

**Delrapport fra Elviraprojektet**  
**Nettbasert pasientinformasjonssystem**

**Sikkerhetsaspekter**  
**ved**  
**nettbasert tilgang til pasientinformasjon**

Av:

Eva Henriksen & Eva Skipenes

Nasjonalt Senter for Telemedisin

Dato: 15.05.2001

# Innhold

Innhold.....	2
1 Innledning.....	4
2 Datatilsynets sikkerhetsforskrifter.....	4
2.1 Personopplysningsloven.....	4
2.2 Personopplysningsforskriften.....	4
3 Sikkerhetskrav ved nettbasert tilgang til journalinformasjon.....	8
3.1 Konfidensialitet.....	8
3.2 Integritet (og ikke-benektning).....	9
3.3 Tilgjengelighet.....	9
3.4 Sikkerhetstiltak og -mekanismer.....	10
3.4.1 Kryptering, PKI og digitale signaturer.....	10
3.4.2 Autentisering.....	12
3.4.3 Autorisasjon og tilgangskontroll.....	12
3.4.4 Logging/sporing.....	13
3.4.5 Rutiner, regler og holdninger.....	13
4 Trusler og risiko i et system for nettbasert tilgang til journalinformasjon.....	13
4.1 Risikoanalyse.....	13
4.2 Trusselkartlegging i Elvira-prosjektet.....	14
4.3 Sikkerhetsnivået i et system for nettbasert tilgang til journalinformasjon.....	16
4.4 Anbefalinger for sikkerhetspolicy og -strategi.....	17
5 Viktige sikkerhetsaspekter ved nettbasert tilgang til journalinformasjon.....	19
5.1 Arkitekturforutsetninger.....	19
5.2 Problemstillinger.....	20
5.3 Løsningsstrategier.....	21
5.3.1 Tilgangskontroll.....	21
5.3.2 Ansvarsforhold.....	24

6	Oppsummering og anbefalinger for videre arbeid.....	26
7	Referanser.....	27

# 1 Innledning

Formålet med denne delrapporten er å gi en oppsummering av noen av de sikkerhetsaspektene vi har jobbet med i Elvira-forprosjektet. Rapporten gir ingen konkrete løsninger, men peker på problemstillinger som må avklares og løses i en eventuell videreføring av prosjektet.

Den ”nettbaserte journalen” det snakkes om i Elvira-prosjektet er ikke noen *ny journal*, det betegner en nettbasert tilgang til de elektroniske journalene som for en gitt pasient allerede finnes i andre virksomheter. Vi forutsetter at dette kun innebærer nettbasert *lesetilgang* til pasientinformasjon i andre virksomheter enn der man selv befinner seg. Det som gjøres tilgjengelig for andre kan være hele innholdet i journalen, eller bare utvalgte deler av innholdet. Hva og hvor mye som skal være tilgjengelig i et system for nettbasert tilgang til journalinformasjon bør imidlertid diskuteres på et mer generelt nivå, det blir ikke drøftet i denne rapporten.

Denne delrapporten oppsummerer Datatilsynets sikkerhetsforskrifter i kapittel 2. Kapittel 3 gjennomgår generelle sikkerhetskrav som vil være relevante for en nettbasert tilgang til journalinformasjon. I kapittel 4 gis det først en kort introduksjon til risikoanalyse, et forsøk på trusselkartlegging i Elvira-forprosjektet oppsummeres, og det gis noen anbefalinger for hva som må være med i en sikkerhetspolicy og -strategi for et system som dette. I kapittel 5 diskuteres forutsetninger, problemstillinger og løsningsstrategier for nettbasert tilgang til journalinformasjon. Oppsummeringen i kapittel 6 gir anbefalinger for det videre arbeidet som må gjøres.

## 2 Datatilsynets sikkerhetsforskrifter

For spørsmål om taushetsplikt og personvern henvises det til delrapporten om juridiske problemstillinger [1]. Vi vil her fokusere på kapittelet om sikkerhet i forskriften til den nylig vedtatte personopplysningsloven (også kalt personopplysningsforskriften). Kapittelet om sikkerhet er i all hovedsak utformet av Datatilsynet, og blir populært kalt Sikkerhetsforskriften. Vi har her tatt med de punktene fra Sikkerhetsforskriften som vi mener er mest relevante for nettbasert lesetilgang til journalinformasjon.

### 2.1 Personopplysningsloven

Personopplysningsloven [3], gjeldende fra 01.01.2001, stiller krav om at den som er ansvarlig for behandlingen av personopplysninger skal, gjennom planlagte og systematiske tiltak, sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

### 2.2 Personopplysningsforskriften

Sikkerhetsbestemmelsene i forskriften til personopplysningsloven [4] gir mange overordnede føringer for hvordan sikkerheten med hensyn til konfidensialitet, integritet og tilgjengelighet i elektroniske journalsystemer skal tilfredsstilles. Datatilsynet har gitt ut et eget hefte kalt ”Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer” [5]. Følgende avsnitt er hentet fra dette heftet. Direkte sitat er omsluttet med ” ”. Sitater fra Datatilsynets kommentarer (og ikke direkte fra sikkerhetsbestemmelsene) står i kursiv.

## **Forholdsmessige krav om sikring av personopplysninger**

Reglene i personopplysningsforskriften ”gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene. Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.” For enkelte spesielle behandlinger av helseopplysninger vil det være *”like nødvendig å sikre opplysningenes tilgjengelighet som konfidensialitet, for å hindre fare for tap av liv og helse”*.

### **Ansvar/Sikkerhetsledelse**

Forskriften krever at den som har den daglige ledelsen av virksomheten (for eksempel sykehuset, legekantoret, sykehjemmet, tannlegekontoret etc.) som den behandlingsansvarlige driver, har ansvar for at sikkerhetsbestemmelsene overholdes. *”Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi skal beskrives i sikkerhetsmål.”* *”Sikkerhetsmål vil omfatte beslutninger om til hva og hvordan informasjonsteknologi skal benyttes i virksomheten.”* *”Videre skal virksomhetens ledelse beskrive valg og prioriteringer i sikkerhetsarbeidet i en sikkerhetsstrategi. Sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet.”*

### **Ledelsens gjennomgang av sikkerhetsmål og strategi**

*”Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.”* *”Virksomhetens ledelse skal jevnlig, eksempelvis årlig, gjennomgå sikkerhetsmål og strategi”* for å vurdere *”hvorvidt de beslutninger som er tatt er i samsvar med virksomhetens behov for informasjonsteknologi og informasjonssikkerhet.”*

### **Risikovurdering**

Forskriften krever at *”det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.”* *”Risikovurderingen kan utføres med utgangspunkt i norsk standard NS-5814, Krav til risikoanalyser [6].”*

### **Sikkerhetsrevisjon**

Det skal også jevnlig gjennomføres sikkerhetsrevisjon av informasjonssystemet. Til forskjell fra risikovurderingen, som skal gi oversikt over trusler og eventuelle konsekvenser, er formålet med sikkerhetsrevisjonen å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt.

## **Avvik**

Forskriften krever at ”bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.” Det skal foreligge rutiner for avviksbehandling, som har som formål å gjenopprette normal tilstand og hindre gjentakelse. For de tilfeller der avviksbehandling har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles og meddeles resultatet fra avviksbehandlingen.

## **Organisering**

Forskriften stiller krav om at ”det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.” Det er spesielt viktig at ansvar og myndighet relatert til drift av informasjonssystemet og for oppfølging av sikkerhetsarbeid er klarlagt. ”Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.” ”Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner.” Ansvarsforhold og konfigurasjon skal dokumenteres.

## **Personell**

”Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt. Autorisert bruk av informasjonssystemet skal registreres.”

*”Den behandlingsansvarlige pålegges å begrense bruk av informasjonssystemet til det som er tjenstlig nødvendig. Som hovedregel vil all bruk av informasjonssystemet medføre risiko. Slik risiko reduseres til akseptabelt nivå ved hjelp av sikkerhetstiltak. Ved å begrense bruk av informasjonssystemet oppnås:*

- *Minst mulig eksponering av personopplysninger overfor trusler*
- *At den behandlingsansvarlige kjenner til, og har vurdert risiko forbundet med den bruk av informasjonssystemet som pågår”*

## **Taushetsplikt**

”Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig.” Taushetsplikten omfatter også informasjon om informasjonssystemet og om sikkerhetstiltak i den grad utlevering av slik informasjon kan få betydning for informasjonssikkerheten.

## **Fysisk sikring**

Det skal treffes tiltak mot uautorisert adgang til utstyr benyttet for å behandle personopplysninger eller med betydning for informasjonssikkerheten. ”Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.”

## **Sikring av konfidensialitet**

”Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten. Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.” Dersom lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig ikke lenger skal benyttes for behandling av slike opplysninger, skal opplysningene slettes fullstendig og permanent fra lagringsmediet.

## **Sikring av tilgjengelighet**

”Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig. Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten. Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk. Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres.”

## **Sikring av integritet**

”Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten. Det skal treffes tiltak mot ødeleggende programvare”, ”eksempelvis ”datavirus” eller ”malicious software”.”

