

KITH

INFORMASJONSTEKNOLOGI
FOR ET BEDRE HELSEVESEN

Delrapport Paraplyprosjektet - Informasjonssikkerhet ved PACS løsninger

Versjon 1.0

Dato: 06.02.2003

KITH Rapport 07/03

ISBN 82-7846-170-8

KITH-rapport

KITH
INFORMASJONSTEKNOLOGI
FOR ET BEDRE HELSEVESEN

TITTEL

Delrapport Paraplyprosjektet - Informasjonssikkerhet ved PACS løsninger

Postadresse
Sukkerhuset
N-7489 Trondheim

Forfatter(e):

Olaf Trygve Berglihn

Magnus Alsaker

Besøksadresse

Sverresgt 15

Telefon

+47 - 73 59 86 00

Oppdragsgiver(e)

Sosial- og Helsedirektoratet

Telefaks

+47 - 73 59 86 11

e-post

firmapost@kith.no

Foretaksnummer

959 925 496

ISBN

82-7846-170-8

Dato

06.02.2003

Antall sider

57

Kvalitetssikret av

Bjarte Aksnes

Gradering

Å (Åpen)

Godkjent av:

Rapportnr.

07/03

Sammendrag

Rapporten inneholder del resultater fra Paraplyprosjektet som er gjennomført i regi av Sosial- og Helsedirektoratet. Rapporten har fokus på sikkerhet ved PACS løsninger, og spesielt med tanke på felles fysiske datalagerløsninger mellom helseforetak.

Det blir belyst hvordan aktuell lovgivning setter rammebetingelser for hvordan PACS løsninger kan fungere. Løsninger som inkluderer felles fysiske datalagerløsninger mellom flere helseforetak gir mange fordeler, men setter ekstra strenge krav til informasjonssikkerheten. Av Helseregisterloven og Helseforetaksloven følger det at pasientinformasjon ikke fritt kan deles mellom flere helseforetak. Felles datalagringsløsninger krever derfor at en kan skille på data tilhørende ulike helseforetak, og det fører også til at tilgangsstyring og tilgangskontroll kan bli omfattende.

Det settes fokus på hvordan løsninger kan utformes med tanke på best mulig samhandling og utveksling av informasjon mellom helseforetak. Det skisseres flere modeller med varierende grad av integrasjon av PACS og RIS systemer. Det skisseres også hvordan løsninger med bruk av felles datalagerløsninger mellom flere helseforetak kan utformes, både med tanke på samhandling og utveksling av informasjon og for å ivareta informasjonssikkerheten på en best mulig måte.

Det blir også belyst aktuelle trusler mot informasjonssikkerheten ved bruk av felles fysiske datalagerløsninger og mulige tiltak mot de ulike truslene. Spesielt kritisk ved felles datalagerløsninger er kommunikasjonslinjer til datalageret og selve datalageret. Redundante løsninger og gode backup rutiner kreves derfor skal en være sikret en stabil tjeneste med høy tilgjengelighet.

Innholdsfortegnelse

Innholdsfortegnelse	5
1. Bakgrunn	7
2. Aktuell lovgivning	8
2.1. Helseregisterloven.....	8
2.2. Annet lovverk	10
2.3. Konsekvenser for PACS løsninger	13
3. DICOM.....	14
3.1. Nettverk og tilgangskontroll med DICOM.....	14
3.2. Innholdskryptering.....	15
3.3. Utlevering og tilgang	16
3.4. Transaksjoner for utveksling	17
4. Modeller for utveksling mellom helseforetak	19
4.1. Lokal PACS + EDI	21
4.2. Lokal PACS + Teleradiologi	22
4.3. Lokal PACS + DICOM over IP.....	22
4.4. Lokal PACS og synkronisering/overføring mot sentral PACS.....	23
4.5. Kun sentral PACS.....	24
4.6. Web-grensesnitt i kombinasjon med sentral eller lokal PACS	25
5. Informasjonssikkerhet ved felles fysisk datalagerløsning for digital røntgen	26
5.1. Rammebetingelser.....	28

5.2.	Muligheter ved felles datalagerløsninger	29
5.3.	Tilgangshåndtering	32
5.4.	Konfidensialitet	33
5.5.	Tilgjengelighet	35
5.6.	Integritet	37
5.7.	Sporbarhet til data	39
6.	Løsninger med felles fysisk datalagring	40
6.1.	Kobling mot felles lager	41
6.2.	Håndtering av DICOM kommunikasjon	43
7.	Konklusjon og anbefalinger	45
	Referanseliste	46
	Vedlegg B: Referat fra workshop	47
	Fokusområde 1: Helselovverk og forskrifter	47
	Fokusområde 2: Akseptkriterier	51
	Fokusområde 3: PACS løsninger	53
	Fokusområde 4: Rammeverk	55

1. Bakgrunn

Løsninger for lagring av medisinske bilder - Picture Archive and Communication System (PACS) - og tilhørende informasjonssystem for røntgen (RIS) er på full fart inn i de fleste helseforetak i Norge. Sykehusene velger forskjellige løsninger for implementering av PACS systemene, ofte uten samordning med andre sykehus i samme region. Det er også store forskjeller på de systemer som er etablert eller under oppføring på tvers av regionene. Dette kan føre til at informasjonssikkerheten blir ivaretatt på ulike måter.

Med tilgang på helsenettverk mellom helseforetakene åpnes det for samordning og etablering av sentrale felles lagerløsninger. Aktuell lovgivning setter begrensninger for hvordan slike løsninger kan være utformet, og det er usikkerhet rundt hvilke løsninger som er innenfor lovverket. Det er også utfordringer i forhold til lovgivning når det gjelder utlevering og tilgang til informasjon på tvers av helseforetak.

Mye av usikkerheten og utfordringene ligger i at det kom nytt lovverk fra 1. januar 2002 som satte nye rammebetingelser for utforming av IT-løsninger innen helsevesenet. Bruk av ny teknologi og de muligheter som nå åpner seg krever også at lover og forskrifter må fortolkes på en ny måte.

KITH arrangerte 19. november 2002 en workshop i forbindelse med prosjektet hvor det ble tatt opp sentrale spørsmål vedrørende sikkerhet i PACS løsninger (se vedlegg A). Deltakere var både fra leverandører og helseforetak i tillegg til at KITH deltok. Det ble blant annet diskutert hva som er de største utfordringene knyttet til informasjonssikkerhet i PACS løsninger og hva som er mulige strategier for aktuelle løsninger.

