

Informasjonsutveksling i helsesektoren

**Web-løsninger
som et alternativ**

**Versjon 2.0
Dato: 13.08.2003**

**KITH Rapport 05/03
ISBN 82-7846-168-6**

KITH-rapport

KITH
INFORMASJONSTEKNOLOGI
FOR ET BEDRE HELSEVESEN

TITTEL

Informasjonsutveksling i helsesektoren

Web-løsninger som et alternativ

VERSJON 2.0

Forfatter(e):

Edgar Glück og Olaf Berglihn

Oppdragsgiver(e)

Sosial- og helsedirektoratet

Postadresse

**Sukkerhuset
N-7489 Trondheim**

Besøksadresse

Sverresgt 15

Telefon

+47 - 73 59 86 00

Telefaks

+47 - 73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

Rapportnr.

R 05/03

URL

<http://www.kith.no/rapportarkiv/R05-03-Web-alternativ.pdf>

Prosjektnr.

ISBN

82-7846-168-6

Dato

13.08.2003

Antall sider

45

Kvalitetssikret av

Espen Stranger Seland

Gradering

Åpen

Godkjent av:

Jacob Hygen
Adm. Direktør

Sammendrag

Dette dokumentet beskriver alternative muligheter for elektronisk informasjonsutveksling mellom to parter med spesiell vekt på hvordan avanserte web-løsninger kan benyttes som et alternativ til tradisjonell EDI.

Rapporten beskriver ulike typer elektronisk kommunikasjon, deres egenskaper og egnethet for bruk i helsesektoren. Sikkerhetsmessige forhold er viet spesiell interesse.

Arbeidet er gjennomført som en del av Standardiserings- og samordningsprogrammet etter oppfordring fra Sosial- og helsedirektoratet.

Forord

Dette dokumentet er utarbeidet som en del av Standardiserings- og samordningsprogrammet.

Denne rapporten beskriver alternative kommunikasjonsformer for utveksling av informasjon med sikte på å avklare hva web-baserte løsninger er og hvor de best kan benyttes. Denne rapporten er første trinn i en slik avklaring.

Arbeidet er utført i en prosjektgruppe under ledelse av Edgar Glück og med representanter fra KITH.

KITH takker Sosial- og helsedirektoratet ved rådgiver Elisabeth Børgesen Mo for assistanse i forbindelse med utarbeidelse av rapporten.

Innhold

1	INNLEDNING	1
1.1	Bakgrunn	1
1.2	Hva skal utveksles	1
1.3	Om dette dokumentet	2
2	OVERSIKT OVER ULIKE TYPER ELEKTRONISK KOMMUNIKASJON	3
2.1	Typiske bruksområder	3
2.1.1	Overføring for gjenbruk i mottakers applikasjon.....	3
2.1.2	Overføring for manuell gjenbruk av bruker (person).....	3
2.1.3	Lokal tilgjengeliggjøring.....	4
2.2	Krav og tilgjengelighet av nødvendig utstyr	4
2.2.1	Bruk av allment tilgjengelig utstyr/programvare.....	4
2.2.2	Bruk av spesialtilpasset programvare	5
2.3	Krav til transport	5
2.3.1	Direkte kommunikasjon.....	5
2.3.2	Bruk av postkasse.....	5
3	BESKRIVELSE AV DE ENKELTE LØSNINGSALTERNATIVENE	7
3.1	Felles database	7
3.2	Elektronisk datautveksling (EDI)	8
3.3	Interaktiv EDI	8
3.4	E-post	9
3.5	Enkle web-løsninger	10
3.6	Avanserte web-løsninger	11
3.7	Kombinerte løsninger	12
4	LOVMESSIGE OG SIKKERHETSMESSIGE PROBLEMSTILLINGER	15
4.1	Web-løsninger i forhold til behandlingsrettede informasjonssystem	15
4.1.1	Lovverk	15
4.1.2	Konsekvenser for bruk av web-løsninger	17
4.2	Sikkerhetsmessige problemstillinger	18
4.2.1	Konfidensialitet.....	19
4.2.2	Integritet	19
4.2.3	Tilgjengelighet.....	20
4.2.4	Kvalitet	21
4.2.5	Bekreftelse på mottak med mer	21
4.2.6	Autentisering og tilgangsstyring	22
5	WEB-TJENESTER	25
5.1	Definisjon	25
5.2	EDI versus web-tjenester	26
5.3	Alternative web-tjenester	26
5.3.1	WSDL.....	26
5.3.2	ebXML.....	27

5.4	Bruk i helse- og trygde-sektoren	27
6	KONKLUSJONER	29
6.1	Løsningen må velges ut fra behovet	29
6.2	Web-løsninger nyttig for helsesektoren	29
6.3	Lovverket begrenser tilgang til pasientopplysninger	29
6.4	Web-tilgang alene ofte utilstrekkelig	30
6.5	Fortsatt behov for utveksling av strukturert informasjon	30
6.6	Helsenett fremfor Internett	30
6.7	Tilgangssystem for webtilgang er essensielt	31
6.8	Administrasjon av tilgang krevende	31
7	FORESLÅTTE AKTIVITETER	33
7.1	Anvendelsesområder for avanserte web-løsninger	33
7.2	Tilgangsrutiner	33
7.3	Regelverk for dokumentasjon av web-tilgang	33
7.4	Definisjon av BIEs for helsesektoren	33
7.5	Rammeverk for avanserte web-tjenester	34
7.6	Sikkerhet i eksisterende løsninger	34
7.7	Prosjekter for bruk av web-løsninger	34
8	REFERANSER	35
VEDLEGG A	SAMMENDRAG EGENSKAPER	37

1 Innledning

Dette kapitlet gir en kort beskrivelse av bakgrunnen for arbeidet, formålet med rapporten samt en kort oversikt over innholdet i dokumentet.

1.1 Bakgrunn

Sosial- og helsedirektoratet har, som en del av Standardiserings- og samordningsprogrammet, bedt KITH utrede hvordan web-baserte løsninger kan benyttes i helsesektoren. Web-baserte løsninger er imidlertid et relativt løst begrep som det er nødvendig å definere i relasjon til andre tilstøtende teknikker. I rapporten er det tatt utgangspunkt i at web-baserte løsninger er løsninger som baserer seg på bruk av web (web-løsninger).

KITH er først og fremst blitt anmodet om å vurdere om web- eller portalløsninger kan være et alternativ til tradisjonell meldingsutveksling mellom på forhånd autoriserte parter som kommuniserer og se på hva dette i tilfelle innebærer med hensyn til:

- sikkerhetsmessige problemstillinger (bl.a. forholdet mellom ytre og indre soner)
- autorisasjonsproblematikk (hvordan styre/beslutte hvem som får tilgang til hva, samt krav til loggføring)

Som et første trinn har KITH sett på ulike kommunikasjonsformer med sikte på å klargjøre begrepene og å identifisere styrker og svakheter ved de ulike løsningene. KITH har også sett på mulighetene for å benytte web-løsninger som et alternativ til tradisjonell EDI. Denne rapporten beskriver dette arbeidet.

Denne rapporten gir ikke svar på alle problemstillingene som bør belyses i forbindelse med bruk av web-løsninger i helsesektoren. Rapporten forsøker å peke på noen sentrale utfordringer slik at det skal være mulig å gå videre med mer konkrete problemstillinger. I kapittel 7 er det omtalt forslag til videre arbeide innenfor dette området.

1.2 Hva skal utveksles

Innenfor helsesektoren er det et utstrakt behov for å utveksle informasjon om individuelle pasienter som følge av at moderne pasientbehandling krever innsats av en lang rekke parter. Informasjonen som utveksles omfatter så vel fri tekst som

strukturert informasjon, bilder, lyd og video. Det er således et omfattende behov for å utveksle informasjon av nærmest ethvert slag både innenfor en institusjon og mellom institusjoner.

Fra et medisinsk faglig synspunkt vil pasientbehandlingen kunne bedres dersom all informasjon gjøres tilgjengelig til riktig tid der pasienten behandles. Forsvarlig og korrekt behandling er avhengig av at alle nødvendige opplysninger foreligger for behandlende lege, og ofte er de mest sensitive opplysningene av vesentlig betydning. På den annen side skal en respektere pasientens rettmessige krav om at pasientopplysninger ikke gjøres tilgjengelig for andre enn det som trengs for forsvarlig behandling. Videre kreves det av hensyn til personvernet og forsvarlig pasientbehandling at opplysningene ikke gjøres tilgjengelig for utenforstående eller endres/forvrenses under overføringen mellom involverte parter. For å oppfylle disse kravene er det behov for forholdsmessige sikkerhetsmekanismer som sikrer overføring av opplysningene.

1.3 Om dette dokumentet

Dokumentet er videre organisert som følger:

Kapittel 2 inneholder en oversikt over ulike typer elektronisk kommunikasjon

Kapittel 3 inneholder en beskrivelse av de ulike løsningsalternativene

Kapittel 4 beskriver lovmessige og sikkerhetsmessige problemstillinger, spesielt problemstillinger knyttet til behandlingsrettede informasjonssystem

Kapittel 5 inneholder en kortfattet beskrivelse av ”web-tjenester”

Kapittel 6 inneholder konklusjoner fra arbeidet

Kapittel 7 inneholder forslag til videre aktiviteter innenfor dette området

Kapittel 8 inneholder referanser

Vedlegg A inneholder en tabellarisk oversikt over de viktigste egenskapene til de ulike løsningene

2 Oversikt over ulike typer elektronisk kommunikasjon

Dette kapittelet gir en oversikt over egenskaper som er karakteristiske for ulike typer elektronisk kommunikasjon og løsninger for transport av informasjonen.

Hensikten er å gjøre informasjon som oppstår på ett sted tilgjengelig på et annet sted. Dette kan gjøres ved at informasjonen lagres ett sted og derfra gjøres tilgjengelig for andre eller ved at informasjonen fysisk overføres til andre steder for bruk på disse stedene. Hvilken teknikk som velges vil blant annet avhenge av hva slags informasjon det er og hva denne informasjonen skal brukes til.