## **Sikkerhetstiltak**

”Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Forsøk på uautorisert bruk av informasjonssystemet skal registreres.” ”*Sikring av konfidensialitet, tilgjengelighet eller integritet kan ikke utelukkende baseres på rutiner den enkelte medarbeider forutsettes å følge. Den behandlingsansvarlige må også etablere tiltak som fungerer uavhengig av medarbeidernes handlinger, eksempelvis i form av nettverks- eller applikasjonskontroll i sikkerhetsbarrierer.*

*Sikkerhetstiltakene bør etableres slik at funksjonen til to uavhengige tiltak må påvirkes før et sikkerhetsbrudd får betydning for konfidensialitet, tilgjengelighet eller integritet for personopplysningene. Sikkerhetstiltakene skal dokumenteres. De handlinger den enkelte forutsettes å utføre for å oppnå tilfredsstillende informasjonssikkerhet, skal fremgå av rutiner.”*

## **Sikkerhetstiltak hos andre virksomheter**

”Den behandlingsansvarlige kan kun overføre personopplysninger til kommunikasjonspartnere, eksempelvis databehandlere, som tilfredsstill bestemmelsene” i personopplysningsforskriften. ”Formålet med bestemmelsen er blant annet å sikre et harmonisert sikkerhetsnivå i hele kommunikasjonskjeden. Unntak fra bestemmelsen gjelder bl.a. ved overføring til utlandet, jmf. personopplysningsloven §§29 og 30.

*Som hovedregel skal den behandlingsansvarlige selv etablere nødvendige sikkerhetstiltak. For enkelte virksomheter, spesielt mindre virksomheter uten tilstrekkelige ressurser, vil*

*dette ofte ikke være praktisk å gjennomføre. Et alternativ til egen etablering av sikkerhetstiltak kan være å få utført sikkerhetsoppgaver hos underleverandør. Fordeling av sikkerhetsoppgaver mellom virksomheten og leverandøren, skal i "sum" gi informasjonssikkerhet som minst tilfredsstillende kravene i" forskriften. "Forholdet mellom den behandlingsansvarlige og kommunikasjonspartnere eller leverandører, skal være klarlagt og beskrives i avtale. Den behandlingsansvarlige skal være kjent med sikkerhetsarbeidet hos kommunikasjonspartnere eller leverandører gjennom kunnskap om sikkerhetsstrategien til slike virksomheter. Videre skal den behandlingsansvarlige forsikre seg om at informasjonssikkerheten hos partner/leverandør er tilfredsstillende."*

### **3 Sikkerhetskrav ved nettbasert tilgang til journalinformasjon**

Når pasientsensitiv informasjon skal kunne aksesseres via datanett må det iverksettes tiltak for at informasjonens konfidensialitet, integritet og tilgjengelighet ivaretas.

#### **3.1 Konfidensialitet**

Konfidensialitet innebærer at "uvedkommende" ikke skal kunne se/lese den pasientsensitive informasjonen. Med uvedkommende tenker vi først og fremst på de som overhode ikke har noe med pasienten å gjøre, f.eks noen som prøver å tappe informasjon som overføres i et datanett. Men uvedkommende er også helsepersonell som på det gitte tidspunktet ikke har et behandleransvar overfor den aktuelle pasienten. Det kan bl.a bety at

- helsepersonell ikke skal ha generell tilgang til informasjon om enhver pasient; ideelt sett skal en person ikke kunne lese en pasientjournal bare fordi han er lege, og skal heller ikke ha tilgang til tidligere pasienters journaler dersom han ikke lenger har et behandleransvar for vedkommende
- ulike kategorier av helsepersonell (ulike roller) skal ha tilgang til ulike typer informasjon, hjelpepleier trenger f.eks ikke all den informasjon som legen trenger
- helsepersonell skal bare ha tilgang til den nødvendige informasjonen, dvs skal ikke se/lese informasjon som er irrelevant for det aktuelle kasuset

Konfidensialiteten er basert på taushetsplikten i helsevesenet. Kravet om konfidensialitet kan imidlertid komme i konflikt med kravet om tilgjengelighet (se mer om "Tilgjengelighet" i avsnitt 3.3). Selv om en tjenesteyter (helsepersonell) generelt ikke har lov til å aksessere informasjon som ikke er relevant for det aktuelle kasuset, må det vurderes om det likevel bør være teknisk mulig for vedkommende å aksessere slik informasjon. En vanlig kritikk mot helsevesenet er at legene ikke ser pasienten som en helhet, men bare behandler det aktuelle/akutte problemet. Hvis legen hadde hatt mulighet til og ville tatt seg tid og bry med å kikke på hva pasienten har vært plaget med tidligere, kunne det i noen tilfeller føre til at mer sammensatte problemstillinger/sykdomstilfeller ble oppdaget på et tidligere tidspunkt enn det som er tilfellet i dag. Elektronisk tilgang til pasientopplysninger vil forenkle denne muligheten. Ved akutsituasjoner vil det også være nyttig om helsearbeiderne kan få tilgang til viktig informasjon om pasienten fra tidligere behandlinger ved andre virksomheter. Men informasjonen må organiseres og struktureres på en hensiktsmessig måte slik at viktig informasjon ikke drukner i mengden, og

helsearbeiderne må gis nødvendig tid til å forholde seg til den økte mengden informasjon dersom elektronisk tilgang til journalinformasjon skal gi den ønskede effekt. All elektronisk aksess til pasientjournaler må imidlertid logges nøye, slik at alle som har kikket på informasjon om en pasient må kunne stilles til rette for det i ettertid (se også avsnitt 3.4 om "Logging").

### **3.2 Integritet (og ikke-benektning)**

Integritet innebærer at informasjon om pasienten ikke er endret av uautoriserte etter at den ble lagt inn i systemet og godkjent av den som er ansvarlig for innleggelsen av dataene. Ved overføring av informasjon over nettet innebærer integritet at dataene ikke endres underveis.

Integritet kan verifiseres ved bruk av (matematiske) hash-funksjoner. Ved bruk av hash-funksjonen lages et kort konsentrat (noen få bytes) av dokumentet. Senderen legger resultatet av hash-funksjonen (konsentratet) ved dokumentet som overføres. Mottaker kjører dokumentet gjennom den samme hash-funksjonen, og sammenligner resultatet med det konsentratet som er mottatt – de skal være identiske. Bare ett tegn endra i dokumentet vil gi et annet resultat av hash-funksjonen.

Bruk av hash-funksjon kombineres ofte med elektronisk signering av dokumenter ved hjelp av en PKI-løsning (se kap. 3.4). Da krypteres resultatet av hash-funksjonen med avsenders private krypteringsnøkkel før oversending. For å kunne sammenligne resultatet av hash-funksjonen hos mottakeren med det tilsendte resultatet, må det tilsendte hash-resultatet først dekrypteres ved bruk av avsenders offentlig kjente nøkkel. Dersom de to hash-resultatene er identiske, beviser dette at dokumentet ikke er endret underveis og at dokumentet bare kunne komme fra avsender. Slik kan digital signatur benyttes for å oppnå "ikke-benektning", dvs at sender ikke kan nekte for å ha sendt dokumentet som er signert.

En utbredt bruk av en nettbasert journalløsning vil kunne gjøre det overflødig å sende fullstendige medisinske meldinger (f.eks henvisninger, epikriser, labsvar). Meldingene bør kunne leses fra der de ligger. Disse meldingene må være signert digitalt, og den som henter ut informasjonen må kunne verifisere signaturen. Melding om at en medisinsk melding er generert i systemet må likevel sendes til relevante mottakere, slik at de som har ansvar for å følge opp pasienten vet når de skal gjøre det.

### **3.3 Tilgjengelighet**

Tilgjengelighet innebærer at informasjonen om pasienten kan nås der det er behov for den og av dem som trenger den. Man må unngå at sikkerhetstiltakene får negativ innvirkning på tilgjengeligheten. Det vil ofte være viktigere at informasjonen er tilgjengelig for den som skal yte helsehjelp, enn at informasjonen er utilgjengelig for de som strengt tatt ikke har behov for den her og nå.

I utkastet til norsk standard for elektronisk pasientjournal (EPJ) [7] legges det opp til at ingen skal gis tilgang til helseopplysninger i egenskap av å være en bestemt person. Det er rollen den enkelte har som skal avgjøre hva vedkommende får tilgang til. Det skal være mulig å tildele en "Person" en eller flere "Roller" i en virksomhet. Enhver rolle skal kunne knyttes opp mot en eller flere "Organisatoriske enheter". Det skal også være mulig å angi at en Tjenesteyter kan opptre på vegne av en annen Tjenesteyter under bruk av EPJ. Det skal da være mulig å skille mellom registreringstilgang og lesetilgang. Den som registrerer

opplysninger på vegne av en annen trenger som regel ikke å ha lesetilgang på annet enn det vedkommende selv har registrert.

I utkastet står det også at det ikke er akseptabelt at alt helsepersonell alltid skal ha tilgang til all helseinformasjon de kan komme til å få behov for. Tilgang i forbindelse med pasientadministrasjon, internkontroll, kvalitetssikring etc, skal baseres på at noen som har myndighet til det, har tatt en beslutning om å gjennomføre et ”Tiltak”, selv om dette tiltaket ikke nødvendigvis retter seg mot noen enkeltpasient. Videre sier utkastet at det skal være mulig å angi hvilke kategorier helseopplysninger det skal gis tilgang til i forbindelse med gjennomføring av et tiltak, og at det til enhver EPJ i sykehus og andre typer virksomheter hvor det er behov for det, alltid skal være tilknyttet et ”Besluttet tiltak” som sikrer at de som har behov for det, får tilgang i forbindelse med utførelse av nødhjelp.