2. Aktuell lovgivning

Her settes det fokus på hvilke rammebetingelser lover og forskrifter setter for PACS/RIS løsninger.

Lovverk og retningslinjer setter rammer for hvordan tilgang til pasientinformasjon på tvers av helseforetak kan foregå. Personopplysningsloven og Helseregisterloven av 1. januar 2002 innebar en del endringer fra det gamle lovverket. Dette skjedde samtidig med innføring av en ny helsereform som delte

helse-Norge opp i fem helseregioner og tilhørende regionale helseforetak. Omstruktureringen åpnet for større lokal frihet og samordningspotensial, spesielt på IT-siden. Disse endringene har skapt usikkerhet rundt hvordan nye IT-løsninger kan fungere og hvordan dette reguleres av eksisterende lover og forskrifter.

2.1. Helseregisterloven

Den nye Helseregisterloven setter flere viktige rammebetingelser for mulige anvendelser av PACS løsninger. Helseregisterloven sier i klartekst at helseopplysninger ikke skal deles mellom ulike helseforetak. Med helseforetak menes det i loven institusjon på behandlingsnivå. Deling av helseopplysninger innen et regionalt helseforetak er altså ikke tillatt. Utlevering av helseopplysninger fra et foretak til et annet skal kun foregå når det er hjemlet i forbindelse med behandling og med pasientens samtykke. Det er en forutsetning at pasienten har blitt informert om sine rettigheter og muligheten til å motsette seg utlevering av pasientinformasjon. Informasjon om at pasienten har blitt informert og hva pasienten har samtykket til skal registreres i pasientens journal.

Sentrale begreper

To sentrale begreper i Helseregisterloven er:

1. **Databehandlingsansvarlig (= behandlingsansvarlig i Personopplysningsloven):** 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

2. **Databehandler:** den som behandler helseopplysninger på vegne av den databehandlingsansvarlige

Noen viktige punkter i Helseregisterloven er:

- ❑ **§ 7. Regionale og lokale helseregistre**
Det kan ikke etableres andre regionale og lokale helseregistre med helseopplysninger enn det som følger av denne eller annen lov.
- ❑ **§ 13. Tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon**
Bare den databehandlingsansvarlige, databehandlere og den som arbeider under den databehandlingsansvarliges eller databehandlers instruksjonsmyndighet, kan gis tilgang til helseopplysninger.
- ❑ **§ 16. Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet**
Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger.
- ❑ **§ 18. Databehandlers rådighet over helseopplysninger**
En databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med den databehandlingsansvarlige.
- ❑ **§ 27. Forbud mot å lagre unødvendige helseopplysninger**
Den databehandlingsansvarlige skal ikke lagre helseopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen av helseopplysningene. Hvis ikke helseopplysningene deretter skal oppbevares i henhold til arkivloven eller annen lovgivning, skal de slettes.
- ❑ **§ 31. Tilsynsmyndighetene**
Datatilsynet fører tilsyn med at bestemmelsene i loven blir fulgt og at feil eller mangler blir rettet, jf personopplysningsloven § 42, med mindre tilsynsoppgaven påligger Statens helsetilsyn eller fylkeslegen etter lov 30. mars 1984 nr. 15 om statlig tilsyn med helsetjenesten.

Ut fra helsepersonelloven (se neste kapittel) er det mottaker som må avgjøre om informasjonen er av betydning for behandlingen eller ikke. Er den nødvendig for behandlingen må den inn i pasientjournalen. Når det gjelder røntgenbilder, kan det være tilstrekkelig å bevare en tekstlig tolkning av bildet, for eksempel en beskrivelse av de funn som ble gjort og ikke nødvendigvis av de bilder som er mottatt.

2.2. Annet lovverk

Foruten Helseregisterloven er det også andre lover som vil påvirke hvordan PACS/RIS løsninger kan benyttes. Vi vil ikke gå i detalj i lovgivningen, men hovedtrekkene ved de aktuelle lover og forskrifter tas opp.

2.2.1. Personopplysningsloven og personopplysningsforskriften

Personopplysningsloven (forkortet POL) regulerer all behandling av personopplysninger. Den ble gjort gjeldende fra 1. januar 2001 og erstattet da *personregisterloven* fra 1978. Viktige punkter i POL er:

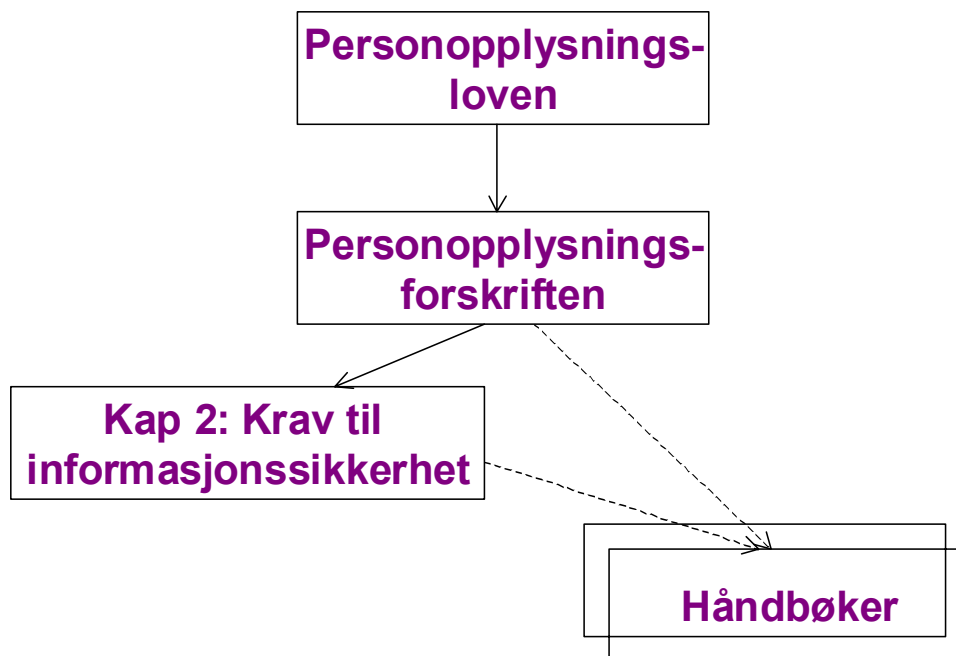
- ❑ Hovedregel er at personopplysninger kan bare behandles dersom den registrerte har samtykket, eller det er fastsatt i lov at det er adgang til slik behandling, eller et av kravene i POL §8 a-f er oppfylt
- ❑ Samtykke må være basert på reell kunnskap om forholdet og konsekvensene
- ❑ Opplysninger som er innsamlet til et formål, skal ikke brukes til et annet
- ❑ Datatilsynet er tilsynsmyndighet

