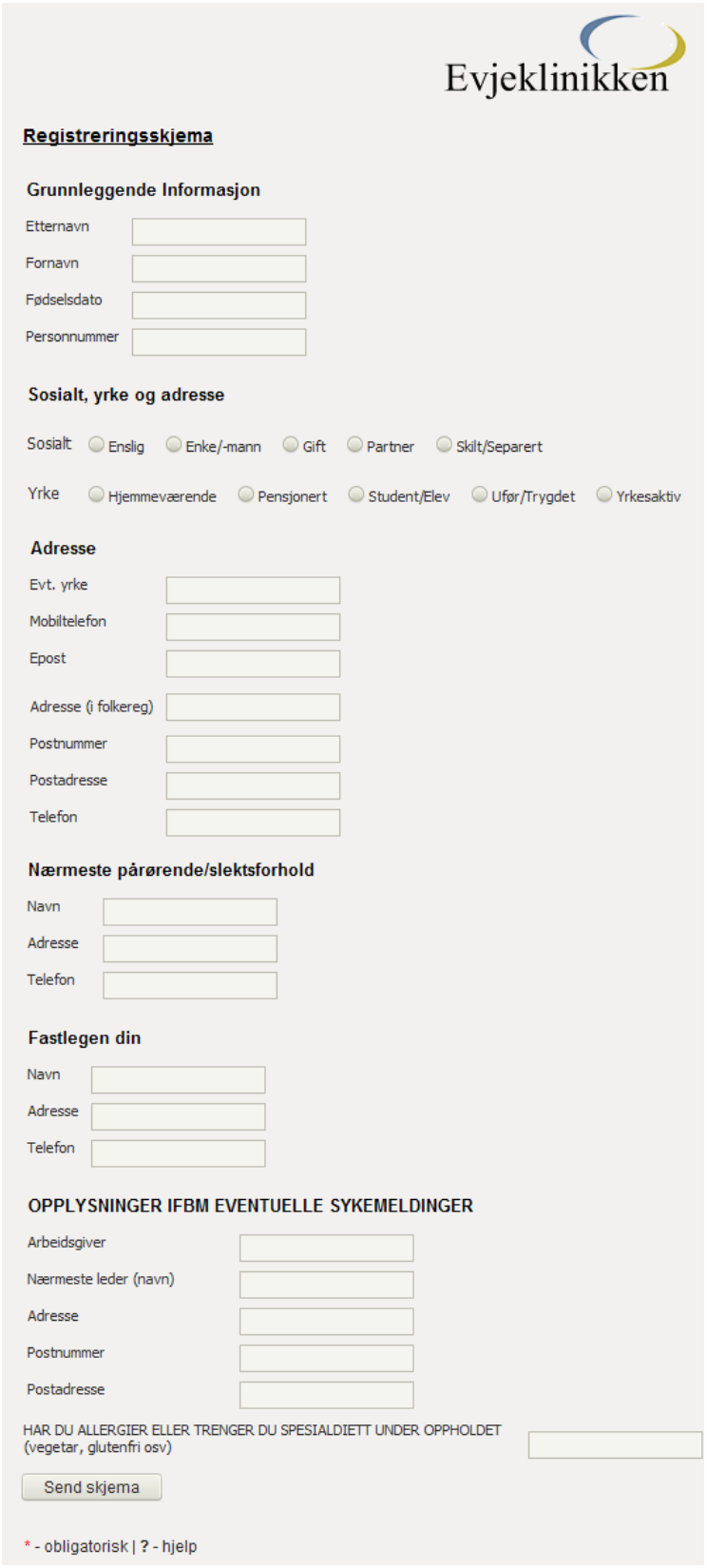
49. **Wikipedia.org.** IPSec. *Wikipedia.* [Internett] [Sitert: 23 mars 2007.] http://en.wikipedia.org/wiki/IPSec.
50. **Rolf Lunder og Michal Glowacki.** *SOMA Front End Internettportal.* Oslo : ITVerket AS, 2006.
51. **Sunnaas TRS.** *Noen "smakebiter" fra minTRSSIDe.* [Se http://trs.sunnaas.no/stream_file.asp?iEntityId=4336] Oslo : Sunnaas TRS, Sunnaas TRS, 2006.
52. **Wikipedia.org.** RC4. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/RC4_%28cipher%29.
53. —. RC2. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/RC2.
54. **Chiba Project.** Chiba. *Sourceforge.net.* [Internett] [Sitert: 15 05 2007.] http://chiba.sourceforge.net/.
55. **Wikipedia.org.** Brute force attack. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Brute_force_attack.
56. —. Wired Equivalent Privacy. *Wikipedia.* [Internett] [Sitert: 14 05 2007.] http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy.

Bøker:

"Information security – principles and practice"
Forfatter: Mark Stamp – San Jose State University
Forlag: Wiley-Interscience
2006
ISBN: 0-471-73848-4

"Beginning XML" 3rd Edition
Forfattere: David Hunter, Andres Watt, Jeff Rafter, Jon Duckett, Danny Ayers, Nicholas Chase, Joe Fawcett, Tom Graven, Bill Patterson
Forlag: Wiley Publishing, Inc
2004
ISBN: 0-7645-7077-3

Vedlegg A: Registreringsskjema



Evjeklinikken

Registreringsskjema

Grunnleggende Informasjon

Etternavn
Fornavn
Fødselsdato
Personnummer

Sosialt, yrke og adresse

Sosialt ○ Enslig ○ Enke/-mann ○ Gift ○ Partner ○ Skilt/Separert

Yrke ○ Hjemmeværende ○ Pensjonert ○ Student/Elev ○ Ufør/Trygdet ○ Yrkesaktiv

Adresse

Evt. yrke
Mobiltelefon
Epost
Adresse (i folkereg)
Postnummer
Postadresse
Telefon

Nærmeste pårørende/slektsforhold

Navn
Adresse
Telefon

Fastlegen din

Navn
Adresse
Telefon

OPPLYSNINGER IFBM EVENTUELLE SYKEMELDINGER

Arbeidsgiver
Nærmeste leder (navn)
Adresse
Postnummer
Postadresse

HAR DU ALLERGIER ELLER TRENGER DU SPESIALDIETT UNDER OPPHOLDET (vegetar, glutenfri osv)

Send skjema

* - obligatorisk | ? - hjelp

Vedlegg B: CD med alt produsert materiale

Innhold:

- Brukerhåndbok for MinJournal i 2007- og PDF-format
- Fullstendig stilark
- Rapporten i Word 2007- og PDF-format
- Utviklede skjemaer med tilhørende kode