Pasientens samtykkerett skal etterleves. Det er likevel slik at pasienten i en del tilfeller ikke kan nekte at viktig informasjon i journalen blir gjort tilgjengelig i forbindelse med gjennomføring av tiltak hvor denne informasjonen er absolutt nødvendig.

EPJ-standarden legger altså opp til at det skal kunne gis ulike typer tilgangsrettigheter til ulike deler av en og samme journal.

Tilgjengelighet kan også ses i relasjon til problemet med informasjons-”overflow”: Elektronisk tilgang kan medføre for mye informasjon, med fare for at kritisk informasjon drukner i mengden. Hensiktsmessig organisering og presentasjon av dataene blir derfor viktig.

### **3.4 Sikkerhetstiltak og -mekanismer**

Blant sikkerhetstiltakene som må settes i verk for å oppnå ønsket grad av konfidensialitet, integritet og tilgjengelighet er mekanismer for

- kryptering av informasjonen som overføres
- digitale signaturer
- autentisering
- autorisasjon og tilgangskontroll
- logging/sporing av tilgang
- rutiner og holdninger

#### **3.4.1 Kryptering, PKI og digitale signaturer**

Informasjon som er lagret lokalt trenger i utgangspunktet ikke å være kryptert, dersom den er lagret i sikre omgivelser og tilgangskontrollen er tilfredsstillende.

Overføring av sensitiv informasjon fra ett sikkert område til et annet skal skje kryptert, fordi informasjonen da vil befinne seg utenfor kontrollert område/nettverk. Krypteringen kan gjøres ved hjelp av symmetriske eller asymmetriske algoritmer. Symmetrisk kryptering innebærer at den samme krypteringsnøkkelen brukes på begge sider, til både kryptering og dekryptering. Ved asymmetrisk kryptering brukes det to krypteringsnøkler

som ”opphever” hverandre; det som er kryptert med den ene nøkkelen kan dekrypteres med den andre, og omvendt.

Bare de som er autorisert til å lese informasjonen skal kunne dekryptere den. Nøkkeladministrasjon, med tildeling og utveksling av nødvendige nøkler, blir en utfordring uansett hvilken krypteringsmetode som velges. Ved symmetrisk kryptering må de, og bare de, som er autorisert til å lese informasjonen bli gitt nøkkelen. Utfordringen blir å overlevere nøkkelen uten at uvedkommende får tak i den. Samme krypteringsnøkkel bør ikke benyttes flere ganger, da det vil gi uvedkommende større mulighet til å avsløre nøkkelen. Dette innebærer at ny nøkkel må overbringes ofte, helst før hver ny kommunikasjonssesjon.

Asymmetrisk kryptering blir også kalt ”Public Key”-kryptering, noe som gjenspeiler at en av de to krypteringsnøkklene i nøkkelparet blir gjort offentlig tilgjengelig, mens den andre nøkkelen ikke skal være kjent av noen andre enn eieren. Det som skal overføres til en bestemt mottaker kan krypteres med denne mottakerens offentlig kjente nøkkel, og bare mottakeren kan dekryptere med den private nøkkelen sin. Disse nøklene kan benyttes mange ganger uten at det går ut over sikkerheten. På den måten unngås problemet med overføring av krypteringsnøkkel fra den ene parten til den andre. Men slik asymmetrisk kryptering krever en infrastruktur for å holde rede på de offentlig kjente nøklene og tilhørigheten til brukerne. Et system for tilbaketrekking av ugyldige nøkler og offentliggjøring av disse er også nødvendig. Denne funksjonaliteten er en del av I-en i PKI (Public Key Infrastructure).

PKI-systemer egner seg godt til generering av digitale signaturer. En viktig egenskap ved slike systemer er at den offentlige og den private nøkkelen til en gitt bruker opphever hverandre. Som nevnt over kan det som er kryptert med den ene nøkkelen dekrypteres med den andre, og kun med denne. Det betyr at det som er kryptert med en brukers private nøkkel bare kan dekrypteres med denne brukerens offentlige nøkkel. Det er kun brukeren selv som kjenner sin private nøkkel og som kan benytte denne til å kryptere meldinger med. Alle andre kan få tilgang til brukerens offentlige nøkkel og dekryptere meldingene og på denne måten sjekke at de kommer fra nettopp denne brukeren.

Når en melding krypteres med en brukers private nøkkel kalles resultatet en digital signatur for denne meldingen. Den digitale signaturen er avhengig både av innholdet i meldingen og av brukerens private nøkkel. Den digitale signaturen beviser derfor både hvem det er som har signert meldingen, og den garanterer at meldingen ikke er blitt endret etter at den ble signert. (Se også avsnitt 3.2 foran, om ”hashing”.)

For å kunne vite om det er den riktige brukerens offentlige nøkkel man har tilgang til, brukes sertifikater. I et sertifikat er brukeridentitet og offentlig nøkkel knyttet sammen på en sikker måte ved at en tiltrodd tredjepart har signert koblingen. Det finnes internasjonale standarder for formatet på slike sertifikater. De inneholder også annen informasjon, som utsteder og gyldighetstidsrom, og de kan inneholde informasjon om f.eks ansettelsesforhold. Sertifikatene er signert av utsteder. Infrastrukturen (I-en i PKI) er en sentral del av sertifikathåndteringen. Den omfatter bl.a. nødvendige funksjoner som å:

- motta og validere forespørsler om sertifisering
- opprette/utstede sertifikater og generere nøkler
- gi garanti for at sertifikater er gyldige

- trekke tilbake sertifikater (sertifikatvedlikehold)

Sertifikatet lagres som oftest i en offentlig katalog hos utstederen av sertifikatet. Den private krypteringsnøkkelen bør lagres på et smartkort for å sikre at ikke uvedkommende får tilgang til den. Andre sikre lagringsmedium vil også kunne tenkes brukt. Sertifikatet kan også lagres på smartkortet slik at det kan sendes med meldinger som er signert av brukeren, men dette er ikke absolutt påkrevd da det av sikkerhetsmessige årsaker anbefales at man slår opp i den offentlige katalogen over sertifikater når man har behov for å sjekke en annen brukers sertifikat/offentlige nøkkel. For å få tilgang til informasjonen på smartkortet trengs det en smartkort-leser koplet til brukerens PC. Brukeren må autentisere seg for å få aksess til informasjonen på smartkortet. Denne autentiseringen gjøres vanligvis ved hjelp av PIN-kode eller passord, men man ser også for seg bruk av biometriske kjennetegn, gjerne fingeravtrykk.

### **3.4.2 Autentisering**

Dette er tiltak for å verifisere identiteten til den som vil hente ut informasjon. I tillegg til identiteten (f.eks brukernavnet) må brukeren bevise at vedkommende kjenner til eller er i besittelse av noe som er unikt for denne brukeren. Det kan f.eks være passord, PIN-kode, privat krypteringsnøkkel, eller en biometrisk egenskap som fingeravtrykk, retinamønster, stemme. For passord, PIN-kode og privat krypteringsnøkkel gjelder de kjente kravene om at disse må hemmeligholdes for alle andre. En kombinasjon av mekanismer kan benyttes, for eksempel ved at privat krypteringsnøkkel oppbevares på et smartkort og at tilgang til informasjonen på smartkortet bare gis ved presentasjon av passord, PIN-kode eller f.eks fingeravtrykk.

Når privat krypteringsnøkkel benyttes, autentiseres brukeren ved at det genereres en digital signatur som sendes til den som skal verifisere identiteten til brukeren. Mottakeren må ha tilgang til brukerens offentlige nøkkel for å kunne verifisere signaturen og dermed identiteten til brukeren. Bruk av digital signatur krever tilgang til en PKI-løsning, med infrastruktur for å finne offentlige nøkler og sertifikater.

### **3.4.3 Autorisasjon og tilgangskontroll**

Dette er mekanismer for å gi og kontrollere tilgangsrettigheter til de som allerede er autentisert. Én slik mekanisme er aksesskontroll-lister som skal definere hvem som skal ha rett til hvilken type tilgang til informasjonen (f.eks opprette, skrive, endre, lese, slette). Tilgangsrettigheter kan gis til en gruppe personer (f.eks alle som har samme "rolle", f.eks alle leger ved legesenteret), eller rettigheter kan gis til enkeltpersoner (f.eks lege NN). Det må også være mulig å ekskludere enkeltpersoner eller grupper (f.eks at alle leger ved medisinsk avdeling skal ha tilgang, men ikke lege NN).

For nettbasert tilgang til pasientinformasjon vil det kun være snakk om leserettigheter. All innlegging av ny informasjon vil skje fra de lokale journalsystemene og gjøres av helsepersonellet når de har et behandlingsforhold til pasienten. Leserettighetene bør avhenge av den relasjonen den aktuelle brukeren har til den aktuelle pasienten, dvs helsearbeiderens rolle og forhold til pasienten på det aktuelle tidspunktet. (Se også under "Tilgjengelighet" i avsnitt 3.3.) Det betyr at aksesskontroll-listene bør kunne endres for å holdes oppdatert mht helsearbeidernes relasjon til pasienten. Det betyr også at helsearbeideren vil kunne ha ulike aksessrettigheter til ulike deler av informasjonen, dvs at aksessrettigheter må kunne gis/defineres for små moduler av informasjonen.