Personopplysningsforskriften

I tillegg til POL finnes personopplysningsforskriften (forkortet POF) som omfatter krav til informasjonssikkerhet ved behandling av personopplysninger. POF erstatter kravene som var i *Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger*. Viktige punkter i forskriften er:

- ❑ Stiller krav til informasjonssikkerhet (i kapittel 2) som blant annet innebærer
 - Sikring av konfidensialitet, integritet og tilgjengelighet
 - Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av ”planlagte og systematiske tiltak”
- ❑ Angir krav til styringssystem for sikkerhet som må etableres for å oppnå *tilfredsstillende* informasjonssikkerhet (intern kontroll)
- ❑ Risikovurderinger står sentralt

- ❑ Datatilsynet kan gi pålegg og overprøve valg av akseptabelt risikonivå (jfr §2.2)
- ❑ Datatilsynet skal informere og gi råd om trusler og anvendelige sikkerhetstiltak
- ❑ Informasjonssystem og sikkerhetstiltak skal dokumenteres (primært for egen del, jfr §2.16)



Figur 1: Oversikt over POL med tilhørende forskrift

2.2.2. Helsepersonelloven

Helsepersonelloven omhandler helsepersonells plikter og ansvar i forbindelse med utøvelse av yrket.

Noen viktige punkter i helsepersonelloven er:

- ❑ **§ 5. Bruk av medhjelpere**
Helsepersonell kan i sin virksomhet overlate bestemte oppgaver til annet personell hvis det er forsvarlig ut fra oppgavens art, personellets kvalifikasjoner og den oppfølging som gis. Medhjelpere er underlagt helsepersonells kontroll og tilsyn.
- ❑ **§ 21. Hovedregel om taushetsplikt**
Helsepersonell skal hindre at andre får adgang eller kjennskap til opplysninger om folks legems- eller sykdomsforhold eller andre personlige forhold som de får vite om i egenskap av å være helsepersonell.

❑ **§ 25. Opplysninger til samarbeidende personell**

Med mindre pasienten motsetter seg det, kan taushetsbelagte opplysninger gis til samarbeidende personell når dette er nødvendig for å kunne gi forsvarlig helsehjelp.

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

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

2.2.3. Pasientrettighetsloven

Pasientrettighetsloven har til hensikt å sikre befolkningen lik tilgang på helsehjelp av god kvalitet ved å gi pasientene rettigheter overfor helsevesenet. Noen viktige punkter i pasientrettighetsloven er:

❑ ***§ 5-1 Rett til innsyn i journal***

Pasienten har rett til innsyn i journalen sin med bilag og har etter særskilt forespørsel rett til kopi.

Pasienten har etter forespørsel rett til en enkel og kortfattet forklaring av faguttrykk eller lignende.

❑ ***§ 5-3 Overføring og utlån av journal***

Pasienten har rett til å motsette seg utlevering av journal eller opplysninger i journal. Opplysningene kan heller ikke utleveres dersom det er grunn til å tro at pasienten ville motsette seg det ved forespørsel.

2.2.4. Helseforetaksloven

Helseforetaksloven trådte i kraft 1. januar 2002 og er lovgrunnlaget for overføring av eierskap for sykehusene fra kommuner og fylkeskommuner til staten. Loven beskriver regionale helseforetak (RHF) og helseforetak (HF), og hvordan foretakene skal organiseres og ansvarsforhold. Noen viktige punkter i loven er:

❑ **§ 1. Lovens og helseforetakenes formål**

Et regionalt helseforetak skal etter eiers (Helsedepartementet) retningslinjer planlegge og organisere spesialhelsetjenesten, og legge til rette for forskning og undervisning.

❑ **§ 2. Lovens virkeområde**

Helseforetak er virksomhet som eies av regionalt helseforetak alene og som er opprettet i medhold av §

9. Helseforetak yter spesialisthelsetjenester, forskning, undervisning og andre tjenester som står i naturlig sammenheng med dette.

□ **§ 9. Opprettelse av helseforetak**

Utøvende virksomhet skal organiseres som helseforetak.

2.3. Konsekvenser for PACS løsninger

Fra Helseregisterloven følger det at det er kun den databehandlingsansvarlige som kan gis tilgang til helseopplysninger. Fra Helseforetaksloven følger det at det kun helseforetak (og ikke på regionalt nivå) som kan være den utøvende part. Bruk av felles PACS og RIS for flere helseforetak med full tilgang til helseopplysninger på tvers av helseforetakene er altså lovstridig. Det utelukker ikke felles drift av PACS/RIS løsninger så fremt informasjonene kan holdes adskilt for hvert helseforetak. De ulike helseforetakene som deltar i en slik ordning og eventuelle andre eksterne parter kan ikke gis direkte tilgang til hverandres bilder og pasientinformasjon i systemet uten at tilgangen er hjemlet, godkjent av pasient, det foreligger en beslutning om utlevering og tilgangen ikke uten videre tidsbegrenses. Det helseforetak som gis tilgang skal i regelen beholde tilgangsrettighet og må være i stand til å benytte den tilgjengeliggjorte informasjon for egen dokumentasjon av behandling og vurderinger.

Informasjoner og bilder må altså utleveres i hvert enkelt tilfelle og kun den relevante informasjon kan utleveres. Det samme gjelder for så vidt også internt i et behandlende helseforetak. Det skal ikke være automatikk i at ansatte i en gitt stillingskategori automatisk skal ha rettigheter til innsyn i vilkårlige pasientinformasjon.

Sett fra en klinikers synspunkt kan dette være en stor kjepp i hjulet for mulighetene til å utnytte ny teknologi for å gi et bedre helsetilbud og en bedre organisering av røntgentjenesten. Men det er fort å se seg blind på begrensningene i stedet for mulighetene. Datatilsynet vil sette foten ned for et system som er åpent og uten kontroll, og som ikke er i samsvar med det gjeldene lov- og regelverk. Hvis det kan dokumenteres at utvekslingen av informasjon er under kontroll og kan styres, er det enklere å få aksept for en løsning. Nøkkelen er dokumentasjon, risikovurdering, apparat for avvikskontroll og avvikshåndtering og oppfølging. Dette gjelder både for personell innad i helseforetaket og eksterne sin tilgang.