2.1 Typiske bruksområder

Behovet for kommunikasjonsløsning kan variere betydelig avhengig av bruksområdet. Men i hovedsak kan en skille mellom noen få hovedtyper av bruk:

- 1 Overføring av informasjon for gjenbruk i mottakerens applikasjon
- 2 Overføring av informasjon for manuell gjenbruk av bruker (person)
- 3 Tilgjengeliggjøring av informasjon for lokal visning for bruker (person)

2.1.1 Overføring for gjenbruk i mottakers applikasjon

Dette omfatter fysisk flytting av informasjon hvor informasjonen befinner seg på et nytt sted (evt. i tillegg til det originale stedet) etter at kommunikasjonen er avsluttet.

For at en mottaende applikasjon skal kunne nyttiggjøre seg informasjonsinnholdet må informasjonen være strukturert på en måte som gir de kommuniserende partene en felles forståelse av de ulike delene av innholdet. Dette gir applikasjonen mulighet for å håndtere overført informasjon på lik linje med tilsvarende informasjon som er registrert direkte i systemet (interoperabilitet).

Eksempler på slike løsninger er EDI og enkelte avanserte web-løsninger hvor nettleseren er utstyr med en formålsspesifikk plug-in som er i stand til å ”forstå” informasjonen som utveksles (vanligvis betegnet ”web-basert EDI”).

2.1.2 Overføring for manuell gjenbruk av bruker (person)

Dette omfatter fysisk flytting av informasjon hvor informasjonen befinner seg på et nytt sted (evt. i tillegg til det originale stedet) etter at kommunikasjonen er avsluttet.

Ved at det her dreier seg om informasjon som overføres mellom brukere (mennesker) er det mulig å håndtere både fri tekst og strukturert informasjon uten at det på forhånd er avtalt hvordan ulike typer informasjon skal overføres. På samme måte som ved muntlig kommunikasjon mellom mennesker, er det fare for at mottatt informasjon blir misoppfattet.

Eksempel på en slik løsning er vanlig e-post.

Etter at informasjonen er overført kan mottakeren benytte informasjonen på lik linje med informasjon som er oppstått lokalt.

2.1.3 Lokal tilgjengeliggjøring

Det dreier seg her om kun å gjøre informasjon tilgjengelig mens kommunikasjonskanalen er åpen og hvor informasjonen etterpå kun befinner seg på det opprinnelige stedet.

I og med at det her kun dreier seg om å presentere informasjon for brukere (mennesker) er det mulig å håndtere både fri tekst og strukturert informasjon.

Eksempler på slike løsninger er databasetilgang via terminal(server) og enkle web-løsninger.

Informasjonen er vanligvis ikke lengre tilgjengelig hos mottaker etter at presentasjon av informasjonen er avsluttet. For web-løsninger vil mange nettlesere kunne lagre skjermbilder for gjentatt visning senere. Brukerne har også mulighet for manuelt å overføre informasjonselementer til egne applikasjonssystem (ved bruk av ”klipp og lim”), men siden dette er en manuell prosess er det begrenset hvor mye informasjon som i praksis kan håndteres på denne måten og løsningen er ikke egnet for rutinemessig bruk. Løsningen innebærer også en sikkerhetsrisiko ved at opplysningene utilsiktet kan bli ufullstendige eller forvrengte samt at opplysningene kan bli plassert på et feil sted.

2.2 Krav og tilgjengelighet av nødvendig utstyr

Behov for utstyr og programvare varierer også for de ulike alternativene. Grovt sett kan løsningene deles i to grupper:

- 1 Bruk av allment tilgjengelig utstyr/programvare
- 2 Bruk av spesialtilpasset programvare

2.2.1 Bruk av allment tilgjengelig utstyr/programvare

Denne gruppen omfatter bruk av felles database, e-post og enkle web-løsninger.

Slike løsninger kan i utgangspunktet benyttes umiddelbart av enhver bruker ved bruk av vanlig tilgjengelig programvare uten behov for spesiell tilpassing mot en tilgjengelig, eksisterende database eller webserver. Ved overføring av personidentifiserbar informasjon vil en måtte implementere nødvendige sikkerhetstiltak rundt overføringen, men slike sikkerhetsløsninger er også tilgjengelige. Det kan imidlertid være et organisatorisk overhead ved å ta i bruk slike sikkerhetsløsninger.

Kostnadene for klienten ved bruk av slike løsninger er vanligvis svært lave – noe høyere ved bruk av omfattende sikkerhetsmekanismer.

2.2.2 Bruk av spesialtilpasset programvare

Denne gruppen omfatter bruk av EDI, interaktiv EDI og avanserte web-løsninger.

For å sikre en felles semantisk forståelse av informasjonsinnholdet mellom avsender og mottaker må hvert enkelt informasjonselement defineres og entydig identifiseres. I og med at informasjonsinnholdet er spesifikt for det aktuelle applikasjonsområdet (i dette tilfellet helsesektoren) er dette ”skreddersøm” som er tid- og arbeids-krevende.

Det pågår imidlertid internasjonalt standardiseringsarbeide med sikte på å komme frem til felles løsninger slik at en kan få løsninger som i større grad kan gjenbrukes.

Kostnadene ved bruk av slike løsninger vil inntil videre være betydelige.

2.3 Krav til transport

De ulike løsningene stiller ulike krav til transporten, blant annet ut fra behovet for rask svartid. I hovedsak er det noen få hovedalternativ:

- 1 Direkte kommunikasjon
- 2 Bruk av postkasse

De ulike transportløsningene stiller også ulike krav til sikkerhetsløsninger.

2.3.1 Direkte kommunikasjon

En direkte kommunikasjon innebærer en etablerer direkte forbindelse mellom de kommuniserende partene. I noen tilfeller kan det være en direkte fysisk forbindelse ved bruk av lokal terminal eller bruk av en fast oppkopling. Mer vanlig i dag er en logisk forbindelse typisk ved bruk av TCP/IP. Det kan være nødvendig å åpne sikkerhetsløsninger som brannmur eller proxy for å kunne etablere direkte kommunikasjon.

Overføringstiden er typisk i størrelsesorden få sekunder.

Kommunikasjonskanalen stiller ikke krav til overføringens innhold, format eller benyttet syntaks. Kommunikasjonen kan foregå lokalt i en institusjon (LAN) eller mer globalt (WAN). Kommunikasjonen kan også foregå som et virtuelt lokalt (privat) nettverk innenfor et globalt nettverk (VPN).

Eksempler på løsninger som typisk bruker en slik løsning er felles databaser, interaktiv EDI og web-løsninger, men løsningen kan også benyttes for tradisjonell EDI og e-post. Løsningen benyttes også ved videokonferanser og annen dialogbasert kommunikasjon hvor begge kommunikasjonsparter er tilgjengelige samtidig.

2.3.2 Bruk av postkasse

Ved bruk av postkasser er det ingen gjennomgående kommunikasjonskanal fra avsender til mottaker. Avsender kommuniserer med et postkassesystem og avleverer sine meldinger der hvorpå mottaker etablerer en ny kommunikasjonskontakt med postkassesystemet periodisk eller ved behov for å hente nye meldinger. Mindre behov for direkte kontakt mellom partene gjør det enklere å skjerme partene for angrep fra utenforstående.

Kommunikasjonen har tidligere vært basert på X.400, men bruk av SMTP benyttes stadig mer. Begge alternativ kan operere side ved side ved bruk av gateways mellom de to løsningene og de fleste kommunikasjonssystem håndterer i dag både X.400 og SMTP.

Overføringstiden er typisk i størrelsesorden sekunder til minutter, men reell svartid er sterkt avhengig av hvor ofte mottaker sjekker om det er kommet post i hans postkasse.

Kommunikasjonsløsningen stiller ikke krav til meldingens innhold, format eller benyttet syntaks.

Løsningen benyttes først og fremst for EDI og e-post.

3 Beskrivelse av de enkelte løsningsalternativene

Dette kapitlet beskriver de viktigste egenskapene til hvert av de aktuelle løsningsalternativene.

For alle beskrevne løsninger forutsettes det at det finnes et avsendende applikasjons-system som kan sende nødvendig informasjon og likeledes at det finnes et mottaende applikasjonsystem som kan motta informasjonen der dette er aktuelt.

Et sammendrag av de viktigste egenskapene til de ulike løsningsalternativene finnes i Vedlegg A.

3.1 Felles database

På initiativ fra mottaker (klient) gjøres informasjon tilgjengelig gjennom et applikasjons-system (server) som henter data fra en tilknyttet database. Tilknytningen foregår enten via en fysisk forbindelse til en terminal eller via en logisk forbindelse ved bruk av en terminalserver.

Informasjon kan registreres, hentes frem og endres i sann tid. Tilgang reguleres ved brukerrettigheter i et tilgangskontrollsystem som en del av applikasjons-systemet.

Nødvendig utstyr/programvare er lett vint tilgjengelig uten større kostnader og løsningen kan raskt tas i bruk.

Typiske anvendelsesområder er tradisjonelt sykehusinterne system, men etter hvert også klient-server løsninger som kan omfatte felles databaser for flere sykehus med logisk adskillelse basert på et tilgangskontrollsystem.

Løsningen er egnet der det er behov for et stort antall aksesspunkter til en relativt lav kostnad for håndtering av mindre datamengder og varierte opplysninger.

Løsningens egnethet, for eksempel i forbindelse med elektronisk pasientjournal, er basert på applikasjons-systemets funksjonalitet og at informasjon fra andre kilder tilføres databasen (via EDI osv.).

Løsningen har i hovedsak mange av de samme egenskapene som enkle web-løsninger, men med den forskjell at brukerne vanligvis har en større tilhørighet til applikasjons-systemet.

3.2 Elektronisk datautveksling (EDI)

På initiativ fra sender ekstraheres informasjon fra lokal database til avsenders applikasjonssystem og sendes derfra strukturert ved bruk av en meldingssyntaks for innholdet (EDIFACT, XML osv.), en syntaks for overføringen (typisk MIME) og ved bruk av nødvendig sikkerhetsløsning. Mottaker får enten meldingen direkte, eller henter den fra en postkasse, og informasjonen overføres til mottakers applikasjonssystem.

Informasjon overføres i løpet av minutter og er senere tilgjengelig for bruk i mottakers applikasjonssystem på lik linje med opplysninger som er registrert lokalt.

EDI omfatter også sikkerhetsmekanismer for å kunne dokumentere hva som ble utvekslet mellom kommunikasjonspartene. Dette baserer seg på meldingslogger med opplysninger om meldingene som ble utvekslet og eventuelle kvitteringer samt en juridisk logg som oppbevares i noen måneder og som inneholder de detaljerte meldingene slik de ble utvekslet over kommunikasjonslinjen.