Ulike rettigheter finnes allerede i dagens manuelle system, og håndteres gjennom rutiner, regler og holdninger. Det er fortsatt behov for disse, ikke alle sikkerhetstiltak kan automatiseres. (Se avsnittet om ”Holdninger” nedenfor, 3.4.5.)

#### **3.4.4 Logging/sporing**

All aksess til pasientinformasjon må logges slik at man i ettertid kan spore hvem som har lest informasjonen. En slik logging bør ikke bare gjøres på toppnivået i journalen (i journalen som helhet), men være spesifisert til informasjonsmoduler i journalen. Selve loggen må være en del av journalen.

Det er imidlertid ikke nok med selve loggingen, det må også iverksettes rutiner for inspeksjon av loggene for å oppdage eventuelle brudd, og det må defineres rutiner for oppfølging når det oppdages brudd på reglene. Å sende pasienten en melding hver gang noen har aksessert vedkommendes journal, eller for eksempel en gang per måned ved lengre behandlingsforløp, er en mulig måte å følge opp loggene på. Dette alene vil likevel ikke være tilstrekkelig. Den behandlingsansvarlige må også følge opp direkte.

#### **3.4.5 Rutiner, regler og holdninger**

De lovene og reglene om tilgang til journalinformasjon som finnes for manuelle/papirbaserte journaler vil også gjelde for elektroniske og nettbaserte journaler. Dette har i alle tider fungert ut fra rutiner og helsepersonells egne holdninger. Mulighetene for tilgang til informasjon blir imidlertid større hvis man kan taste seg fram til pasientjournalen via PCen på kontoret i stedet for å låse seg inn i et arkivskap et eller annet sted på avdelingen. Derfor trengs det tekniske sikkerhetstiltak, på samme måte som det trenges lås og kode på arkivskapet. Men rutiner og helsepersonellens egne holdninger er fortsatt viktige.

## **4 Trusler og risiko i et system for nettbasert tilgang til journalinformasjon**

Sikkerhetsforskriftene stiller krav til gjennomføring av risikovurdering/risikoanalyse av elektroniske system for behandling av personopplysninger der konfidensialitet, integritet og tilgjengelighet er viktig (se avsnitt 2.2 foran). Et system for å gi tilgang til pasientinformasjon over nettet må gjøres til gjenstand for en grundig risikovurdering/-analyse før det settes i drift.

### **4.1 Risikoanalyse**

Datatilsynet definerer risikoanalyse slik: En systematisk metode for å undersøke trusler, sårbarhet, årsaker og konsekvenser som følge av uønskede hendelser [8]. Metoden som vanligvis benyttes er å klassifisere hver enkelt trussel (hver uønsket hendelse) gjennom kategoriene

- Frekvens (Sannsynlighet)
- Konsekvens

Kategoriene defineres vanligvis med kvalitative beskrivelser, men kvantitative verdier kan også tilordnes disse. Frekvens eller sannsynlighet angis ofte som: ”Svært sjelden – sjelden – ofte – svært ofte” (eller ”Lite sannsynlig – mindre sannsynlig – sannsynlig – meget sannsynlig”). Konsekvens angis vanligvis som: ”Liten – moderat – stor – katastrofal” (eller ”Ufarlig – noe farlig – kritisk – katastrofal”). Dette gir en to-dimensjonal matrise der hver trussel er representert. Risikonivået bestemmes utfra plassering i matrisen, og akseptkriteriene avgjør om tiltak skal settes i verk for å redusere trusselen. (For en grundigere beskrivelse av Risikoanalyse, se [9].)

Viktige forutsetninger for gjennomføring av en risikoanalyse er bl.a:

- Avklaring av oppdragsgivers forventninger (hva skal resultatet av risikoanalysen brukes til?)
- Beskrivelse og avgrensning av analyseobjektet
- Avklaring av analyseobjektets rammebetingelser
- Avgrensning av hva analysen skal omfatte/ikke omfatte
- God kompetanse på analyseobjektet
- Definerings av akseptkriterier (hvor stor risiko aksepteres for de ulike typer trusler)

Trussel-kartlegging er den første og viktigste delen av en risikoanalyse. Denne egner seg å gjennomføre som en idemyldring blant deltakere som har god kjennskap til analyseobjektet.

#### **4.2 Trusselkartlegging i Elvira-prosjektet**

En grundig analyse av sikkerhetsrisikoen må gjøres ved en eventuell videreføring av Elvira-prosjektet. I et tidlig stadium av forprosjektet ble det - som en øvelse - gjort en begynnende trusselkartlegging – selv om få av de viktige forutsetningene som er listet i avsnittet foran kunne sies å være oppfylt på dette tidspunktet. Øvelsen ble f.eks gjort uten tanke på hvilken arkitekturmodell som ville bli valgt. – En oppsummering av denne ”øvelsen” tas med her.

Først identifiserte vi følgende sikkerhetsområder som bør risikovurderes:

- Konfidensialitet for pasientsensitive opplysninger
- Integriteten til informasjon som lagres og oversendes må ivaretas
- Informasjon må være tilgjengelig for de som trenger den når de trenger den (men samtykke-kravet må overholdes)
- Logging av alle hendelser og kontroll av loggene, oppfølging

Så gjorde vi en sterk avgrensning av trusselkartleggingen (i denne øvelsen) til å omfatte bare det første punktet: Konfidensialiteten.

Vi identifiserte overordnede trusler mot konfidensialiteten. Slike trusler kan komme fra:

1. Uautoriserte interne (i samme institusjon)
  - Helsepersonell som ikke har pleie- eller behandlingsansvar for pasienten
  - Andre ansatte i institusjonen
2. Andre brukere av helsenetet
3. Eksterne
  - Hackere
  - Eksterne samarbeidspartnere
  - Konkurrenter

Uautorisert tilgang fra interne brukere i helsenetet anses som en mye større trussel enn uautorisert tilgang fra eksterne, fordi de interne har lettere tilgang til systemet.

Den overordnede trusselen ”Tilgang til pasientsensitiv informasjon fra uautoriserte interne” kan detaljeres slik:

- Alle journaler er tilgjengelige for alle med lovlig tilgang til systemet
- Dårlig tilgangskontroll
  - o Svake passord
  - o Passordene er tilgjengelig for alle (gule lapper)
  - o Manglende skjermbeskyttelse
- Dårlig fysisk sikkerhet
  - o Servere i ulåste rom
- Utro tjenere
- Dårlige loggemekanismer/sporing

En tilsvarende detaljering for trusselen ”Tilgang til pasientsensitiv informasjon fra andre aktører i helsenetet” blir:

- Dårlige tilgangskontrollmekanismer til systemer/nettverk
- Ukryptert overføring av sensitive opplysninger
- Virus
- Dårlige loggemekanismer/sporing

Og tilsvarende for trusselen ”Tilgang til pasientsensitiv informasjon fra eksterne aktører”:

- Inntrengning gjennom brannmur(er)
  - o Knekking av tilgangskontrollmekanismer
  - o Ukrypterte meldinger avlyttes
- Avlytting av ukrypterte meldinger på det åpne nettet (Internett)
- Virus
- Dårlige loggemekanismer/sporing

Vi identifiserte også noen konsekvenser ved brudd på konfidensialiteten:

- Informasjon kommer på avveie
- Media-oppslag
- Saksøking av behandlingsansvarlig og/eller institusjon
- Svekket tillit til institusjonen og/eller helsevesenet
- Ubehag for pasienten ved at helseinformasjon om vedkommende blir allment kjent
- Pasienten kan bli utsatt for økonomisk utpressing
- Pasienten kan bli nektet livsforsikring eller få forhøyet forsikringspremie

Arbeidet videre vil naturlig være å identifisere konsekvensnivå og sannsynlighet for hver enkelt trussel mot konfidensialiteten. For å kunne gjøre dette må man vite noe mer om den/de aktuelle systemarkitektur(er) og de planlagte/implementerte sikkerhetsmekanismene enn det som er tilfelle i skrivende stund. Så må akseptkriteriene defineres, og ut fra disse kan man til slutt si noe om hvilke trusler det må settes i verk sikkerhetstiltak mot.

En tilsvarende risikovurdering må gjøres med hensyn på integritet og tilgjengelighet.

### **4.3 Sikkerhetsnivået i et system for nettbasert tilgang til journalinformasjon**

Vi har gjort et par forutsetninger for konseptet med nettbasert tilgang til journalinformasjon:

- Det er bare behov for leseaksess til den nettbaserte journalinformasjonen. Innlegging av ny informasjon gjøres fortsatt i de lokale (journal-)systemene, og den innlagte informasjonen gjøres tilgjengelig "nettbasert" i hht den modellen som er valgt
- Det "nettet" som tilgang til journalinformasjonen er basert på er (i første omgang) et lukket helsenett, det er ikke det åpne Internettet.