3. DICOM

Her gis en kort beskrivelse av DICOM standarden som benyttes i PACS systemer. Det presenteres muligheter for utveksling av bildeinformasjon og metoder for å ivareta informasjonssikkerheten.

De aller fleste løsninger for elektronisk bildearkivering til medisinsk bruk (PACS) gjør seg i dag nytte av DICOM-standarden i varierende grad. DICOM (Digital Imaging and Communication in Medicine) er et resultat av et standardiseringsarbeid med formål å kunne utveksle digitale bilder i et standard format uavhengig av utstyr- og programvareleverandører. DICOM er en omfattende standard og det finnes få systemer tilgjengelig som støtter standarden fullt ut.

For å vise hvilke deler av DICOM standarden som et PACS-system støtter legges det ofte ved en samsvarserklæring fra leverandøren som sier hvilke funksjoner i DICOM-standardens det aktuelle PACS systemet støtter.

3.1. Nettverk og tilgangskontroll med DICOM

Mekanismene for autentisering innebygd i DICOM v.3 (1993) er svake. Som eksempel kan en DICOM-applikasjon benytte portnummer, IP-adresse og DICOM AE_TITLE (nettverksidentitet i DICOM) til å autentisere en annen kommunikasjonspart. Portnummer og AE_TITLE kan enkelt modifiseres og det er også mulig å identifisere seg med falsk IP-adresse.

Supplement 31 til DICOM gir mulighet for å legge til sikrere løsninger. Ved å ta i bruk kryptering på transportnivå med protokollene TLS (Transport Layer Security) eller ISCL (Integrated Secure Communication Layer) kan to parter autentisere hverandre på en sikker måte og kryptere overføringen av bildedata om ønskelig. Autentiseringen er kun knyttet til kommunikasjonen mellom partene (DICOM applikasjonene), og protokollene gir ikke noen brukerautentisering eller sikring av informasjonselementer innenfor ende-applikasjoner. Autentisering av brukere må løses av den enkelte ende-applikasjon.

I regi av IHE (Integrating the Health Care Enterprise) er det etablert et rammeverk for integrasjon av it-systemer i en helsevirksomhet. Rammeverket beskriver hvordan standarder skal benyttes for å oppnå kommunikasjon på tvers av systemer og er delt inn i såkalte profiler for hvert anvendelsesområde. Ett av disse omhandler hvordan sikkerheten kan ivaretas i hele kjeden mellom to systemer og to brukere. Kort fortalt beskriver IHE denne prosedyren for autentisering og overføring:

1. Autentisering av bruker utføres av ende-systemet (f.eks. ved brukernavn og passord).
2. Ende-systemer (eller ende-system og tjener) autentiserer hverandre ved hjelp digitale sertifikater (over TLS).
3. Kommunikasjonen krypteres med TLS om ønskelig.
4. Transporten foregår over et skjermet nettverk.
5. Kommunikasjonen logges.

3.2. Innholdskryptering

Nåværende versjon av DICOM støtter ikke kryptering og tilgangsstyring på enkeltelementer eller attributter i et DICOM objekt. Men det er åpnet for kryptering av hele DICOM-objekter ved bruk av Cryptographic Message Syntax (CMS, RFC 2630) i en "Secure DICOM file". Hvis det kommuniseres direkte med PACS modaliteter vil dette vanligvis ikke være en tilgjengelig metode.

Kryptering av store røntgenbilder krever betydelig maskinkraft. Et godt alternativ til kryptering av selve bildedataene, er å kryptere informasjonen som knytter bilde til person og sensitive opplysninger. Dette kan gjøres ved å kryptere DICOM-header i en bildefil, men ikke selve bildedataene. DICOM-header inneholder metadata om bildeopptaket og den undersøkte. Med disse data gjort utilgjengelig for utenforstående vil ikke bildet lenger være å regne for sensitive personopplysninger. Ved bruk av en EDI-melding (XML/EDIFACT) kan meldingen være kryptert og koblet opp mot et ukryptert bilde som sendes sammen med EDI-meldingen (samme tekniske innpakking/konvolutt). Koblingen gjøres ved å pseudonymisere¹ personidentiteter i DICOM-header til bildefilene. EDI-meldingen må da inneholde informasjon som knytter nøkkelen brukt for pseudonymisering til de reelle personidentiteter som er beskrevet i EDI-meldingen.

¹ Opplysninger hvor identiteten til opplysninger er kryptert eller på annen måte skjult, men samtidig individualisert slik at det er mulig å spore en enkelt person uten at identiteten er kjent.

Kryptering av informasjonsobjektene som beskrevet over, gjør at kommunikasjonen kan gå på et åpent nettverk som helsenett eller Internett. Ved kun bruk av DICOM og proprietære RIS-løsninger hvor disse ikke er sikret, kan bruk av krypterte nettverkstunneler (VPN) være et alternativ for å sikre kommunikasjonen. Dette kompliserer kommunikasjonen og krever at hvert par av som skal utveksle bilder og bildeinformasjon må ha egnet utstyr.

Sendes bildet over en annen protokoll med web-services eller lignende, vil det være muligheter for å definere rigide sikkerhetsmekanismer. Men da må transaksjonene til utveksling av bilder defineres først, og disse finnes ikke i dag. Når eller hvis disse kommer, kan overføringen knyttes sammen med PKI (Public Key infrastructure) for å gi god sikring av informasjonen ende-til-ende.

3.3. Utlevering og tilgang

Et åpent system hvor alle parter som er gitt tilgang kan hente alle data er naturligvis veldig fleksibelt. Den som har behov for informasjon henter etter behov eller ønske. Like fullt må to samarbeidende parter på en eller annen måte bli enige om arbeidsflyt og rutiner seg i mellom. Utfordringen er at dette kan stride mot lover og forskrifter. Ved utlevering overføres kopi av informasjon til mottaker etter avsender sin beslutning. Mottaker kan da ikke hente informasjon etter ønske men må få aksept for en overlevering av avsender.