Løsningen krever spesiell tilpassing mellom brukers applikasjonssystem og de enkelte meldingene som benyttes og krever derfor en del forberedelse før løsningen kan tas i bruk. Av samme grunn er det også en del kostnader forbundet med ibruktakingen. Behovet for slik tilpassing forventes å kunne reduseres etter hvert som en tar i bruk bedre standardiserte dataelementer (Business Information Entities – BIEs).

Typiske anvendelsesområder er periodisk distribusjon av laboratoriesvar fra laboratorier til faste svarmottakere og utsending av epikriser fra sykehus til henvisende/innleggende lege.

Løsningen er egnet for regelmessig distribusjon av store datamengder av veldefinert informasjonsinnhold mellom faste kommunikasjonsparter med veletablert infrastruktur og hvor overført informasjon skal gjenbrukes i mottakers applikasjonssystem.

Løsningen er ikke egnet for kommunikasjonsparter som ikke har den nødvendige infrastruktur, hvor informasjonsinnholdet stadig endrer seg eller hvor kommunikasjonsbehovet er lite.

3.3 Interaktiv EDI

På initiativ fra mottaker (klient) rettes en forespørsel til en kommunikasjonspartner (server) som ekstraherer relevant informasjon fra databasen i sitt applikasjonssystem. Denne informasjonen sendes strukturert ved bruk av en meldingssyntaks for innholdet (EDIFACT, XML osv.), en syntaks for overføringen (typisk MIME) og ved bruk av nødvendig sikkerhetsløsning til mottaker hvor informasjonen overføres til mottakers applikasjonssystem. Dialogen kan repeteres mot samme eller en annen kommunikasjonspart.

Løsningen adskiller seg fra web-løsninger ved at det benyttes strukturerte meldinger og ikke HTTP, men avanserte web-løsninger har for øvrig en rekke fellestrekk med interaktiv EDI.

Informasjon overføres i tilnærmet sann tid og er senere tilgjengelig for bruk i mottakers applikasjonssystem på lik linje med opplysninger som er registrert lokalt.

Løsningen krever spesiell tilpassing mellom brukers applikasjonssystem og de enkelte meldingene som benyttes og krever derfor en del forberedelse før løsningen kan tas i bruk. Av samme grunn er det også en del kostnader forbundet med ibruktakingen. Også her vil bruk av bedre standardiserte dataelementer (BIEs) kunne redusere behovet for tilpassing.

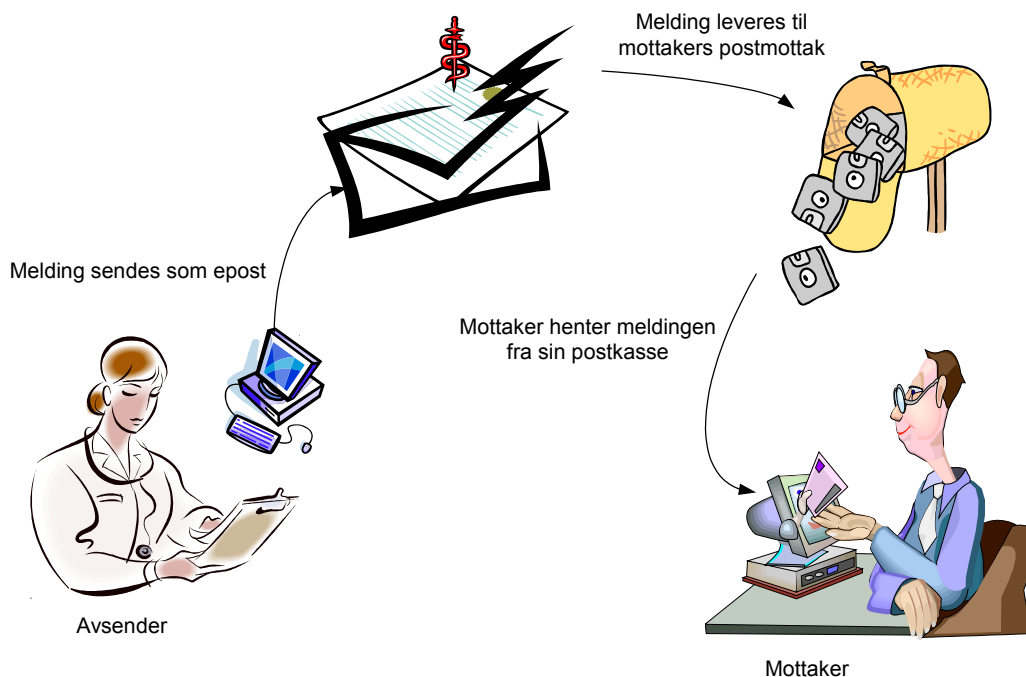
Typiske anvendelsesområder er bestilling av varer og tjenester som krever en dialog mellom partene for å finne frem til riktig ”produkt”, for eksempel flyreiser eller timebestilling av røntgenundersøkelser. Klienten er tilknyttet sitt applikasjonssystem som kommuniserer med en eller flere applikasjonsservere.

Løsningen er egnet for gjentatte forespørsler med et veldefinert informasjonsinnhold av begrenset omfang mellom faste kommunikasjonsparter med veletablert infrastruktur (reisebyrå, legekantor) og hvor overført informasjon skal gjenbrukes i klientens applikasjonssystem.

Løsningen er ikke egnet for kommunikasjonsparter som ikke har den nødvendige infrastruktur (pasienten selv), hvor informasjonsinnholdet stadig endrer seg eller hvor behovet for kommunikasjon kun forekommer en gang i blant.

3.4 E-post

På initiativ fra sender skrives informasjonen inn som fri tekst ved bruk av avsenders e-post klient og sendes ved bruk av en syntaks for overføringen (typisk MIME) og ved bruk av nødvendig sikkerhetsløsning. Mottaker henter meldingen, vanligvis fra en postkasse, og informasjonen presenteres ved bruk av mottakers e-post klient. Meldingen kan også ha vedlegg av nærmest vilkårlig slag, men produksjon av vedlegget samt lesing av dette hos mottaker kan kreve egen programvare.



Figur 1: E-post

Informasjon overføres i løpet av minutter og er senere tilgjengelig for bruk i mottakers e-postsystem på lik linje med opplysninger som er registrert lokalt.

Nødvendig programvare er lettvinntilgjengelig uten større kostnader og løsningen kan raskt tas i bruk, inklusiv vanlig benyttede sikkerhetsløsninger.

Typiske anvendelsesområder er tradisjonell e-post og eventuell sikker e-post.

Løsningen er egnet for sending av mindre dokumenter med vilkårlig innhold (og eventuelt med vedlegg begrenset i størrelse til noen Mb) til varierende kommunikasjonsparter uten større krav til utstyr eller driftskostnader. Behovet for samspill med andre applikasjoner hos mottaker kan håndteres av ”klipp og lim”.

Løsningen er ikke egnet for større og hyppige distribusjoner av informasjon eller hvor informasjonen regelmessig skal gjenbrukes hos mottakeren.

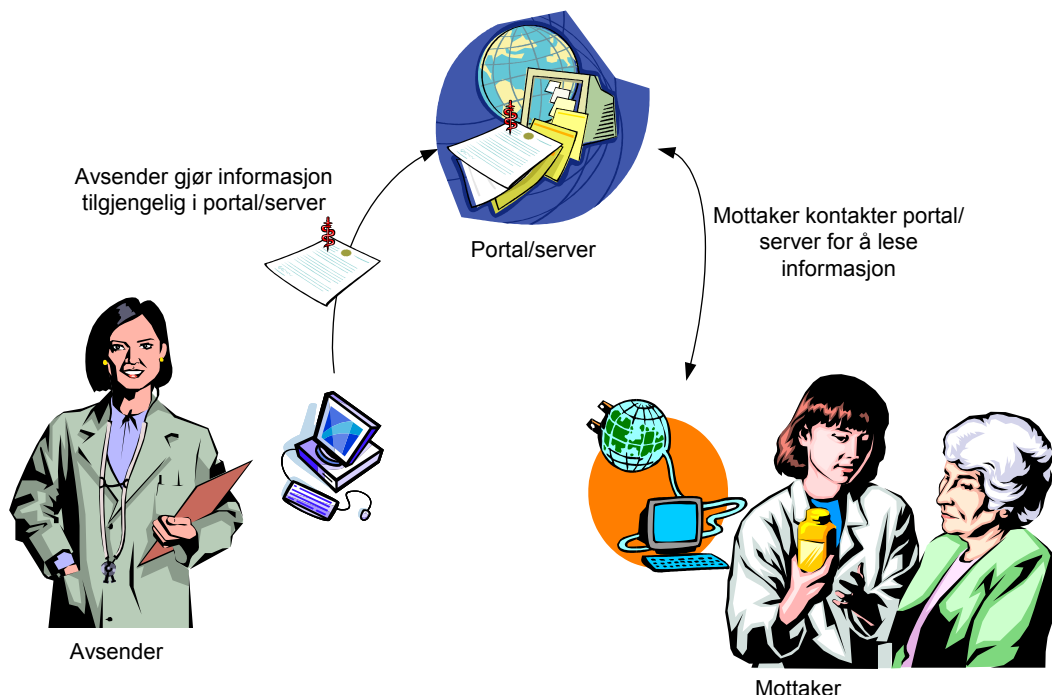
3.5 Enkle web-løsninger

Med ”enkle” web-løsninger menes vanlige web-løsninger hvor klienten kun forutsettes å ha en vanlig nettleser med allment tilgjengelige plug-ins og hvor opplysningene som gjøres tilgjengelig blir håndtert av en bruker (person).

På initiativ fra mottaker (klient) gjøres etterspurt informasjon tilgjengelig gjennom et applikasjonssystem (server) som henter data fra en tilknyttet database. Tilknytningen foregår via en logisk forbindelse i et åpent eller lukket nett.

Informasjon kan registreres, hentes frem og eventuelt endres i sann tid. Tilgang reguleres ved brukerrettigheter i et tilgangskontrollsystem tilknyttet serveren.

Nødvendig programvare er lettvinntilgjengelig uten større kostnader og løsningen kan raskt tas i bruk.