Noen sikkerhetsrelaterte avgjørelser må tas på et overordnet nivå i prosjektet. Det gjelder spørsmål som:

- Hva skal være tilgjengelig via nettet; hvilken del av pasientinformasjonen? Vi ser vel neppe for oss at det blir tilgang til all journalinformasjon?
- Hvem skal ha tilgang til hvilken del av informasjonen?
- En person kan ha rett til å se én del av en pasients journal, men ikke en annen del.
- Tilgangsrettighetene kan være rollebasert eller individbasert.
  - o Rollebasert: Tilgang for noen roller, men ikke for alle ("Er du lege så får du tilgang")
  - o Individbasert: Lege NN og sykepleier YY får tilgang men ikke lege KK og ikke sykepleier ZZ
- Tilgangsrettighetene bør også kunne endres over tid, for eksempel når en pasient skifter fastlege.

Innføring av nettbasert tilgang til pasientinformasjon fra hvor som helst i helsevesenet vil, i tillegg til innføring av nye tekniske løsninger, også medføre behov for nye organisatoriske prosedyrer og rutiner. I mange institusjoner, for eksempel syke- og aldershjem er den fysiske tilgangskontrollen til lokalene minimal. Det er ønskelig at pårørende kan komme og gå relativt fritt (dette gjelder også for en del sykehusavdelinger). Vaktrommet er sjelden låst. De ansatte har behov for tilgang til informasjon om pasientene relativt ofte, noe som medfører hyppig trafikk inn og ut av vaktrommet. Dette gjør at det er ønskelig med færrest mulig barrierer for å komme inn og få tilgang til nødvendig informasjon. Det er uvisst om innføring av elektronisk journalsystem på PC på vaktrommet vil føre til strengere adgangskontroll til vaktrommet i disse institusjonene.

På de fleste sykehjem er det stadig behov for å trekke inn nye vikarer for kortere eller lengre tid. Dersom sykehjemmene har innført elektroniske journalsystemer, vil også vikarene trenge tilgang til det elektroniske journalsystemet for å hente og legge inn informasjon om de enkelte pasientene. Opplæring i sikkerhetsmessige rutiner og regler vil være en stor utfordring i disse tilfellene, på grunn av knapphet på tid og opplæringsressurser.

Ved tilgang til nettbasert pasientinformasjon vil det være behov for en grundig vurdering av sikkerheten, både på det organisatoriske, teknologiske og fysiske plan for alle institusjoner som får slik tilgang. Det vil også være nødvendig med innføring av nye prosedyrer og rutiner. Disse kan omfatte både fysisk tilgangskontroll til rom der PCer med tilgang til journalsystemer står, opplæring i sikkerhet, opplæring i bruk av sikkerhetsmekanismer - for eksempel smartkort ved pålogging til journalsystem, og innføring av rutinekontroller for å sjekke om sikkerheten er tilfredsstillende. På det teknologiske planet vil det være behov for sikkerhetsbarrierer, for eksempel brannmurer, mot utenomverdenen. Behovet for kompetanse på datasikkerhet vil også bli større. Slik kompetanse må sannsynligvis kjøpes/leies inn.

Konsekvensene for andre virksomheter vil kunne være tilsvarende.

#### **4.4 Anbefalinger for sikkerhetspolicy og -strategi**

En overordnet sikkerhetspolicy er et dokument som beskriver målsetninger, regler og retningslinjer for hvordan informasjonssikkerhet skal etableres og vedlikeholdes i en virksomhet [10]. Arbeidet med utforming av en sikkerhetspolicy vil ha stor nytte av resultatene fra utførte risikoanalyser.

Vi vil her nevne noe av det som er viktig å ha med i en sikkerhetspolicy for distribuert nettbasert tilgang til pasientinformasjon.

- 1) Beskrivelse av målsetning med etablering av systemet for nettbasert tilgang til pasientinformasjon. Hva ønsker man å oppnå? Hva slags informasjon skal gjøres tilgjengelig? Hva skal informasjonen brukes til? Hva skal informasjonen ikke brukes til? Hva er ikke lov? Hvorfor ikke?
- 2) Beskrivelse av akseptabelt risikonivå med hensyn på konfidensialitet, tilgjengelighet og integritet/kvalitet
- 3) Beskrivelse av den tekniske infrastrukturen og systemarkitekturen (overordnet funksjonell beskrivelse)

- 4) Etablering av en sikkerhetsorganisasjon som forvalter og styrer en tverrfaglig organisering av arbeidet med sikker informasjonsbehandling. Ansvars- og myndighetsforholdene må klargjøres (hvem har ansvar for hva, både når det gjelder drift, opplæring, kontroll og oppfølging og videreutvikling av sikkerheten). Dette kan bli en utfordring i et distribuert system
- 5) Rutiner for konfigurasjonskontroll
- 6) Definere rutiner for godkjenning av nye applikasjoner/ny funksjonalitet/ny bruk
- 7) Hvordan opprettholde/utvikle nødvendig sikkerhetskompetanse
- 8) Planer for opplæring, bevissthet og motivasjon knyttet til sikkerhetsrutiner. Vurdere behov for eksplisitt taushetserklæring knyttet til nettbasert tilgang til pasientinformasjon.
- 9) Eksterne leverandørers forpliktelser i den grad det er relevant å bruke eksterne utstys- eller systemleverandører, og i den grad det er relevant med service fra eksterne
- 10) Rutiner for utførelse av service
- 11) Kriterier for tilgjengeliggjøring av informasjon (samtykke etc.)
- 12) Rutiner som sikrer ferskhet og kvalitet på informasjonen (inkludert status, for eksempel om informasjonen er foreløpig eller endelig)
- 13) Krav til samtykke og anonymisering ved bruk av informasjon til forskning, statistikk eller annen aktivitet som ikke direkte retter seg mot behandling av pasienten
- 14) Rutiner for gjennomføring av risikoanalyse ved endringer som har betydning for informasjonssikkerheten, og rutiner for jevnlig sikkerhetsrevisjoner
- 15) Beredskapsplaner (nødprosedyrer, alternativ-prosedyrer, gjenopprettingsprosedyrer, testprosedyrer)
- 16) Rutiner for logging av all nettbasert aksess til pasientinformasjon
- 17) Rutiner for gjennomgang/oppfølging av loggene for å oppdage misbruk
- 18) Rutiner for rapportering og oppfølging av sikkerhetsbrudd
- 19) Definere klare rutiner for tildeling av autorisasjoner (hvem skal ha lov til å aksessere hvilken informasjon når?)
- 20) Definere krav til tilgangskontrollmekanismene

## 5 Viktige sikkerhetsaspekter ved nettbasert tilgang til journalinformasjon

Dette kapitlet diskuterer forutsetninger, problemstillinger og løsningsstrategier for nettbasert tilgang til journalinformasjon.

### 5.1 Arkitekturforutsetninger

Man ser for seg minst tre ulike arkitekturmodeller for en nettbasert journalløsning [2]:

Modell 1 : Datavarehus

Data (her: journalinformasjon) blir eksportert fra de lokale databasene (produksjonssystemene) til en sentral/felles database (et "datavarehus"), bl.a for slippe problemene med at de ulike databasene/systemene har ulik struktur og dataene har ulikt format, og for å slippe at man må gjøre oppslag direkte i produksjonssystemene.

Modell 2 : Mellomvare-løsning

Dataene beholdes i de lokale databasene/produksjonssystemene. "Mellomvaren" er programvare som skal løse problemet med ulike format og strukturer, dvs 'dekke over' forskjellene slik at de applikasjonene/systemene som aksesserer informasjonen ikke skal trenge å forholde seg til mer enn ett format - det globale formatet.

Modell 3 : Mobile Agenter

Agenten er programvare som "sendes rundt" for å lete opp den informasjonen som søkes. Man ser for seg en løsning der selve agent-programvaren ligger rundt om i de lokale systemene, og bare input og oppstartsinformasjon for denne programvaren distribueres.

En PKI-løsning vil utgjøre en sentral del av sikkerhetsmekanismene uansett hvilken modell for arkitektur som velges. Vi anbefaler at det ikke lages en dedisert PKI-løsning for nettbaserte tilgang til journalinformasjon. PKI-tjenester bør være en del av de tjenestene som tilbys sentralt i helsenet. Det forutsettes at det eksisterer en nasjonal offentlig nøkkel-infrastruktur (PKI-løsning) for helsevesenet. En slik infrastruktur eksisterer ikke i dag. For å realisere en slik løsning må kravene til løsningen spesifiseres. Det er nødvendig å definere både hva slags sertifikater det er behov for (rollesertifikater, personsertifikater, virksomhetssertifikater etc.), hva de ulike sertifikatene skal inneholde, og hvilke sertifikater som skal benyttes i hvilke sammenhenger.