Forskjellen mellom utlevering og tilgang kan synes å være bagatellmessig i praksis. I forhold til lovverk og rutiner er forskjellen viktig. Hvis informasjon utleveres, trenger ikke avsender holde kontroll med hvem som til et hvert tilfelle skal ha tilgang. Mottaker av utlevert materiale skal også bare oppbevare sensitive personopplysninger når det er nødvendig. Det må altså utføres en forespørsel og en eventuell utlevering av informasjonen i stedet for at mottaker bare henter det som er av interesse. Teknisk kan dette løses på måter som gir tilgang til et informasjonsobjekt når det foreligger hjemmel og beslutning om utlevering. Hvorvidt informasjonsobjektet er lagret i avsenders eller i et felles lager skal prinsipielt ikke ha betydning så fremt det tilgangsrettigheter blir gitt til det aktuelle HF.

Løsninger med tilgang for eksterne synes å være attraktive blant enkelte pådrivere i helseforetakene. Motivasjonen for å løse utveksling av informasjon med tilgang til et system styrt av avsender er blant annet muligheten for kontroll med hvordan materialet presenteres for mottaker og hvordan mottaker kan nyttiggjøre seg informasjonen. Bruk av tilgang til system kontrollert av avsender ses også på som en mulighet for å trekke tilbake tilgangsrettigheter. En slik bruk kan komme i strid med mottakers dokumentasjonsbehov og eventuelle bevisførsel i en tvist. Det kan også påtvinge mottaker et

grensesnitt som gjør det vanskelig å integrere informasjonsflyten med mottakers eksisterende systemer. Med hensyn til mottakers muligheter for bruk av informasjonen og dokumentasjonsbehov vil det være et viktig prinsipp at det ikke skilles mellom oversendelse av informasjonsobjekter til lagring og behandling av mottaker, og tilgang til et grensesnitt som er strengt kontrollert av avsender. Ønsket kontroll med bruk av informasjonsobjekter må foregå i henhold til avtaler, lovverk og forskrifter – ikke ved bruk av tekniske mekanismer og påtvungne grensesnitt som avsender kan diktere.

Utleveringen av tilgang til et informasjonsobjekt eller oversendelse av en kopi av informasjonsobjektet kan formaliseres slik at det blir minimalt med byråkrati rundt dette. Men for at det skal bli mulig å gjennomføre i en større skala uten felles bildelager og RIS, for eksempel inter-regionalt, vil det være behov for å definere et sett med transaksjoner for utveksling.

3.4. Transaksjoner for utveksling

Standardisering av utlevering av røntgenbilder og pasientinformasjon kan gi et klart definert sett med transaksjoner. Disse vil gjøre det mulig for en hvilken som helst part å be om en utlevering, motta en utlevering og sende et svar på en forespørsel. Forespørslene kan håndteres delvis automatisk av endesystemene. Eksempelvis kan dette omfatte:

- Rekvirering av tolkning for røntgenbilde
- Rekvirering av ”second-opinion” til røntgenbilde
- Svar på tolkning av røntgenbilde
- Forespørsel om utlevering av røntgenbilder
- Svar på forespørsel om utlevering med eventuelle bilder

Bruk av DICOM-protokoller for kommunikasjon av dette på tvers av regionsgrenser og helseforetak blir fort vanskelig eller umulig med veldig mange kommunikasjonsparter. Sannsynligvis vil bruken av strukturerte meldinger (for eksempel XML) i kombinasjon med webservices være et aktuelt alternativ. Dette letter også kommunikasjonen og gir større fleksibilitet rundt kryptering, autorisasjon og tilgangskontroll.

Innholdet i transaksjonene er det bare brukerne som kan definere på en god måte. Dette må være fundert på behovet radiologimiljøet har. Det foregår prosesser for å definere slike transaksjoner for utveksling av journalinformasjon generelt. Mye av dette kan nok brukes direkte, men noen tilpassinger kan bli nødvendig for å understøtte særegne behov innenfor røntgen.

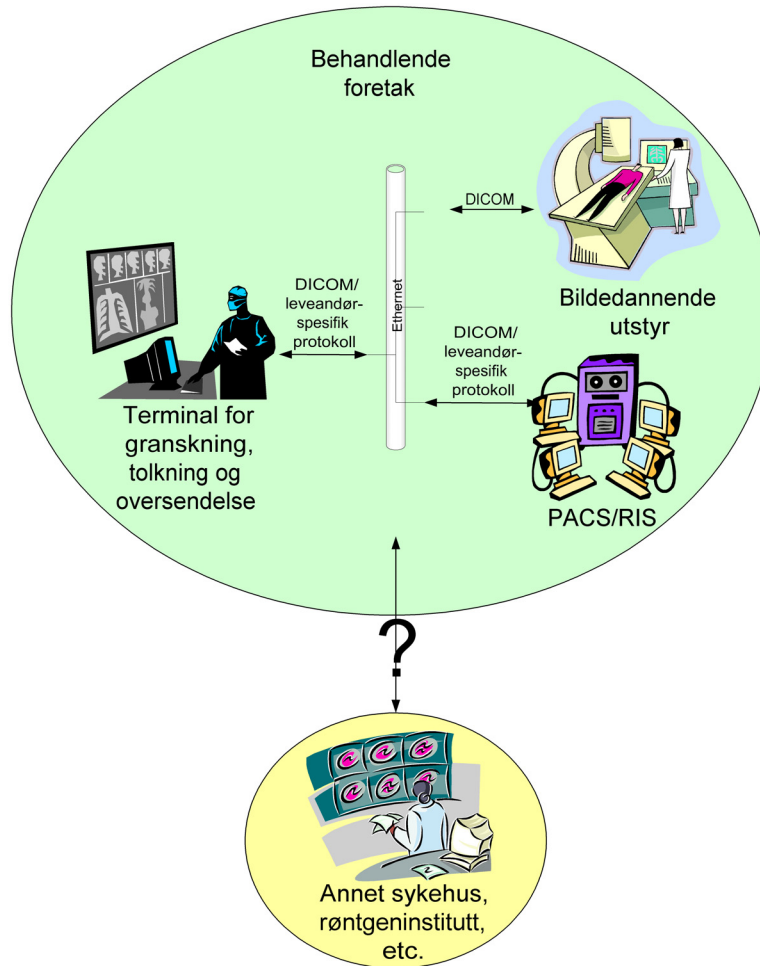
4. Modeller for utveksling mellom helseforetak

Her skisseres det kort de mest aktuelle PACS løsningene som er tilgjengelige i dag. Dette dreier som alt fra PACS løsninger som kjøres lokalt i en helsevirksomhet, til integrerte PACS/RIS løsninger som benytter seg av en sentral datalagerløsning.