Figur 2: Web-løsning

Typiske anvendelsesområder er fremhenting av generelt tilgjengelig informasjon, for eksempel publikumsinformasjon. For helsesektoren spesielt kan det være aktuelt med timebestilling fra pasienten selv, melderutiner for avviks- og uhellsrapportering eller fremhenting av pasientopplysninger (i den utstrekning gjeldende lovverk tillater dette).

Løsningen er egnet for en vilkårlig bruker og krever ikke tilgang til spesielt utstyr. Løsningen gir brukeren mulighet for å kunne orientere seg om informasjon som enten er fritt tilgjengelig eller som brukeren har fått spesiell tilgang til. Det er mulig å bestille varer og tjenester hos leverandører som tilbyr slik tjenester. Løsningen er egnet for brukere som har et begrenset kommunikasjonsbehov og hvor det gjerne er stor variasjon i den informasjon som etterspørres.

Løsningen kan være egnet for fremhenting av enkle pasientopplysninger, for eksempel på ferie eller andre reiser, men det er tvil om hvor langt dette lar seg gjennomføre med dagens lovverk. Uansett vil løsningen være en dårlig erstatning for et avansert journalsystem hvor tilgjengelig informasjon kan sammenstilles og presenteres på ulike måter ut fra brukerens behov. Løsningen er heller ikke egnet som et rutinemessig hjelpemiddel i pasientbehandlingen hvor helsepersonellet i etterhånd vil ha behov for å kunne dokumentere hvilken informasjon som lå til grunn for deres handlinger.

Løsningen er ikke egnet for omfattende og hyppig distribusjon av informasjon eller hvor informasjonen regelmessig skal gjenbrukes hos klienten.

3.6 Avanserte web-løsninger

Med ”avanserte web-løsninger” menes web-løsninger hvor klienten i tillegg til en vanlig nettleser også må ha egne plug-ins som er spesielt utviklet for det aktuelle bruksområdet og hvor opplysningene som hentes eventuelt kan bli overført til klientens eget applikasjonssystem. I enkelte tilfeller er nettleseren funksjonelt integrert i annen programvare.

På initiativ fra mottaker (klient) gjøres etterspurt informasjon tilgjengelig gjennom et applikasjonssystem (server) som henter data fra en tilknyttet database. Tilknytningen foregår via en logisk forbindelse i et åpent eller lukket nett.

Informasjon kan registreres, hentes frem og eventuelt endres i sann tid. Tilgang reguleres ved brukerrettigheter i et tilgangskontrollsystem. Ved bruk av spesielt tilpassede plug-ins kan informasjon overføres til og fra klientens applikasjonssystem hvor mottatte opplysninger senere er tilgjengelig for bruk i mottakers applikasjonssystem på lik linje med opplysninger som er registrert lokalt. Løsningen kan på denne måten tilby et vidt spekter av funksjonalitet, herunder også EDI-funksjonalitet.

Løsningen krever spesiell tilpassing mellom brukers applikasjonssystem og de enkelte meldingene som skal benyttes og krever derfor en del forberedelse før løsningen kan tas i bruk avhengig av løsningens omfang og funksjonalitet på lik linje med annen programutvikling. Av samme grunn er det også en del kostnader forbundet med ibruktakingen. Behovet for slik tilpassing forventes å kunne reduseres etter hvert som en tar i bruk bedre standardiserte dataelementer (Business Information Entities – BIEs).

Avanserte web-løsninger er en heterogen gruppe med mange ulike typer funksjonalitet. Det er her fokusert på aspekter som gjelder overføring av informasjon og tilgjengeliggjøring av denne hos mottaker. Det pågår mye arbeide i forsøk på å lage et mer generelt rammeverk for slike typer tjenester (web-tjenester) for å gjøre denne teknologien mer generelt anvendelig og samtidig senke kostnadene ved å ta en slik løsning i bruk. Slik tilpassing har startet innenfor området elektronisk handel (e-commerce) og det vil ventelig ta tid før generelle løsninger kan tilbys helsesektoren.

Denne type løsninger er foreløpig lite utbredt i helsesektoren.

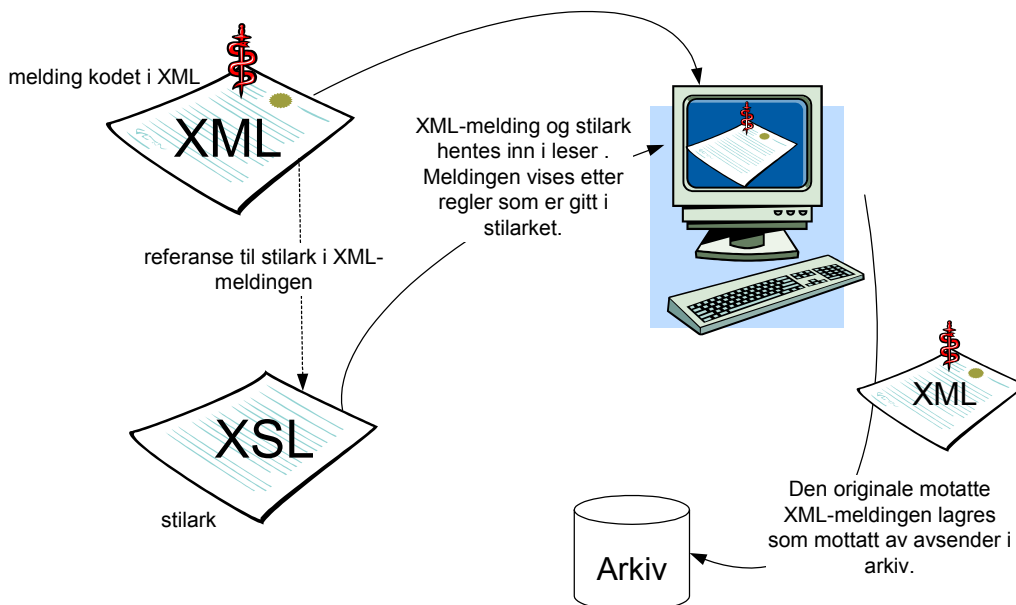
Løsningen er potensielt egnet for mange ulike formål avhengig av de applikasjoner (plug-ins) som blir benyttet. Løsningen kan være et alternativ til tradisjonell EDI og kan på sikt tilby løsninger til større brukergrupper forutsatt at det blir utviklet nødvendige applikasjoner. Det må vurderes nærmere hvor det vil være mest formålstjenlig å anvende slike løsninger siden programutviklingskostnader må veies mot funksjonalitet.

Generelt er løsningen best egnet for mange-til-en kommunikasjon som for eksempel sentral innrapportering.

Løsningene som er antydnet under enkle web-løsninger kan også være aktuelle dersom det er nødvendig med tilleggsfunksjonalitet og/eller integrering med klientens applikasjonssystem, for eksempel timebestilling, fornyelse av resept og innrapportering av ulike opplysninger.

3.7 Kombinerte løsninger

Avanserte web-løsninger er som nevnt en heterogen gruppe som til tider også kombineres med andre løsningsalternativ, for eksempel e-post.



Figur 3: XML og XSL

En annen kombinasjon omfatter EDI ved at informasjonen sendes strukturert i form av en XML-melding sammen med en styrefil som bestemmer hvordan informasjons-

innholdet skal vises i brukerens nettleser. Bruken av et rikt semantisk format sammen med styrefil (XML + CSS/XSL) gir muligheten for å styre brukergrensesnitt og layout, samtidig som brukeren har tilgang til kildefilen og kan kontrollere, arkivere og prosessere denne i sitt applikasjonssystem. For helsesektoren vil slike løsninger ventelig kunne være et godt alternativ.

Det er også mulig å kombinere web-løsninger og EDI på andre måter ved at web-siden benyttes for å orientere seg om tilgjengelig informasjon eller registrer forespørsler etter informasjon mens den aktuelle informasjonsoverføringen foregår ved bruk av tradisjonell EDI. Slike løsninger er nærmere diskutert i neste kapittel.

4 Lovmessige og sikkerhetsmessige problemstillinger

Dette kapittelet beskriver sikkerhetsmessige problemstillinger ved bruk av elektronisk kommunikasjon generelt og spesielt problemstillinger knyttet til bruk av web-løsninger mot behandlingsrettede informasjonssystemer.

4.1 Web-løsninger i forhold til behandlingsrettede informasjonssystem

4.1.1 Lovverk

Hovedregelen og grunnlaget for all pasientbehandling, herunder behandling og utlevering av pasientinformasjon, bygger på at pasienten samtykker. Et samtykke kan i noen tilfeller anses for underforstått.

Helseregisterloven – Tilgang til opplysninger innenfor en institusjon

Tilgang til helseopplysninger reguleres av helseregisterloven [9] § 13 som angir 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".

Helseregisterloven definerer databehandlingsansvarlige som "den som bestemmer formålet med behandlingen av helseopplysningene og hvilke hjelpemidler som skal brukes, hvis ikke databehandlingsansvaret er særskilt angitt i loven eller i forskrift i medhold av loven". Databehandlingsansvarlig for behandlingsrettede informasjonssystem vil for eksempel være et helseforetak. Det er for øyeblikket usikkert om også det regionale helseforetaket kan være databehandlingsansvarlig. Spørsmålet er forelagt Datatilsynet og Sosial- og helsedirektoratet avventer en uttalelse fra Datatilsynet. Sannsynligvis vil imidlertid ikke et regionalt helseforetak kunne være databehandlingsansvarlig, slik at tilgang til informasjon mellom foretakene alltid må regnes som utlevering.

Når et helseforetak regnes for å være databehandlingsansvarlig, vil helseopplysninger kunne gjøres tilgjengelig mellom sykehusene i det samme helseforetaket "i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt" ifølge helseregisterloven § 13 siste setning.

Databehandler er i følge helseregisterloven, en juridisk eller fysisk person utenfor den databehandlingsansvarliges virksomhet som ikke har et selvstendig formål med behandlingen, f.eks. en datasentral eller en som utelukkende bearbeider dataene til forskningsformål på vegne av den databehandlingsansvarlige. Dette begrepet vil være av mindre interesse i forbindelse med vurdering av tilgang til behandlingsrettede informasjonssystem for helsepersonell som er involvert i behandling av den pasienten opplysningene vedrører.

En lege som fører eller leser journalen vil i helseregisterlovens forstand ikke være databehandler, men en som arbeider under helseforetakets instruksjonsmyndighet. Med instruksjonsmyndighet menes i denne sammenheng at det foreligger et arbeidsgiver-arbeidstakerforhold. Tilgang til opplysninger for andre enn de som er nevnt i helseregisterloven § 13, eksempelvis et annet helseforetak innenfor eller utenfor regionen, vil anses som utlevering av opplysninger. Slik utlevering må ha hjemmel.