En katalogfunksjon vil være en annen nødvendig tjeneste for nettbasert tilgang til journalinformasjon. Katalogen(e) må dekke behov for både autentisering og autorisering. Katalogen(e) må derfor bl.a inneholde:

1. unik identifikasjon av alle ansatte i helsevesenet
2. informasjon om profesjon og ansettelsesforhold (rolle) for hver enkelt helsearbeider, inkludert eventuelle personlige begrensninger i autorisasjon (f.eks at lege NN ikke har rett til å skrive ut resepter på visse legemidler)
3. linker til en sentral/nasjonal sertifikatkatalog (offentlig-nøkkel-sertifikat)

Mye av den informasjonen som trengs finnes allerede i eksisterende kataloger. F.eks har RTV et helsepersonellregister der autorisasjonen for noen typer helsearbeidere (bl.a. leger og psykologer) er registrert. Slike eksisterende kataloger bør utnyttes i størst mulig grad. Hvordan katalogene bør organiseres og hvordan forholdet mellom dem bør være har vi ikke drøftet her. Dette bør man komme tilbake til ved en eventuell videreføring av Elvira-prosjektet.

Det vil også være behov for andre typer kataloger. En entydig måte å identifisere pasienter på i de ulike journalsystemene i Norge er en forutsetning for å finne informasjon om riktig pasient via nettverket. Dette betyr ikke nødvendigvis at alle systemer registrerer pasientidentifikasjon på en entydig måte, men det må i det minste finnes en måte å relatere en entydig pasientidentifikasjon til pasientidentifikasjonen som benyttes i de lokale journalsystemer. Vi anser ikke dette som et sikkerhetsproblem men mer som et arkitekturproblem eller en teknologisk forutsetning for nettbasert tilgang til pasientinformasjon, dog med sikkerhetsmessige aspekter, og vil derfor ikke drøfte dette videre i denne rapporten.

## 5.2 Problemstillinger

Gjennom de nye sikkerhetsforskriftene til personopplysningsloven stiller Datatilsynet krav om sikringstiltak med hensyn til konfidensialitet, integritet og tilgjengelighet. De samme sikkerhetsaspektene er sentrale også ut fra et helsesynspunkt:

- Konfidensialitet – for å støtte helsevesenets krav om taushetsplikt
- Integritet – viktig for kvaliteten, for korrekt behandling av pasientene
- Tilgjengelighet – viktig for kvaliteten på behandling av pasientene

Ved nettbasert tilgang til pasientinformasjon som er lagret andre steder enn lokalt, må sikkerheten ivaretas og kontrolleres på en enda strengere måte enn det som kan være akseptabelt så lenge tilgangen kun dreier seg om lokal informasjon. Det bør stilles klare og strenge krav til sikkerhetstiltakene knyttet til slik tilgang. For å sikre at tilgangskontrollen er like sterk alle steder (en lenke er som kjent ikke sterkere enn sitt svakeste ledd), vil det være en fordel med sentral administrasjon av denne. Med sentral administrasjon menes ikke i denne sammenheng at alt nødvendigvis skal styres fra sentralt hold, men at krav, retningslinjer og muligens valg av mekanismer (på et overordnet nivå) avgjøres sentralt.

Datatilsynet stiller krav om at det skal etableres klare ansvars- og myndighetsforhold knyttet til sikkerhet. Sikkerhetsnivået må bestemmes av den som er ansvarlig for behandlingen av pasientopplysningene, og skal være basert på gjennomføring av risikoanalyse og definering av akseptkriterier for sikkerhet.

Delrapporten om arkitektur og visualisering [2] forutsetter for alle sine modeller at det eksisterer en indeks med informasjon om hvor det finnes journalinformasjon om den enkelte pasient. Informasjonen som er lagret i indeksen må anses som konfidensiell på lik linje med informasjonen den henviser til. Kravene til beskyttelse av indeksen må derfor være like strenge som kravene til beskyttelse av informasjonen som er lagret i de ulike journalsystemene. Ansvarsforholdene knyttet til indeksen, og hvordan sikkerhetskravene skal defineres og følges opp må utredes nærmere.

Forskriften til personopplysningsloven krever at alle hendelser av sikkerhetsmessig betydning skal logges, og at det skal finnes rutiner for å avdekke og følge opp avvik og brudd på sikkerheten.

På samme måte som for pasientjournaler må det føres logg over hvem som aksesserer *indeksen* og informasjonen som er lagret der.

Hvordan skal oppfølgingen av loggene foregå? Hvem skal ha ansvar for hva? Hvordan skal for eksempel misbruk eller avvik defineres? Og hvordan skal det avdekkes? Hvem skal følge opp avvik eller misbruk? En oppfølging av loggene vil kunne være problematisk, da den som følger opp loggene og iverksetter sanksjoner ikke nødvendigvis har noe myndighetsforhold overfor den som er misbruker. Et annet problem vil kunne knytte seg til uenigheter når det gjelder hvilke typer sanksjoner som skal iverksettes. Hvem skal ha det avgjørende ordet for dette? Disse spørsmålene må utredes nærmere i en eventuell videreføring av prosjektet.

### **5.3 Løsningsstrategier**

Under følger noen forslag til løsningsstrategier. Disse utgjør ikke nødvendigvis den beste måten å realisere sikkerhetsutfordringene knyttet til nettbasert tilgang til pasientinformasjon, men må anses som et bidrag til en større diskusjon om hvordan dette kan løses.

#### **5.3.1 Tilgangskontroll**

Tilgangskontroll-mekanismene må i hovedsak omfatte:

- Autentisering (hvordan kontrollere hvem en bruker er?)
- Autorisering (tildeling av rettigheter; rollebasert og individbasert)

Autentiseringen bør baseres på en nasjonal PKI-løsning (se kap. 3.4), slik at det blir mulig å sjekke identiteten til en bruker fra hvor som helst i helsevesenet.

Uansett om det velges en sentralisert løsning (for eksempel basert på datavarehus) eller en desentralisert løsning (for eksempel basert på mellomvare eller mobile agenter) for nettbasert tilgang til pasientinformasjon, kan tilgangen til systemet/informasjonen tenkes realisert ved hjelp av et web-grensesnitt. Vi ser da for oss at brukeren logger seg på en web-klient, for eksempel ved å klikke på et "Elvira-ikon" på sin desktop.

#### **Autentisering**

Autentiseringen kan i første omgang gjøres lokalt. Brukeren bør slippe å autentisere seg hver gang informasjon om en ny pasient skal innhentes. Ved bruk av en web-klient for nettbasert tilgang til pasientinformasjon, bør det være tilstrekkelig å autentisere seg når web-klienten startes. Dersom brukeren avslutter web-klienten, bør vedkommende autentisere seg på nytt neste gang programvaren startes. Autentiseringen må baseres på at brukeren oppgir ID/brukernavn (systemet kan eventuelt foreslå et brukernavn som brukeren kan akseptere eller endre). IDen eller brukernavnet bør være knyttet til brukerens navn i systemet. For å bli autentisert må brukerens smartkort med privat PKI-nøkkel settes/stå i smartkortleseren og brukeren må taste PIN-kode eller lignende for å aktivisere smartkortet. Det er mulig å tenke seg at web-klienten kan benytte seg av autentiseringsinformasjonen fra brukerens pålogging på PCen, slik at brukeren ikke trenger å autentisere seg på nytt overfor web-klienten. En forutsetning må da være at smartkortet fortsatt står i smartkortleseren. Dersom smartkortet fjernes fra leseren må systemet logge brukeren av. I framtiden kan det også tenkes at man benytter kontaktløse kort i stedet for smartkort i en smartkortleser. Kravet kan da være at hvis brukeren fjerner seg fra PCen må systemet

logge brukeren av etter et gitt tidsrom, eventuelt starte skjermsparer etter et gitt tidsrom og logge brukeren av etter et lengre fravær. Web-klientens autentisering av brukeren bør også omfatte hvilken rolle vedkommende har på det gitte tidspunkt, for eksempel avdelingslege på avdeling XYZ, kommunelege i kommune QRS, legevaktlege, legesekretær i kommune QRS, avdelingssykepleier på sykehjem A, etc.

Vi vil presisere at dette kun er en av flere mulige måter å tenke seg realiseringen av nettbasert tilgang til pasientinformasjon. Eksempelet med bruk av web-klient for tilgang til pasientinformasjon er brukt for å konkretisere sikkerhetsproblemstillingene.

### **Autorisering**

Autorisering av brukeren, dvs. avgjørelse av hva brukeren skal få tilgang til, bør gjøres for hver gang brukeren forespør informasjon om en ny pasient. Dette bør gjøres transparent for brukeren, dvs. at det gjøres av systemet uten at brukeren trenger å gjøre noe aktivt. Autoriseringen må minimum baseres på

- brukerens identitet
- brukerens profesjon (helsearbeider av type: ...)
- brukerens rolle på det gitte tidspunkt (for eksempel lege/sykepleier/hjelpepleier på en gitt avdeling på et gitt sykehus, primærlege på et gitt legekontor/en gitt bydel/kommune, legevakt-lege på en gitt legevakt, at vedkommende opptrer på vegne av helsearbeider X, etc.)
- brukerens forhold til pasienten (for eksempel at brukeren er pasientens fastlege eller jobber på det samme legekontoret som fastlegen, at brukeren jobber på avdelingen der pasienten på det aktuelle tidspunkt er innlagt, eller lignende)
- pasientens status (har brukeren som sin fastlege, er innlagt på en gitt avdeling på et gitt sykehus, har vært innlagt på en gitt avdeling men epikrisen er ikke ferdigskrevet, eller lignende)
- begrensninger knyttet til den enkelte informasjonsmodul for pasienten (for eksempel at informasjonen kun skal være tilgjengelig for avdelingen/legekantoret som har lagt den inn, at informasjonen i tillegg skal være tilgjengelig for tilsvarende avdelinger på andre sykehus som den avdelingen som la inn informasjon, at informasjonen skal være tilgjengelig for alle som i fremtiden får et behandlingsforhold til pasienten, at informasjonen ikke skal være tilgjengelig for helsearbeider XX, etc. Det må også skilles på hvilke profesjoner som kan få tilgang til hvilke informasjonsmoduler.)