Med utgangspunkt i tilgjengelige mekanismer for overføring av bilder mellom ulike PACS enheter er det satt opp alternative strategier og teknikker for utveksling av informasjon. Hovedutfordringen er hvordan en skal få til problemfri utveksling av PACS og RIS informasjon *mellom* helsevirksomheter/foretak innenfor det gjeldene lovverk. PACS informasjonsflyt *innad* i en røntgenavdeling er ivaretatt ved at røntgenutstyr og modaliteter bruker DICOM standarden ved kommunikasjon av PACS informasjon. Initiativer for integrasjon av systemer innenfor foretaksgrensen til et behandlende helseforetak er på sterk fremvekst. IHE – Integrating the Healthcare Enterprise er et eksempel på en organisasjon om arbeider med denne typer problemstillinger.

IHE beskriver i stor grad kun samhandling innen en helsevirksomhet og ikke mellom ulike helsevirksomheter. Det er derfor få (eller ingen) modeller for hvordan en bør bygge opp et rammeverk med tanke på samhandling på tvers av helseforetak. Norge og resten av Skandinavia er blant dem som er komst lengst innen bruk av PACS/RIS løsninger. Mens andre land er i startfasen med å innføre digital røntgen i helsevirksomheter er en i Norge komst så langt at elektronisk kommunikasjon *mellom* helsevirksomheter er blitt et aktuelt tema. Dette er trolig en årsak til at det finnes lite kunnskap om hvordan samhandling mellom helsevirksomheter bør foregå.

Under er det gitt en overordnet skisse over problemstillingen ved utveksling av røntgenbilder og røntgeninformasjon mellom helseforetak.



Figur 2: Hvordan overføres informasjon til en annen helsevirksomhet?

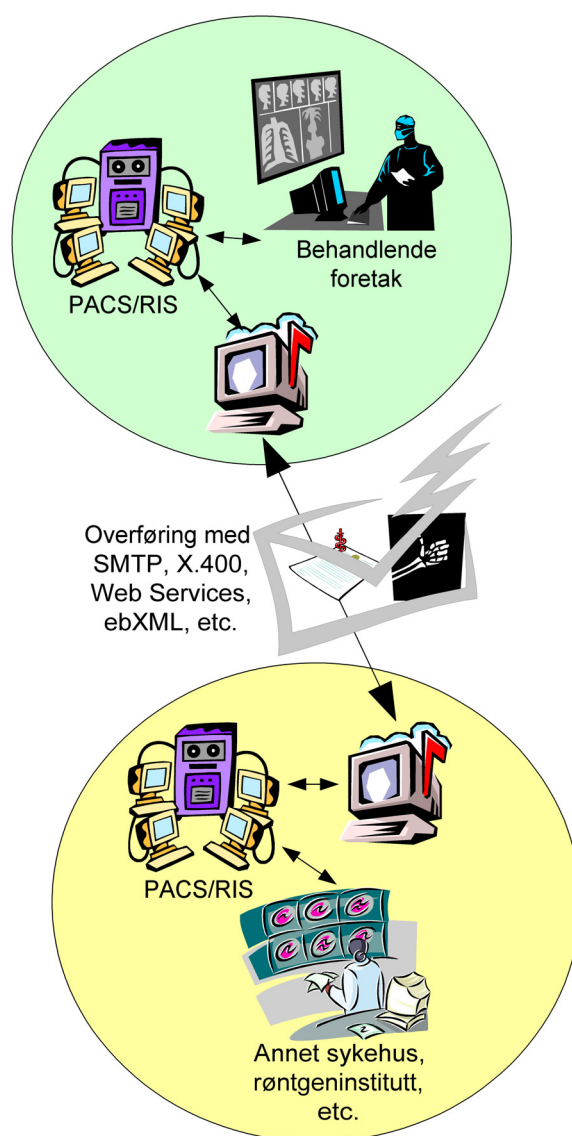
DICOM standarden håndterer kommunikasjon innen en helsevirksomhet (se kapittel 3). Utfordringen kommer når PACS og RIS informasjon skal kommuniseres på tvers av helseforetak. Ulike PACS systemer kan støtte ulike deler av DICOM standarden, og leverandører har varierende grad av integrasjon mellom PACS og RIS systemer.

Et problem er også at dagens PACS systemer har manglende funksjonalitet for historikk/sporbarhet til PACS informasjonen som mottas fra andre systemer.

Det som må til er støtte i PACS systemene for eksterne arbeidsprosesser og ikke bare interne arbeidsprosesser i helsevirksomheten. Dette er nødvendig skal en kunne få til samhandling på tvers av helseforetak og mellom ulike PACS systemer. Dette var blant annet et av temaene som kom frem under PACS workshopen som ble avholdt (se vedlegg A).

4.1. Lokal PACS + EDI

I denne varianten benyttes det lokale PACS og RIS i helsevirksomheten. Bilder og annen informasjon knyttet til bildeopptaket (journalelementer, etc) overføres til mottaker ved hjelp av standardisert svar- eller henvisningsmelding. Meldingssyntaks er uavhengig av overføringsprotokoll, slik at spesialiserte Web-services, ebXML-systemer eller tradisjonell e-post over X.400 eller SMTP kan benyttes. Svarmelding benyttes i sammenhenger hvor det svares på en forespørsel. Henvisningsmelding benyttes der hvor helseforetaket ber mottaker om bistand, ”second opinion”, etc. Figur 3 gir en oversikt for en slik løsning.