Helsepersonelloven – Utlevering av opplysninger til annen institusjon

Helsepersonell har et legitimt behov for å få utlevert relevante helseopplysninger om pasienten fra tidligere omsorgsepisoder og dette er ofte også en forutsetning for adekvat behandling av pasienten. Dette reguleres av helsepersonelloven [10] § 45 som angir at "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."

Helsepersonelloven § 22 åpner for at pasienten kan samtykke i at helseopplysninger utleveres: "Taushetsplikt etter § 21 er ikke til hinder for at opplysninger gjøres kjent for den opplysningene direkte gjelder, eller for andre i den utstrekning den som har krav på taushet samtykker.". Det antas at slikt samtykke skal gjelde mer eller mindre konkrete opplysninger, men ikke pasientens nåværende og fremtidige helseopplysninger uspesifisert.

Helsepersonelloven § 25 første ledd åpner for at helseopplysninger kan utleveres 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."

Håndheving av lov- og regelverk

Det er også ansett som tillatt i helsesektoren at helsepersonell i nødsituasjoner får tilgang til helseopplysninger som vedkommende normalt ikke har tilgang til ("Blålysfunksjon") dersom dette er nødvendig for å kunne gi adekvat behandling av pasienten. Det vil da være vedkommende helsepersonells ansvar å kunne begrunne dette i ettertid.

Lovverket forutsetter således at helseopplysninger skal kunne utveksles, men setter strenge krav til når dette er lovlig å gjøre. Mens det er rimelig kurant å verifisere personers formelle rettigheter, er det atskillig vanskeligere for et automatisert system

å avgjøre om utlevering av opplysninger er nødvendig for vedkommendes arbeid og i tilfelle hvilke opplysninger som er nødvendige.

Dette reiser både tekniske og juridiske utfordringer når det gjelder å finne frem til hensiktsmessige løsninger for å kunne yte pasientene optimal behandling innenfor rammen av lovverket. I det følgende punkt 4.1.2 vil vi skissere hvilke umiddelbare konsekvenser dette medfører for bruk av web-løsninger.

Dersom helsevesenet finner at det nåværende lovverket ikke er hensiktsmessig for å kunne yte pasientene optimal behandling må en i tilfelle vurdere om det kan være aktuelt å endre gjeldende lov- og/eller regelverk. Dette vil i så fall forutsette saklige vurderinger etter en grundig utredning av forhold som måtte tale både for og imot.

4.1.2 Konsekvenser for bruk av web-løsninger

Web-løsninger kunne tenkes benyttet for å gjøre pasienters helseopplysninger (Pasientjournalen – EPJ) lettere tilgjengelig for andre instanser enn der pasienten alt er under behandling. Ved bruk av slike løsninger kunne pasientopplysninger gjøres umiddelbart tilgjengelig for behandlende helsepersonell når pasienten blir syk på reiser eller må få behandling fra andre instanser enn de pasienten tidligere har benyttet.

Slik tilgang/utlevering kan bare skje såfremt det er i samsvar med gjeldende bestemmelser om taushetsplikt og personvernregler. For at en slik tilgang skal være lovlig under dagens forståelse av regelverket kreves det enten at pasienten på forhånd har gitt sitt samtykke til uthenting av de konkrete opplysningene, eller at det eksisterer et avansert tilgangskontrollsystem som er i stand til å verifisere om lovens krav for utlevering av opplysningene er oppfylt i det konkrete tilfellet. Det finnes i dag adgangskontrollsystem som kan verifisere (autentisere) at den som etterlyser opplysningene er autorisert for håndtering av helseopplysninger, men det finnes neppe løsninger i dag som kan bekrefte eller dokumentere at vedkommende i den konkrete situasjonen har et berettiget krav på utlevering. Dagens automatiserte systemer kan neppe verifisere at parten er involvert i behandling av den aktuelle pasienten og at de etterspurte opplysningene er nødvendige for å kunne gi helsehjelp på forsvarlig måte, jf. helsepersonelloven § 45.

I praksis vil en i dag kreve at en forespørsel om utlevering av opplysninger fra en ny part som behandler en pasient, er begrunnet og at forespørselen legges frem for en person hos avgivende instans som er bemyndiget til å håndtere slike forespørsler om hvorvidt utlevering kan skje. Forespørselen kan fremføres pr. telefon, fax, sikker e-post eller brev, men også via web. Dette innebærer at det blir en svartid som kan variere fra minutter til dager, men en får ikke opplysninger i løpet av sekunder slik en web-løsning kunne gitt.

Et annet problem er at mottaker vil måtte kunne dokumentere i sitt eget informasjonssystem hvilke opplysninger vedkommende eventuelt er blitt gitt tilgang til og som følgelig vil være av betydning for den videre behandling av pasienten. Dette krever i praksis at opplysningene ikke bare gjøres tilgjengelig på en dataskjerm for den som etterspør opplysningene, men at opplysningene i tillegg overføres til vedkommendes eget informasjonssystem.

Selv om direkte tilgang til fullstendige pasientopplysninger på web ikke tillates nå, vil web-løsninger likevel kunne spille en betydelig rolle i å lette utveksling av pasientopplysninger. En web-løsning kan være et godt alternativ for å håndtere forespørsler etter pasientopplysninger ved å tillate registrering av nødvendige opplysninger for at avgiver skal kunne vurdere spørrerens rettmessige krav på å få overført opplysningene. Web-stedet vil kunne formidle forespørselen til den eller de steder som har opplysninger som er etterspurt. Det enkelte sted vil så måtte vurdere henvendelsen og eventuelt sende etterspurte opplysninger tilbake til spørreeren. En slik oversendelse foregår antakelig best ved bruk av en eksisterende EDI-melding som for eksempel en epikrise eller en journalmelding, men også sikker e-post kan være et alternativ i visse tilfeller.

Som nevnt gir lovverket mulighet for utlevering av helseopplysninger med pasientens samtykke. Selv om et generelt samtykke til utlevering av all nåværende og fremtidig informasjon neppe aksepteres kan en tenke seg løsninger hvor pasienten gir sitt samtykke til utlevering av et begrenset og på forhånd avtalt sett av opplysninger. Slike datasett kan være:

- "Kjernejournal" som er godkjent av pasienten
- Historikk over tidligere omsorgsepisoder
- Epikriser fra tidligere omsorgsepisoder
- Laboratoriesvar med nye undersøkelsesresultat og relevante historiske opplysninger
- Aktuell medikasjon ved siste kontakt

Slike opplysninger kan lettvis sendes automatisk i form av EDI-meldinger eller avanserte web-løsninger som svar på en forespørsel som er formidlet via web.

Det kan også tenkes løsninger hvor kun pasienten selv har web-tilgang til opplysningene og hvor pasienten kan uttrykke sitt samtykke til utlevering av opplysninger til tredjepart ved å anvende sitt private passord (for eksempel i form av en kode på et pasientkort) eller elektroniske signatur. Det kan imidlertid være begrensninger i hvilke opplysninger pasienten selv har innsyn i.

4.2 Sikkerhetsmessige problemstillinger

Enhver behandling av pasientopplysninger, herunder overføring, må ivareta nødvendig teknisk og organisatorisk informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet, jf. helseregisterloven § 16. Vektlegging av de ulike sikkerhetsmomentene er imidlertid noe annerledes for en kommunikasjonsløsning enn for selve informasjonsbehandlingen i endesystemene.

Organisatorisk informasjonssikkerhet knytter seg i denne sammenheng særlig til beslutningsmyndighet og -prosesser i forbindelse med autorisasjon av brukere for tilgang til opplysninger. Vi vil imidlertid i det følgende hovedsakelig konsentrere oss om teknisk informasjonssikkerhet ved elektronisk kommunikasjon.

De forskjellige kommunikasjonsformene har ulike egenskaper og de kan derfor også ha ulikt behov for ulike sikkerhetsmekanismer. Det er til dels et avhengighetsforhold

mellom de ulike sikkerhetsmekanismene, for eksempel ved at kryptering av en melding sikrer både konfidensialitet og integritet.

Sikkerhet kan bygges opp omkring hele utvekslingen som overføres og/eller hvert av de informasjonselementene som inngår i en enkelt melding. I denne sammenheng legges det først og fremst vekt på sikring av selve meldingsinnholdet.

4.2.1 Konfidensialitet

Konfidensialitet innebærer at informasjoninnholdet ikke blir tilgjengelig for uvedkommende (uautorisert innsyn). Ved elektronisk overføring må informasjonen sikres ved kryptering eller på annen måte, for eksempel midlertidig aidentifisering¹. Kryptering kan benyttes for alle nevnte kommunikasjonsformer.

Kryptering kan foretas på tre nivåer:

- beskyttelse av meldingsinnhold
- beskyttelse av meldingstransport på nivå til meldingsprotokoll
- beskyttelse av nettverksforbindelse

Hvilke av disse mekanismene (en eller flere) som benyttes er noe avhengig av hvilken overføringsmetode som benyttes.

Beskyttelse av meldingsinnhold ved kryptering sikrer at meldingen er uleselig for uvedkommende helt frem til den endelige mottakeren. Dette er i de fleste tilfeller den sikreste metoden.

Alternativt eller i tillegg kan overføringen krypteres på nivået til meldingsprotokoll, men sikringen gjelder da bare mellom avsendersystemet og frem til mottaker-systemet (postmottak for e-post, kommunikasjonsprogramvare for EDI). Dette er imidlertid tilsvarende til det som vanligvis gjøres ved kryptering av meldingsinnholdet i EDI-meldinger.

Ved web-løsninger og bruk av nettleser vil sikring på nivå til meldingsprotokoll (HTTP/TLS²) beskytte informasjonsutvekslingen hele veien mellom avsender og mottaker så fremt det ikke benyttes en proxy.

Beskyttelse av nettverksforbindelse ved bruk av dedikerte linjer eller VPN skjermer trafikken fra uvedkommende, men alle med tilgang til linjene eller VPN'et vil også ha mulighet for å avlytte kommunikasjonen.

Med tradisjonell EDI og bruk av PKI [2] vil adgangen til krypterte meldinger være styrt av sertifikater og tilhørende private nøkler. PKI og sertifikater kan også benyttes til adgangskontroll mot web, men det er mer vanlig å benytte brukernavn og passord.