Autoriseringen av brukeren vil kunne gjøres i flere operasjoner. Man kan tenke seg at den lokale web-klienten utfører en første sjekk av om helsearbeideren for øyeblikket står i en relasjon til pasienten som gir vedkommende rett til å innhente den informasjon som forespørres. Dette krever at web-klienten både har tilgang til informasjon om helsearbeideren (hvem helsearbeideren er og hvilken rolle vedkommende har på det gitte tidspunkt) og tilgang til informasjon om pasienten (for eksempel at pasienten er innlagt på en gitt avdeling på sykehuset, hvem som er pasientens fastlege, hvilken kommune pasientene er hjemmehørende i etc.). Dersom web-klienten ikke har tilstrekkelig informasjon, må

avgjørelsen i sin helhet overlates til andre deler av prosessen/systemet. Tilstrekkelig informasjon om både helsearbeideren, pasienten og i hvilken grad pasienten har gitt eller nektet tilgang til journalinformasjon må være tilgjengelig for de delene av systemet som skal håndtere tilgangskontrollen.

### **Informasjonsindeks – og tilgangen til denne**

Som nevnt tidligere (avsnitt 5.2) er alle realistiske løsninger av en nettsentrisk journal avhengig av en indeks over hvor informasjon om den enkelte pasient befinner seg, for å forenkle tilgang/søking etter pasientinformasjon. Innholdet i denne indeksen må ses på som sensitiv på lik linje med informasjonen i pasientjournalssystemene, og må beskyttes på lik linje med annen pasientinformasjon. De samme kravene til autentisering og autorisasjon må gjelde for tilgang til indeksen som for tilgang til pasientjournalinformasjon. Det innebærer at de enkelte elementene i indeksen må inneholde samme informasjon om hvem som kan få tilgang som de elementene de henviser til i pasientjournalene. Autentiserings- og autorisasjonsmekanismene som benyttes må være tilsvarende de som benyttes for tilgang til informasjonen i pasientjournalene.

En måte å realisere dette på er at tilgangskontrollmekanismen som styrer tilgangen til indeksen, får oversendt informasjon fra web-klienten om brukerens identitet, godkjenning av passord, brukerens profesjon, brukerens rolle/funksjon i øyeblikket, pasientens identitet og brukerens ønske om informasjon (kun informasjon fra en gitt helseinstitusjon/virksomhet, kun røntgenbilder, kun informasjon knyttet til lunger, all tilgjengelig informasjon om pasienten etc.). Basert på den tilsendte informasjonen om brukeren, informasjon om pasientens status (for eksempel at pasienten er innlagt på en gitt avdeling og hvem som er pasientens fastlege) og informasjonen om tilgjengelighet knyttet til hver informasjonsmodul om pasienten i indeksen, vurderer tilgangskontrollmekanismen hvilke informasjonsmoduler som kan vises til brukeren.

Informasjonsmodulene i indeksen bør i det minste inneholde informasjon om hvor i helsevesenet det er lagret informasjon om pasienten. Hvor mye mer informasjon som skal lagres i indeksen må vurderes av andre. Mengden og typen informasjon vil kunne påvirke sikkerhetsnivået for indeksen. Det vil sannsynligvis være mer følsomt om indeksen inneholder en URL/Internett-adresse til hver av de ulike dataelementene om pasienten (for eksempel URL til et gitt røntgenbilde, etc.), enn om den kun inneholder navnet på de kommunene som har journaldata om pasienten i sine helse-virksomheter. Informasjonen må krypteres før oversending, gjerne med brukerens offentlige krypteringsnøkkel. Da må i tilfelle brukerens offentlige nøkkel-sertifikat, eller tilstrekkelig informasjon om hvor dette kan finnes, gjøres tilgjengelig for indeksen.

Etter at indeksen har sendt web-klienten en oversikt over hvor det finnes informasjon om pasienten som er tilgjengelig for den gitte brukeren, må web-klienten sende forespørsler til de ulike stedene dataelementene er lagret for å få nok informasjon til å kunne lage en oversiktlig presentasjon for brukeren (dersom indeksen ikke inneholder nok informasjon til å generere dette). Web-klienten må sende den samme informasjonen om brukeren og pasienten til journalssystemene ved forespørsel om informasjon som til indeksen. Hver enhet som gir fra seg informasjon om pasientdata bør sjekke om den som spør har lovlig tilgang til de forespurte data. Dersom de aktuelle pasientdataene er lagret i et sentralt datavarehus, vil tilgangen til de ulike dataelementene måtte sjekkes på samme måte som om de ligger desentralisert der de er produsert. Dette forutsetter i alle tilfeller tilgang til

informasjon om pasientens status, dvs. hvor pasienten befinner seg, om han er under behandling, etc.

En eventuell videreføring av Elvira-prosjektet bør vurdere om tilgangskontrollsystemene både for indeksen og for de systemene der pasientdataene er lagret kan nyttiggjøre seg autentiseringen som er gjort av brukerens lokale system, eller om autentiseringen bør foretas på nytt i disse systemene.

### **Kommunikasjon mellom ulike virksomheter**

Delrapporten om arkitektur og visualisering [2] setter som forutsetning for de desentraliserte modellene at det blir lovlig å opprette en forbindelse fra en datamaskin med sensitiv informasjon i et sikret nettverk i én virksomhet til en datamaskin med sensitiv informasjon i et sikret nettverk i en annen virksomhet for å hente ut informasjon. Fra et juridisk synspunkt vil det sannsynligvis ikke være mulig å innhente sensitiv informasjon fra en annen virksomhet uten å involvere helsepersonell direkte. Helsepersonell-loven tillater at den som behandler en pasient kan utlevere informasjon til andre gitt pasientens samtykke, men den tillater ikke at noen fra en annen virksomhet kan hente informasjon selv. Denne problemstillingen bør være noe av det første som utredes ved en eventuell videreføring av Elvira-prosjektet. Mulige lovendringer må sannsynligvis drøftes i denne sammenheng.

Fra et sikkerhetsmessig synspunkt har det tidligere ikke vært tillatt å initiere en forbindelse utenfra og inn i et nettverket med sensitiv informasjon. Den nylig vedtatte Sikkerhetsforskriften setter ikke forbud mot dette, men sier i stedet at sikkerhetsnivå og sikkerhetsmekanismer skal være basert på risikovurdering. En forutsetning må være at denne type aksess initieres fra en virksomhet med tilsvarende sikkerhetsregime som den virksomheten som aksesseres, og at brukerne som etterspør informasjonen er autorisert for tilgang til denne informasjonen. Vi har ikke sett eksempler på hvordan slik tilgang på tvers av sikre nettverk i ulike virksomheter kan løses på en sikkerhetsmessig forsvarlig måte, men vil ikke utelukke at det kan være mulig. I en eventuell videreføring av Elvira-prosjektet er dette også noe av det første som bør utredes.

### **Nødfunksjonalitet**

Blålysfunksjonen (tilgang til pasientinformasjon på tvers av vanlige tilgangsrutiner i nødsituasjoner) har ikke vært drøftet i dette notatet. Men en mulig måte å løse tilgangsspørsmålet i nødsituasjoner på, er å definere en egen rolle for nødsituasjoner som gir tilgang til all pasientinformasjon som ikke eksplisitt er sperret fordi pasienten har bedt om at den ikke gjøres tilgjengelig. For slik tilgang må det stilles ekstra sterke krav til logging og oppfølging av loggene.

#### **5.3.2 Ansvarsforhold**

Enhver virksomhet bør utforme en sikkerhetspolicy/-strategi som bl.a. definerer ansvars- og myndighetsforhold, beskriver systemet og hvordan dette skal brukes (overordnet funksjonalitetsbeskrivelse), og beskriver krav til sikkerhet og sikkerhetsmekanismer, prosedyrer og rutiner.

Sikkerhetsforskriften understreker at det er den behandlingsansvarlige, ved virksomhetens daglige ledelse, som skal sørge for tilfredsstillende informasjonssikkerhet, og som dermed har ansvar for at bestemmelsene i forskriften følges. Videre skal virksomheten selv

fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Risikonivået skal klarlegges gjennom en risikovurdering. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriteriene for akseptabel risiko, og eventuelle tiltak skal iverksettes for å få sikkerheten opp på ønsket nivå.

Hvis man velger en datavarehus-løsning må statusen til dette sentraliserte systemet defineres. Med status mener vi hva slags type register dette skal være. Er det å anse som et journalsystem eller er det en ny type helseregister? Dette må vurderes ut fra et juridisk perspektiv, se delrapport om juridiske aspekter ved nettbasert tilgang til pasientinformasjon [1]. Ut fra sikkerhetsforskriftene vil det være den ansvarlige leder for virksomheten som tilbyr datavarehus-tjenesten som har ansvar for at sikkerhetsbestemmelsene overholdes for dette systemet.