Figur 3: Overføring ved hjelp av EDI

4.2. Lokal PACS + Teleradiologi

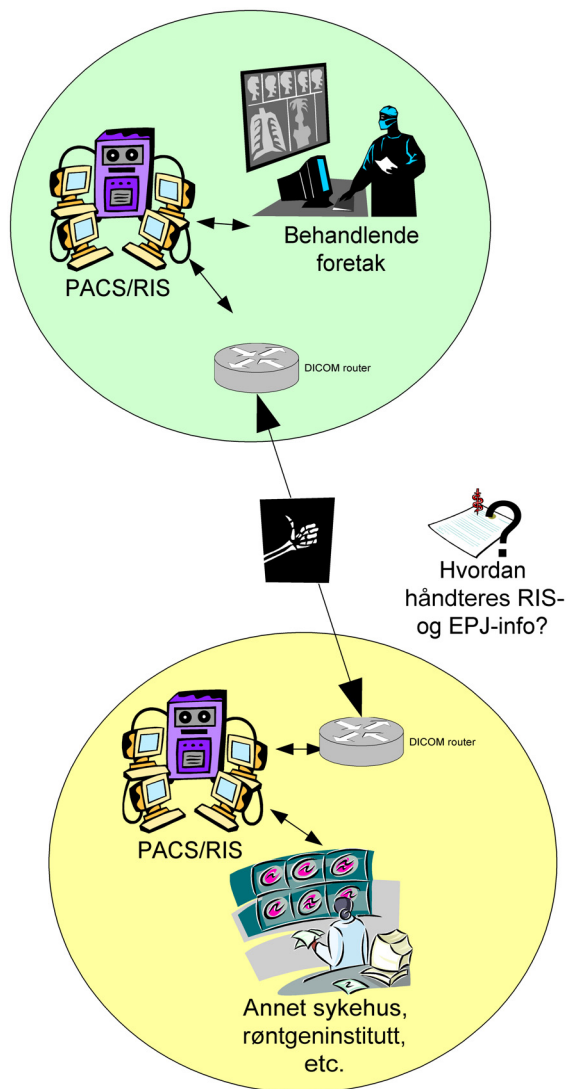
Dette er kanskje den mest vanlige konstellasjonen som benyttes i dag. Helseforetaket har eget PACS/RIS system og benytter en spesialtilpasset løsning for teleradiologi for å kommunisere med andre parter. I mange tilfeller vil løsningen basere seg på DICOM, men det er også vanlig at både avsender og mottaker må ha spesielt proprietært utstyr for overføringen. Overføring kan skje over ISDN, leide linjer, Internett eller andre kommunikasjonslinjer.

En slik løsning håndterer ikke RIS informasjon. Slik som løsningene er i dag må dette i stor grad behandles med manuelle prosedyrer med telefonsamtaler og telefaks.

4.3. Lokal PACS + DICOM over IP

Dette er for så vidt bare en variant av ovenstående, men med en litt annen teknisk løsning. Her benyttes lokalt PACS og kommunikasjonen foregår over IP med de andre enhetene. Dette kan tenkes foregå åpent over et helsenett, noe som kan være en noe tvilsom løsning med tanke på informasjonssikkerheten. Bedre alternativ kan være overførsel over private nett ved hjelp av nettverksteknikker som krypterte VPN (Virtuelt Privat Nettverk) eller VLAN (Virtuelt Lokalt Nettverk).

Også med en slik løsning vil det være utfordringer forbundet med håndtering av RIS informasjon. Figur 4 viser en oversikt over en slik løsning.



Figur 4: Lokal PACS med overføring via DICOM

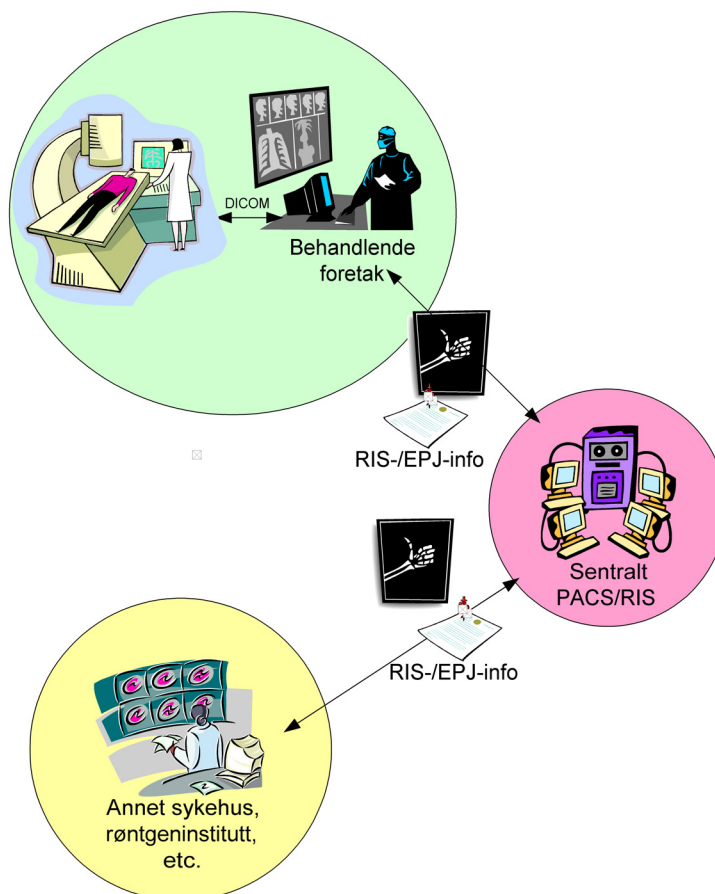
4.4. Lokal PACS og synkronisering/overføring mot sentral PACS

Et løsning med sentralt PACS system åpner for å kunne redusere behovet for å håndtere alt bildemateriale på lokalt PACS system. Dette kan være implementert på en slik måte at lokal PACS benyttes til en begrenset produksjon (en dag, eller en uke) og bilder overføres til sentral PACS for arkivering. Lokal PACS kan også øke driftsikkerheten ved at en ikke er fullt ut avhengig av tilgang til det sentrale lageret. En sentral løsning kan også gjøre det enklere å implementere funksjonalitet som

gjør deling og utveksling av PACS bilder mulig mellom helseforetak som er tilknyttet. Region Midt-Norge har under innføring en RIS/PACS løsning med lokal PACS og synkronisering mot sentralt lager.

4.5. Kun sentral PACS

Dette er en avart av ovenstående hvor bufring og lager ikke finnes lokalt, og er den løsningen som i størst grad bygger på samarbeid mellom helsevirksomheter. Alle bilder som skal lagres hos en DICOM Storage Class Provider (SCP) sendes over nettverk til sentral SCP. Tilgjengeligheten til nettverkforbindelsen mellom bruker og opptaksutstyr til sentralt lager blir kritisk ved en slik løsning.



Figur 5: PACS løsning med sentralt lager

Figur 5 viser hvordan en slik løsning fungerer. All informasjon ligger kun i det sentrale lageret og aktuelle helsevirksomheter kommuniserer kun til det sentrale lageret. En slik løsning kan også inneholde RIS integrasjon slik at både RIS og PACS informasjon ligger lagret i det sentrale lageret. Utveksling av informasjon mellom ulike helsevirksomheter foregår via sentralt lager.

Utfordringer og problemer knyttet til samhandling og kommunikasjon av PACS/RIS informasjon mellom de involverte helseforetakene blir i stor grad løst ved å velge en løsning med sentral PACS. En bakdel med slike løsninger er de ikke nødvendigvis løser problemer knyttet til samhandling/kommunikasjon mot andre typer PACS systemer. Det samme gjelder mot helseforetak som ikke er med i den sentrale PACS løsningen, for eksempel i andre helseregioner.