4.2.2 Integritet

Med integritet menes det her teknisk informasjonsintegritet, dvs. at informasjoninnholdet ikke blir endret som følge av tilsiktede uautoriserte eller utilsiktede autoriserte handlinger. Dette kan forekomme enten ved at mennesker eller systemer

¹ For eksempel hvor personidentifikator sendes adskilt fra selve personopplysningene.

² Også betegnet HTTPS.

(programvare, maskinvare, nettverk, etc.) feilbehandler data, eller ved at personer eller systemer urettmessig får tilgang til å endre eller slette informasjon.

Fingeravtryksalgoritmer (hash-algoritmer)³ og krypteringsmekanismer som digitale signaturer og innholdskryptering, er de mest vanlige måtene å sikre integritet på. Sikringen sørger for at mottaker kan kontrollere at meldingsinnholdet ikke er endret under transporten fra avsender.

Sikring av integritet ved programvarens behandling av data er vanskeligere å kontrollere. Data som brukeren gir til programmet kan feilaktig modifiseres av programvaren i prosessen frem til og med kryptering/signering og oversendelse. På samme måte kan data feilaktig behandles av mottakers programvare og gi feilaktig eller misvisende informasjon til mottaker. Testing av programvare og krav til utviklingsmetode er virkemidler for å få korrekt fungerende programvare som reduserer faren for tap av integritet.

For web-løsninger generelt er det mer vanlig at informasjonen pakkes avhengig av layout og at den rike semantiske informasjonen (for eksempel i form av den tilgrunnliggende XML-melding) ikke lenger er tilgjengelig. Det kan være tilfredstillende for presentasjon av informasjonen, men lar seg vanskelig forene med bruken av digitale signaturer eller fingeravtrykk. Informasjonens integritet kan da ikke uten videre kontrolleres eller sammenholdes med arkivert informasjon hos mottakeren. Informasjonen som presenteres på web vil også kunne endres ved skifte av brukergrensesnitt og layout som ytterligere kan forvanske kontrollen av meldingens integritet.

4.2.3 Tilgjengelighet

Et viktig sikkerhetsmessig aspekt er at informasjonen må være tilgjengelig når brukeren har behov for denne informasjonen, dvs. på den tid, det sted og i det omfang det er nødvendig. Dette stiller både krav til sikkerhet for at informasjon ikke går tapt for godt og til at informasjonen er tilgjengelig i det daglige. Sikkerhetskopier på elektroniske medier og/eller papir vil ivareta at informasjonen ikke går tapt for godt, mens tilgjengeligheten i det daglige avhenger av den tekniske løsningen som er benyttet for å gi brukerne tilgang til opplysningene. Ved bruk av lokale løsninger innebærer dette at det lokale applikasjonssystemet må være operativt. For henting av informasjon fra avsenders system (portal) vil mottaker være avhengig av at nettverksforbindelsen og alle delsystemer mellom seg og avsender er i normal drift.

En alminnelig internett-forbindelse vil normalt ikke kunne anses som tilstrekkelig for å tilgjengeliggjøre tidskritisk informasjon. Lukkede helsenett med mekanismer som sikrer redundans og høy oppetid vil redusere risikoen for at informasjon er utilgjengelig i kritiske situasjoner.

Med mindre det benyttes varslingstjenester over e-post eller andre kanaler så vil ikke mottaker få beskjed om at ny informasjon er tilgjengelig i avsenders system/portal. Mottaker må selv aktivt sjekke for ny informasjon hvis slik varsling ikke gis.

³ Også kalt hash-funksjoner. SHA-1 og MD5 er algoritmene som er mest brukt.

4.2.4 Kvalitet

Kvalitet innebærer at opplysningene til enhver tid må være korrekte og oppdaterte samt relevante og tilstrekkelige som grunnlag for beslutninger. Kvaliteten av opplysningene i forbindelse med kommunikasjonsløsninger sikres først og fremst hos avsender av informasjonen. Kommunikasjonsløsningens oppgave er å bibeholde kvaliteten ved hjelp av teknikker som omtalt under 4.2.2 ovenfor.

EUs personverndirektiv fra 1995 stiller krav til kvalitet og integritet av personopplysningene. Dette direktivet er relevant for Norge og er implementert gjennom personopplysningsloven og helseregisterloven. Direktivet fremmer krav om at dersom det er nødvendig å korrigere et informasjonselement så skal tilsvarende endringer også gjennomføres på alle steder hvor informasjonen er blitt overført til. Dette innebærer en utfordring for de tilfeller hvor informasjonen er fysisk overført. Ved tradisjonell EDI overføres en melding fra avsender til mottaker. Etter at meldingen har forlatt avsender har avsender ikke lenger teknisk kontroll på hvordan mottaker behandler informasjonen som er overført. Avsender har derfor ikke mulighet for tilbaketrekking av informasjon eller å kontrollere bruken av informasjonen i en melding etter at den er mottatt, men kan måtte varsle mottaker ved senere å sende endringsmeldinger.

Avsender kontrollerer i større grad informasjonen når mottaker aktivt må hente den i en portalløsning eller annet system hos avsender. Avsender har muligheten til å angre på tilgang til informasjon helt frem til mottaker forsøker å hente den. Avsender kan også få oversikt over hvilken informasjon mottaker har hentet ut fra logg over uthentet informasjon.

Rutinene beskrevet ovenfor beskriver overføring av informasjon og har ingen direkte føring for hvordan mottaker eller mottaende applikasjon skal forholde seg til endringsmeldinger. Mottaker og mottaende applikasjon må forholde seg til det regelverk som gjelder, for eksempel i forhold til endring eller sletting av pasientopplysninger.

4.2.5 Bekreftelse på mottak med mer

Kravet til informasjonssikkerhet innebærer et ansvar for gode sikkerhetsmessige løsninger helt frem til og med mottaker. Det betyr at det i forbindelse med risikovurderingen også må ta i betraktning mottakerens sikkerhetssystem. Det blir også viktig å enes om når informasjonen kan betraktes som mottatt av mottaker og om det må benyttes tilbakemelding i form av kvittering for å få bekreftet at mottaker har gjort seg kjent med innholdet. En loggføring hos avsender alene av informasjonen som er overført vil neppe kunne benyttes som en bekreftende kvittering. Kvitteringen bør kunne kontrolleres i ettertid, og det krever digital signatur. Dagens EDI-rutiner med kryptert logg (juridisk logg) både hos avsender og mottaker ivaretar disse kravene.

Det er ikke imidlertid like klart på hvilket tidspunkt mottaker får ansvaret for informasjonen som overføres ved bruk av web-løsninger. Det har til nå ikke vært vanlig å stille samme krav til for eksempel logging som ved tradisjonelle EDI-løsninger, men dette kan bli nødvendig for bruk av web-løsninger i helsesektoren. Dette kan vanskelig løses i praksis dersom systemet til avsender ikke tilbyr et format som egner seg for arkivering hos mottaker.

Ved overføring av pasientopplysninger kan mottakere som er helsepersonell også være lovmessig forpliktet til å arkivere mottatt informasjon lokalt. Dette kan kreve at informasjon som gjøres tilgjengelig på web også må kunne overføres til mottakers applikasjonssystem.

4.2.6 Autentisering og tilgangsstyring

Autentisering og tilgangsstyring er nødvendig når en kommunikasjonspart skal hente informasjon i avgivers system eller et system som er felles for både avgiver og mottaker. Med autentisering menes kontroll av en brukers identitet. Tilgangsstyring omfatter mekanismene som skal sikre tilgangen til de rette funksjoner og informasjonsobjekter for et begrenset sett av brukeridentiteter. Det vises for øvrig til gjennomgangen ovenfor i pkt. 4.1.

Interne IT-systemer i helsevesenet er beskyttet av en rekke sikkerhetsmekanismer som skal hindre uautorisert tilgang til systemene. Et prinsipp som benyttes i de fleste nettverksløsningene baserer seg på å dele nettverket inn i ulike soner basert på hvorvidt systemene behandler sensitive personopplysninger eller ikke. Systemer i disse sonene kan ha muligheten til å kommunisere med systemer på utsiden hvis slik funksjonalitet er nødvendig, men systemer på utsiden av sonen skal ikke ha mulighet til å initiere kommunikasjon mot systemene på innsiden. Dette gjør det vanskeligere å rette angrep mot systemene ved at nettverkstrafikk kan hindres i å nå systemene med sensitiv informasjon.

Web-baserte systemer baserer seg på at en mottaker av informasjon selv initierer en forespørsel mot systemet hvor informasjonen er lagret ("pull" framfor "push"). En klar utfordring blir da på en kontrollert måte å tillate autoriserte brukere å initiere forespørsler mot systemer i sensitiv sone. Ofte gjøres dette ved hjelp av proxy-tjenester som fungerer som mellom-menn og håndterer kontakten med det sensitive systemet. Denne proxy-tjenesten må da være konfigurert på en slik måte at den kan skille autorisert trafikk fra ikke-autorisert trafikk, og kan evt. "vaske" forespørsler slik at kun lovlige forespørsler får slippe igjennom.

Typisk autentisering vil foregå ved oppstart av en kommunikasjonssesjon ved bruk av en terminal, terminalemulator eller nettleser mot en applikasjon eller web-server. Vanligvis benyttes i hovedsak brukernavn og passord. Dette kan kombineres med eller erstattes av digitale sertifikater. Passord kan også være engangspassord som bruker lister eller såkalte kodekalkulatorer. Av nyere dato er også autentisering ved at mobiltelefonnummer til brukeren er kjent, og at et engangspassord sendes med SMS. Korrekt autentisering forutsetter at en enhet fører register over brukere som skal ha tilgang. Dette kan gjøres av den enkelte avsender (det vanligste ved bruk av brukernavn/passord) eller av en sentral part, f.eks. en TTP (det vanligste ved bruk av digitale signaturer).

Tilgangstyringen er i større grad en organisatorisk utfordring. Det finnes mange teknologier som støtter opp under tilgangsstyring – eksempelvis katalogtjenester med bruker- og rolledefinisjoner. Utfordringen ligger i å tildele brukeridentiteter, tilordne roller og systematisere hvilke brukeridentiteter som skal ha tilgang til et gitt informasjonsobjekt eller en funksjon – når skal det være tilgang, hvor lenge, hvem skal kunne tildele osv. Denne informasjonen om hvem som skal ha tilgang m.v. må

til enhver tid være oppdatert og korrekt for at tilgangsstyringen skal fungere som tilsiktet.