Problemene knyttet til ansvarsforhold vil til en viss grad være de samme for en indeks over hvor informasjon om den enkelte pasient finnes, som for en sentral database med kopi av journalinformasjon. Men begrensninger i typen informasjon som lagres i indeksen vil kunne begrense problemene knyttet til ansvarsforholdene for denne.

En annen ting som kan være problematisk i denne sammenheng er ansvaret for å fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysningene. Hvis nivået for akseptabel risiko for datavarehuset eller indeksen avviker (vesentlig) fra nivået i de virksomhetene informasjonen kommer fra, vil dette kunne underminere sikkerheten i helsevesenet. Et forslag til løsning på problemet med mulig avvikende risikonivå er at det fra sentralt hold defineres et nasjonalt akseptnivå for risiko som alle må forholde seg til. Dette vil imidlertid ikke løse hele problemet, da risikonivået alltid må relateres til lokale tekniske løsninger etc.

Det som kan være noe uklart, er hvem som har ansvaret for etablering og oppfølging av tiltak som fungerer uavhengig av medarbeidernes handlinger, eksempelvis i form av nettverks- eller applikasjonskontroll i sikkerhetsbarrierer. Sikkerhetstiltakene bør etableres på en slik måte at funksjonen til to uavhengige tiltak må påvirkes før et sikkerhetsbrudd får betydning for konfidensialitet, tilgjengelighet eller integritet for personopplysningene. Hvor skal disse barrierene stå, og hvem skal ha ansvar for dem? Hvem skal ha ansvaret for å følge opp eventuelle sikkerhetsbrudd overfor den enkelte bruker? Kan dette ansvaret distribueres? I tilfelle på hvilken måte? Disse problemstillingene må drøftes nærmere i en eventuell videreføring av prosjektet.

En problemstilling ved alle de foreslåtte modellene er at informasjon som skal vises på en dataskjerm i en annen virksomhet enn der informasjonen er generert og lagret, må lagres midlertidig på en server/datamaskin lokalt der den skal vises. Dette innebærer at pasientinformasjon "dupliseres" og (for en stund) lagres utenfor journalen den hører til i. Kravet til sikkerhet må være like stort for systemet/serveren/datamaskinen der slik mellomlagring finner sted, som der dataene er generert. I tillegg må det stilles krav om og etableres mekanismer som sørger for at disse dataene slettes fra det midlertidige lagringsstedet straks det ikke er bruk for dem lengre. Kriteriene for når dataene skal slettes må spesifiseres nærmere. (Er det f.eks når helsearbeideren bytter skjerm bilde, eller må helsearbeideren eksplisitt gi beskjed om at han/hun er ferdig med å se på dataene før de slettes?)

## 6 Oppsummering og anbefalinger for videre arbeid

Denne delrapporten gir ingen endelige sikkerhetsløsninger for nettbasert tilgang til journalinformasjon, men diskuterer problemstillinger som må avklares og løses i en eventuell videreføring av prosjektet.

Vi har forutsatt bruk av nasjonale PKI-løsninger og en nasjonal standard/profil for sertifikater til bruk i helsevesenet, inkludert retningslinjer for hvordan sertifikater skal benyttes i ulike sammenhenger. Dette eksisterer ikke i dag. Det må blant annet avklares hva slags sertifikater helsearbeidere skal ha, og om de kan benytte samme sertifikat i ulike roller (for eksempel som lege på en sykehusavdeling og som legevaktlege på kveldstid). Hvordan RA-funksjonaliteten (godkjenningsinstans for identiteten til brukere som ønsker å få offentlig nøkkel-sertifikat) skal realiseres for helsearbeidere (og pasienter?) må også avklares.

Løsninger for autentisering og autorisasjon forutsetter videre et sett av katalogfunksjoner sentralt i helsenettet. Mye av dette er kataloger som enten finnes i dag eller funksjonalitet som må finnes i et helsenett uavhengig av en eventuell videreføring av Elvira-prosjektet. For eksempel vil det måtte finnes regionale/nasjonale oversikter over hvem som er fastlege til den enkelte pasient.

Det er likevel en rekke spørsmål som må avklares i et videre arbeid.

- Hvordan kan man realisere tekniske løsninger som tillater sikker aksess inn i systemer med sensitiv informasjon i en virksomhet, for autoriserte brukere fra en annen virksomhet med et tilsvarende sikkerhetsregime?
- Hvordan kan man realisere tekniske løsninger som gir systemet informasjon om hvilken rolle og relasjon en helsearbeider på et gitt tidspunkt har til en gitt pasient? Det finnes sannsynligvis ulike måter å gjøre dette på.
- Det må utredes nærmere hvilken informasjon det vil være behov for i tilknytning til roller. Eksempler er profesjon (lege, sykepleier, fysioterapeut, etc) og virksomhetstilknytning (kommunehelsetjenesten i kommune A/bydel B, hjemmetjenesten i kommune C, avdeling X på sykehus Y, legevakt-ordning i bydel/kommune, etc).
- Systemet som skal lages skal gi tilgang til informasjon kun om de pasienter som den aktuelle helsearbeider er autorisert for å få tilgang til, og ha et risikonivå som er akseptabelt samtidig som en blålysfunksjon ivaretas. Omfanget av arbeidet med å utvikle løsninger som ivaretar alle disse aspektene samtidig må utredes nærmere.
- Uansett arkitekturløsning ser det ut til at det må finnes pasientinformasjon lagret sentralt i nettet. Det vil i alle fall være behov for en sentral indeks med henvisning til tilgjengelig journalinformasjon. Ved valg av en sentralisert datavarehusløsning vil det i tillegg også dreie seg om direkte journalinformasjon. Ansvarsforholdene omkring pasientinformasjon som er sentralisert i nettet må utredes nærmere.
- Det er også mange spørsmål omkring tilgangskontrollsystemet til informasjonsindeksen som må avklares nærmere. Kan f.eks tilgangskontrollsystemet her nyttiggjøre seg den autentiseringen som allerede er gjort av brukerens lokale

system, eller må autentiseringen foretas på nytt? De samme problemstillingene vil gjelde tilgangskontrollen i de systemene der selve journalinformasjonen er lagret.

- Hendelser av sikkerhetsmessig betydning skal logges. Hva som skal logges og alle spørsmål omkring oppfølging av loggene må utredes nærmere. Dette er avklaringer som hører hjemme i en sikkerhetspolicy og -strategi for et slikt system.
- Det kan være behov for å gi tilgang fra bare én bestemt maskin eller én bestemt nettsadresse på et legekantor, og det kan være behov for å autentisere tjenestene som aksesseres. Mulige løsninger for autentisering av applikasjoner og maskiner ved bruk av PKI (for eksempel virksomhetssertifikater?) må utredes nærmere.
- Hva med aksess til journalinformasjon fra hjemme-pc? Man kan tenke seg at en lege har behov for aksess til sin pasients journal fra hjemmekontoret. Skal det i så fall tillates med aksess til informasjon som er lagret andre steder enn lokalt på egen arbeidsplass? I et framtidig system kan man også tenke seg at en pasient ønsker å kunne lese sin egen pasientjournal hjemmefra. Hvordan skal sikkerheten ivaretas hvis dette tillates?
- Sikkerhet knyttet til mobile agenter, og mulighetene med mellomlagring ved forespørsler i en distribuert løsning.
- Innføring av nettbasert tilgang til pasientinformasjon fra hvor som helst i helsevesenet vil, i tillegg til innføring av nye tekniske løsninger, også medføre behov for nye sikkerhetsprosedyrer og -rutiner. Omfanget av dette for ulike typer institusjoner må utredes i en eventuell videreføring av prosjektet.

Ved en eventuell videreføring av Elvira-prosjektet må det gjennomføres grundige risikoanalyser for de løsningene som man velger å gå videre med.

## 7 Referanser

1. Delrapport om Elvira og juridiske problemstillinger; Christiansen E. K., Nohr L. E.
2. Delrapport om arkitektur og visualisering; Bellika J. G., Hartvigsen G., Loftesnes L. E., Strandenæs T.
3. Lov om behandling av personopplysninger (Personopplysningsloven)
4. Forskrift til Personopplysningsloven (Personopplysningsforskriften)
5. Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, Datatilsynet desember 2000.
6. Norges Standardiseringsforbund (NSF): "Krav til risikoanalyser", NS-5814, 1. utgave, august 1991
7. KITH: EPJ standard – Arkitektur, arkivering og sikkerhet, Del I
8. Datatilsynet: "Veiledning i risikoanalyse av informasjonssystem"

[http://www.datatilsynet.no/infosik/veiledn/risiko/TV201\\_98.pdf](http://www.datatilsynet.no/infosik/veiledn/risiko/TV201_98.pdf)  
TV-201:1998

9. KITH: "Risikoanalyse. Metodegrunnlag og bakgrunnsinformasjon"  
<http://www.kith.no/rapportarkiv/rosmet.pdf>  
KITH Rapport 13/2000, Versjon 1.0, 8.september 2000 (ISBN 82-7846-091-4)
10. KITH: Overordnet sikkerhetspolicy for helseinstitusjoner (Sikker  
informasjonsbehandling i helsevesenet, temahefte nr 2)