En hovedutfordring ved tilgangskontroll ligger i å kontrollere tilgang på tvers av organisasjoner. Normalt opererer uavhengige virksomheter, f.eks. helseforetak, med egne register/kataloger som identifiserer sine egne brukere og tilknyttede tilgangsrettigheter innad i virksomheten. En annen virksomhet vil ikke uten videre kunne akseptere den første virksomhetens krav til f.eks. identifisering, og dennes beslutninger knyttet til tilgangsrettigheter. Hvis brukere i en virksomhet skal gis tilgang til opplysninger i systemene hos en annen virksomhet forutsetter dette både at utvekslingen av opplysningene skjer i en gitt behandlingssituasjon (jf. ovenfor pkt. 4.1) samt at virksomhetene har en omforent policy og lik håndtering av brukeridentiteter og tilgangskontroll og at det eksisterer en gjensidig tillit mellom virksomhetene.

5 Web-tjenester

Dette kapittelet gir en grov oversikt over begrepet web-tjenester (web services).

5.1 Definisjon

Web-tjenester er foreløpig ikke et enhetlig og veldefinert begrep som blant annet omfatter:

- ”Distribuerte objekter” eller ”applikasjonsintegrering” som omfatter utveksling av programobjekter eller oppkalling av programvarefunksjoner over et nettverk
- EDI/B2B som omfatter utveksling av elektroniske forretningsdokumenter over et nettverk

En web-tjeneste (web services) defineres i W3C dokumentet ”Web Services Architecture” [7] som et applikasjonssystem identifisert ved en URI og hvor systemets allment tilgjengelige interfacer og tilkoblinger er definert og beskrevet ved bruk av XML og som kan kontaktes av andre applikasjonssystem. Disse applikasjonssystemene kan deretter kommunisere med web-tjenesten på en måte som følger av dets definerte egenskaper ved bruk av XML over internettprotokoller.⁴

Arkitekturen omfatter løsninger som gjør det mulig å:

- Utsveksle meldinger
- Beskrive web-tjenester
- Publisere og gjøre tilgjengelig web-tjenester som er beskrevet

Formålet med alle disse anstrengelsene er å samordne bruken av mer avanserte web-løsninger med sikte på å få en mer ensartet praksis for bruk av slike løsninger. Innenfor dette området er det flere aktører som til dels har foreslått overlappende løsninger. Felles for disse løsningene er at en forsøker å standardisere tilstøtende områder til informasjonsutvekslingen i større grad enn tidligere.

⁴ Begrepet forutsetter ikke nødvendigvis bruk av verken SOAP eller WSDL.

5.2 EDI versus web-tjenester

Det er ingen motsetning mellom det arbeidet som foregår med tradisjonell EDI over SMTP/X.400 og web-tjenester. Det brukes fremdeles XML-meldinger nøyaktig på samme måte som for tradisjonell EDI, men i tillegg tar web-tjenester sikte på å publisere grensesnittet for informasjonsutvekslingen og de operasjoner som kan utføres av en tjeneste slik at løsningene på sikt bedre kan automatiseres.

Tradisjonell EDI baserer seg vanligvis på en postkasseløsning. Bruker kobler seg opp og ned på et nettverk kun når vedkommende vil sende eller hente dokumenter. Et svar fra mottaker, enten fra systemet eller fra en som har behandlet dokumentet, kommer gjerne en tid etter, avhengig av kommunikasjonsløsning og/eller behandling.

Ved interaktiv EDI er det en direkte kommunikasjon mellom avsendende og mottaende applikasjon under overføring av en melding, men kommunikasjonskanalen er ikke nødvendigvis kontinuerlig åpen under hele dialogen mellom de to partene. Svar fra mottaker foreligger vanligvis i løpet av sekunder.

Når web-tjenester benyttes som et alternativ til EDI er det også direkte kommunikasjon mellom avsendende og mottaende applikasjon og kommunikasjonskanalen er kontinuerlig åpen under hele dialogen mellom de to partene. Svar fra mottaker foreligger vanligvis i løpet av sekunder.

Ved tradisjonell og interaktiv EDI benyttes typisk EDIFACT, HL7 eller XML som meldingssyntaks, mens det for web-tjenester benyttes XML og ulike varianter av HTML. I motsetning til tradisjonell og interaktiv EDI benytter web-tjenester typisk HTTP som syntaks for overføringen.

5.3 Alternative web-tjenester

De to hovedløsningene er:

- 1 ebXML
- 2 WSDL

Disse to løsningsalternativene er delvis overlappende og delvis supplerende.

Begge alternativ benytter SOAP som transportprotokoll. Transporttjenester definerer hvordan meldingsinnholdet skal pakkes inn. SOAP definerer en plattformuavhengig protokoll for kommunikasjon mellom to applikasjoner over Internett. SOAP benytter DOM over HTTP hvor innholdet er definert ved bruk av XML.

Det defineres også regler for samhandling mellom partene, herunder meldingsbekreftelse og samhörighet mellom meldinger som er relatert til en forretnings-transaksjon. Løsningen inkluderer også regler for bruk av nødvendige sikkerhetsløsninger, håndtering av vedlegg med mer.

5.3.1 WSDL

WSDL [4] er lansert av IBM og samarbeidende parter.

WSDL (Web Service Definition Language) definerer først og fremst et sett av tjenester ved bruk av et formelt defineringspråk samt en web-basert distribuert

katalog (UDDI - Universal Description, Discovery and Integration Service) over tilgjengelige tjenesteytere og deres tjenester.

Microsofts .NET [8] er et eksempel på en løsning som benytter WSDL (og UDDI, SOAP osv.), men som også inkluderer andre funksjoner.

5.3.2 ebXML

ebXML [3] er lansert av OASIS [5] og UN/CEFACT [6].

ebXML har definert følgende hovedkomponenter:

- E-business architecture (Overordnet arkitektur)
- Core components (Sentrale informasjonselementer)
- Messaging (Transporttjenester)
- Repository (Katalog over tjenesteytere)
- Collaboration protocol (Samhandlingsprotokoller)
- Implementation (Implementering)

ebXMLs overordnede arkitektur beskriver generelle prinsipper for elektronisk samhandling.

Core components definerer sentrale informasjonselementer samt deres avledninger slik de benyttes mer spesifikt innenfor en gitt sektor, for eksempel helsesektoren, ved bruk av BIE (Business Information Entities). Når aktuelle informasjonselementer engang er definert som internasjonale standarder vil arbeidet med å implementere EDI-løsninger kunne automatiseres og implementasjonskostnadene reduseres.

Samhandlingsprotokoller definerer hvordan tjenesteyter og tjenestesøker skal kunne forhandle seg frem til samhandlingsformer som begge parter kan håndtere for å få utført en tjeneste. Slike tjenester kan være laboratorier som utfører en gitt analyse, et sykehus som tilbyr en spesifikk operasjon, en leverandør som selger et gitt produkt osv.

Katalogen over tjenesteytere lar tjenestesøkere finne frem til samhandlingsparter som kan løse deres behov for tjenester. Katalogen inneholder opplysninger om hvilke tjenester som kan ytes og premissene for disse ytelsene.

5.4 Bruk i helse- og trygde-sektoren

Helse- og trygde-sektoren har alt basert nye løsninger på bruk av deler av ebXMLs transportløsninger som et rammeverk for meldingsutveksling. Det er grunn til å anta at det vil være formålstjenlig å ta i bruk også andre deler av dette rammeverket etter hvert.

Neste trinn vil være å definere sentrale informasjonselementer (Core components) og de avledede BIEs som er aktuelle for sektoren.

6 Konklusjoner

Dette kapittelet beskriver noen konklusjoner som kan treffes ut fra de ulike løsnings egenskaper og anbefalinger for bruk av web-løsninger i helsesektoren.

Gjennomgangen av de ulike alternativ leder frem til følgende konklusjoner:

6.1 Løsningen må velges ut fra behovet

De ulike tekniske løsningene har ulike egenskaper som gjør dem egnet for ulike formål. Det er viktig at web-løsninger (og tilsvarende for andre kommunikasjonsløsninger) benyttes på de områder hvor den aktuelle teknologien løser spesielle behov.

6.2 Web-løsninger nyttig for helsesektoren

Bruk av web-løsninger vil være av betydelig nytte for helsesektoren i likhet med andre deler av samfunnet. Web-løsninger vil kunne gi tilgang til publikumstjenester som etter hvert blir allment tilgjengelig og også tillate interaksjon i form av e-post-kommunikasjon, timebestilling hos lege, på laboratorier og poliklinikker, osv.

Web-løsninger er godt egnet for å gi oversikt over hvor mer detaljert informasjon finnes og tilgang til informasjon som er allment tilgjengelig.

Begrepet ”portal” er et markedsmessig moteord for en vanlig webside på et nettsted som er ment å tilby informasjon for et bestemt formål eller en bestemt brukergruppe. Begrepet innebærer ikke noen ny funksjonalitet og krever ikke at portal håndteres vesensforskjellig fra enhver annen webside.

6.3 Lovverket begrenser tilgang til pasientopplysninger

Web-løsninger er egnet for å gjøre informasjon tilgjengelig fra et hvilket som helst sted, for eksempel pasientopplysninger ved sykdom under reiser. Lovverket forbyr imidlertid tilgjengeliggjøring av den fullstendige pasientjournalen på web for en vilkårlig behandler. En web-løsning er heller ikke særlig velegnet for å sammenstille og presentere detaljerte og omfattende opplysninger som for eksempel opplysningene i en pasientjournal.

Web-løsninger kan imidlertid med fordel benyttes for å gjøre utvalgte helseopplysninger tilgjengelig innenfor lovverkets rammer. Videre kan web være et sted for å

rette forespørsler om utlevering av mer detaljert informasjon som da først sendes (som EDI) etter menneskelig vurdering.

6.4 Web-tilgang alene ofte utilstrekkelig

For mange operative behov i helsesektoren vil det neppe være tilstrekkelig kun å kunne se tilgjengelig informasjon ved bruk av en nettleser. Mottaker vil ofte være lovmessig forpliktet til å dokumentere i sitt eget system hvilken informasjon vedkommende har hatt tilgang til og som for eksempel pasientbehandlingen er basert på. Avgivende system kan tilsvarende være lovmessig forpliktet til å dokumentere hva som er utlevert.

Brukerne vil ventelig ønske å kunne sammenstille og presentere samlet opplysninger som fås fra web med opplysninger som forefinnes i eget applikasjonssystem og/eller andre kilder – for eksempel journalopplysninger i forbindelse med pasientbehandling. Slike brukere vil derfor ofte ønske å ha data tilgjengelig lokalt.

Ved bruk av enkle web-tjenester vil opplysningene som hovedregel kun kunne betraktes og i liten grad benyttes i egen applikasjon. Bruk av ”klipp og lim” er en mulig løsning, men den er relativt tidkrevende og det er fare for at data håndteres feil og i strid med krav til informasjonssikkerhet. Løsningen er derfor lite egnet for rutinemessige operasjoner i helsesektoren, og vil muligens heller ikke bli tillatt brukt i forbindelse med helseopplysninger. Løsningen kan være et alternativ for ting som kun gjøres unntaksvis.

Ved registrering av informasjon kan avsender ønske å kunne ta vare på kvittering for at informasjon er avlevert samt selve informasjoninnholdet.

6.5 Fortsatt behov for utveksling av strukturert informasjon

Det vil fortsatt være nødvendig med overføring av strukturert informasjon når informasjonen skal kunne gjenbrukes i mottakers applikasjonssystem. Det finnes så langt ikke noe alternativ som gjør det mulig å unngå dette. Det arbeides imidlertid med å standardisere deler av informasjoninnholdet i form av Business Information Entities (BIE) som på sikt skal bidra til å forenkle forarbeidet som er forbundet med utveksling av strukturert informasjon.

Det kan også være aktuelt å overføre informasjonen strukturert i tillegg til at den betraktes via web for å kunne verifisere opplysningenes korrekthet samt å logge lokalt hvilke opplysninger en har hatt tilgang til.

6.6 Helsenett fremfor Internett

Et nasjonalt helsenett må betraktes som et åpent nett som også må ha samme sikkerhetsrutiner som ved bruk av Internett. Det vil imidlertid ventelig være bedre tilgjengelighet i et helsenett samtidig som en har bedre kontroll med brukere og infrastrukturen.

6.7 Tilgangssystem for webtilgang er essensielt

I og med at opplysninger på web i utgangspunktet er tilgjengelig for nær sagt enhver uansett sted vil opplysninger som ikke skal være allment tilgjengelige måtte sikres ved bruk av et omfattende tilgangssystem.

Et slikt tilgangssystem kan i teorien styre de ulike parter tilgang til informasjon som er tilgjengelig via web. I praksis vil en ikke kunne sikre seg 100% mot uautorisert utlevering av opplysninger, men en må vurdere når sikkerheten er tilstrekkelig ivaretatt.

6.8 Administrasjon av tilgang krevende

For å administrere tilgang til informasjon på web må det etableres rutiner for å identifisere (autentisere) autoriserte brukere og deres tilgangsrettigheter samt et apparat for å vedlikeholde og drifte tilgangsopplysningene.

7 Foreslåtte aktiviteter

En rekke av konklusjonene innebærer forslag om videre aktiviteter. Disse er oppsummert nedenfor.

7.1 Anvendelsesområder for avanserte web-løsninger

Avanserte web-løsninger kan i likhet med ordinære EDB-program løse nær sagt en vilkårlig oppgave. Det er behov for å utrede videre hvor slike avanserte web-løsninger kan tilby ny og etterspurt funksjonalitet eller hvor eksisterende tradisjonelle løsninger kan erstattes av mer kostnadseffektive web-løsninger.

7.2 Tilgangsrutiner

For å begrense tilgang til informasjon på web som ikke skal være allment tilgjengelig, for eksempel pasientopplysninger, må det planlegges og senere driftes et system som identifiserer (autentiserer) autoriserte brukere og deres tilgangsrettigheter, herunder beslutningsrutiner for tilgang og utlevering utenfor den databehandlingsansvarliges virksomhet.

Denne aktiviteten er det rimelig å se i sammenheng med det arbeidet som er gjort innenfor HER (Helsetjenestesteenhetsregisteret [1]) som definerer alle parter som kommuniserer elektronisk i helsesektoren og også PKI-prosjektet [2] som definerer håndtering av sertifikater for disse brukerne.

7.3 Regelverk for dokumentasjon av web-tilgang

Opplysninger som en bruker kun ser på web blir ikke lagret lokalt på en slik måte at opplysningene kan verifiseres eller at en senere kan dokumentere entydig hvilken informasjon som ble presentert. Dersom slik informasjon benyttes for eksempel i pasientbehandling kan det være et krav at dette skal kunne spores og at relevant og nødvendig informasjon oppbevares lokalt.

Det er derfor være nødvendig å se nærmere på rutiner for lagring av informasjon lokalt i tilslutning til at pasientopplysninger, som benyttes som underlag for kliniske beslutninger, hentes via web.

7.4 Definisjon av BIEs for helsesektoren

Arbeidet med å legge til rette for strukturert overføring av informasjon er tid- og kostnadskrevende. Mye av årsaken til dette er at det aktuelle datainnholdet må

defineres spesielt for hver enkelt funksjon (EDI-melding). Dersom helsesektoren kunne benytte et standard klasse-bibliotek ville arbeidet med integrasjon mellom applikasjon og melding kunne reduseres betydelig både i omfang og tid.

Det pågår for tiden et betydelig arbeide med å definere informasjonsinnholdet som det er aktuelt å utveksle i form av generelle komponenter (Core components). I neste omgang starter arbeidet med å benytte slike Core components i den enkelte sektor i form av BIE – Business Information Entities. Norge bør delta aktivt i arbeidet med å definere informasjonselementer til bruk for helsesektoren.

7.5 Rammeverk for avanserte web-tjenester

For å kunne arbeide videre med avanserte web-tjenester er det nødvendig å utarbeide retningslinjer for hvordan relevante deler av web-tjenester og nye deler av ebXML-rammeverket skal benyttes i praksis i helsesektoren og i samsvar med lovverket.

7.6 Sikkerhet i eksisterende løsninger

Det finnes en rekke eksempler på bruk av enkle web-løsninger i helsesektoren. Tilgangen til informasjon er vanligvis styrt av et tilgangskontrollsystem. Sikkerheten i disse løsningene bør evalueres.

7.7 Prosjekter for bruk av web-løsninger

Det bør innledes et samarbeide med relevante leverandører og aktører i helsevesenet om bruk av enkle og avanserte web-løsninger på områder der dette kan være aktuelt.

8 Referanser

Dette kapittelet omtaler dokumenter som er referert i rapporten.

I dokumentet er det referert til følgende dokumenter:

1. KITH rapport R10/03: Helsetjenesteenhetsregisteret - HER
2. KITH rapport R03/02: PKI-prosjektet. <http://www.kith.no/rapportarkiv/pkiforp.pdf>
3. ebXML: <http://www.ebxml.org/>
4. Web Services Description Language (WSDL) Version 1.2:
<http://www.w3.org/TR/2002/WD-wsdl12-20020709/>
5. OASIS: <http://www.oasis-open.org/>
6. UN/CEFACT: <http://www.unece.org/cefact/>
7. W3C: Web Services Architecture – W3C Working Draft 14.11.2002.
<http://www.w3.org/TR/2002/WD-ws-arch-20021114/>
8. Microsoft .NET: <http://www.microsoft.com/net/basics/>
9. Helseregisterloven: LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger <http://www.lovdatab.no/all/hl-20010518-024.html#3>
10. Helsepersonelloven: LOV 1999-07-02 nr 64: Lov om helsepersonell m.v.
<http://www.lovdatab.no/all/hl-19990702-064.html>

Vedlegg A Sammendrag egenskaper

I den følgende tabellen er de ulike kommunikasjonsformene og deres egenskaper sammenstilt. For beskrivelse av egenskapene vises det til kapittel 1 og 3.

Flere av de angitte egenskapene er ikke absolutte i den forstand at en angitt verdi for en egenskap for en løsning nøyaktig tilsvare egenskapen for en annen løsning selv om denne har samme verdi.

Med strukturert informasjon menes informasjon som er formatert i henhold til en syntaks. Med ustrukturert informasjon menes fri tekst.

Under sikkerhetskrav angir ”Tilgang” at løsningen krever tilgangskontroll, mens ”Melding” angir at løsningen krever meldingssikkerhet som beskrevet i kapittel 4.2.

Begrepet ”Egnet for gjentatt bruk” angir om løsningen er velegnet hvor samme type informasjonsutveksling stadig gjentas.

INFORMASJONSUTVEKSLING
I HELSESEKTOREN

	Felles database	EDI	Interaktiv EDI	E-post	Enkle web-løsninger	Avanserte web-løsninger
Mellom	Applikasjon og Bruker	Applikasjon og Applikasjon	Applikasjon og Bruker	Bruker og Bruker	Applikasjon og Bruker	Applikasjon og Bruker/applikasjon
Initiers av	Mottaker	Sender	Mottaker	Sender	Mottaker	Mottaker
Overføringstid	Sekunder	Minutter	Sekunder	Minutter	Sekunder	Sekunder
Informasjons-innhold	Strukturert informasjon	Strukturert informasjon	Strukturert informasjon	Ustrukturert informasjon	Ustrukturert informasjon	Strukturert informasjon
Kommunikasjons-retning	$A \rightleftharpoons B$	$A \rightarrow A$	$A \rightleftharpoons B$	$B \rightarrow B$	$A \rightarrow B$	$A \rightleftharpoons B$
Kommunikasjons-kanal	LAN/WAN	LAN/WAN	LAN/WAN	LAN/WAN	LAN/WAN	LAN/WAN
Utstyrskrav klient	Lite	Mye	Mye	Lite	Lite	Mye
Nødvendig utstyr hos klient	Fysisk terminal / Terminalemulator	Applikasjon	Applikasjon	E-post klient	Nettleser	Nettleser med applikasjon
Sikkerhetskrav	Tilgang	Melding	Melding Tilgang	Melding	Melding Tilgang	Melding Tilgang
Egnet for store datamengder	Delvis	Ja	Nei	Nei	Nei	Ja
Egnet for gjentatt bruk	Nei	Ja	Ja	Nei	Nei	Ja

**INFORMASJONSUTVEKSLING
I HELSESEKTOREN**