4.6. Web-grensesnitt i kombinasjon med sentral eller lokal PACS

Dette er noe mange leverandører kan tilby. Det gir muligheten for at klinikere eller eksterne kan få tilgang til PACS/RIS via en webleser. Tilgangsstyringen er da spesialtilpasset den aktuelle løsningen og det benyttes ofte brukernavn og passord for autentisering. Håndtering av tilgangsstyringen kan bli en omfattende oppgave ved denne typen løsninger.

5. Informasjonssikkerhet ved felles fysisk datalagerløsning for digital røntgen

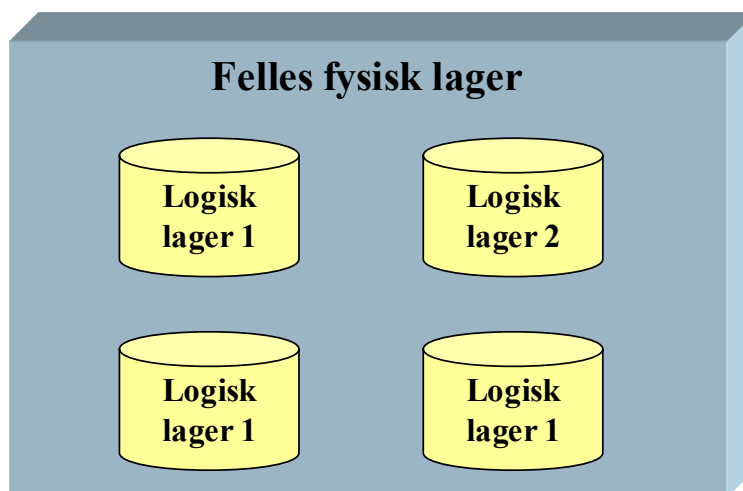
Felles datalagerløsninger for fysisk bildelager mellom helsevirksomheter er aktuelt ved innføring av digital røntgen. Her tas det opp hvilke muligheter slike løsninger kan gi og det beskrives aktuelle trusler mot informasjonssikkerheten ved felles datalagerløsninger.

En felles datalagerløsning vil i denne sammenhengen være at flere helsevirksomheter samarbeider om en felles fysisk arkivløsning (bildelager) for PACS/RIS informasjon. Samarbeid kan for eksempel omfatte flere helsevirksomheter som danner et helseforetak eller alle helseforetak innenfor en helseregion.

Fysisk samlokalisering av et datalager betyr ikke at lageret fungerer som et lager hvor alle har tilgang til alle dataobjekter. Lagringen kan foregå slik at grupper av dataobjekter kan skilles logisk fra hverandre. Det logiske lageret sier noe om hvordan det fysiske lageret er delt opp og fungerer mot ulike brukere av lageret.

Eksempelvis kan et felles fysisk datalager mellom to helseforetak deles opp i to logiske lager. Hvert helseforetak får da adgang til hver sin logiske del av den felles datalagerløsningen.

Logiske lager i et felles fysisk datalager kan deles opp med vanntett skott slik at de logiske lagrene fungerer som to uavhengige og selvstendige lager. Dvs. at de ikke deler noen felles data og at et helseforetak kun har tilgang til sine tilhørende data.



Figur 6: Fysisk og logisk lager

Figuren over viser en enkel skisse over hvordan et felles fysisk datalager kan deles opp i flere logiske lagere. I dette eksemplet kan hvert av de logiske lagrene tilhøre ulike helseforetak i en helseregion.

Det finnes andre metoder for å dele opp et datalager på enn med logiske lagere. Bruk av ulike identifikatorer knyttet for eksempel til hver helsevirksomhet kan også nyttes for å skille informasjonen i en felles datalagerløsning. Uansett metode må en tilfredsstillende lovverket som sier at deling av pasientinformasjon mellom helseforetak ikke er tillatt.

Informasjonssikkerhet

Det er ikke gått i detalj i vurdering av de ulike truslene mot en felles datalagerløsning. Det er satt fokus på hvordan de ulike truslene kan true sikkerheten til informasjonen på følgende områder:

- ❑ **Konfidensialiteten** - at informasjonen gjøres utilgjengelig for uautoriserte
- ❑ **Tilgjengeligheten** - informasjonen er tilgjengelig for autorisert tilgang når det er behov for det
- ❑ **Integriteten** - at informasjonen er ikke endret, slettet, lagt til eller på annen måte endret av andre enn de som har hatt autorisert tilgang til informasjonen
- ❑ **Sporbarhet** - det å kunne produsere bevis, av en eller annen styrke, i ettertid for at en gitt hendelse virkelig fant sted

Det er i denne rapporten ikke lagt så stor vekt på å kartlegge tradisjonelle trusler ved datalagerløsninger. En årsak til dette er at slike trusler er relativt godt kjent og slike trusler er ofte de samme for ulike datalagerløsninger. Prinsipp om for eksempel redundante løsninger eller backup er

ting som etter hvert begynner å bli godt kjent. I KITH rapport nr. 21/02 ”Driftssikkerhet ved bruk av kritiske IT-systemer i helsevesenet” blir aktuelle tema beskrevet nærmere.

En annen årsak er at vi ikke ser de tradisjonelle truslene som den største utfordringen ved felles datalagerløsninger for PACS løsninger. Vi ser større problemer med å løse utfordringer knyttet til hvordan en skal utforme felles løsninger som tilfredsstillende det gjeldende lovverket. Eksempelvis er tilgang og utlevering av informasjon på tvers av helseforetak nevnt som en av de største utfordringene en må løse i forhold til felles PACS løsninger.

5.1. Rammebetingelser

Aktuell lovgivning påvirker bruken av felles fysiske datalagerløsninger som deles mellom flere helseforetak (se kapittel 2).

Vi vil i første omgang trekke frem noen sentrale punkter som kan påvirke aktuelle løsninger:

- ❑ **Helseregisterloven og Helseforetaksloven** - som sier at deling av pasientinformasjon mellom helseforetak ikke er tillatt. Dette skaper restriksjoner for tilgangen til en felles bildelagerløsning og tilgang til informasjon på tvers av helseforetak.
- ❑ **Personopplysningsloven** - som sier at det er den behandlingsansvarlige som skal sørge for tilstrekkelig informasjonssikkerhet (dette gjelder også ved utlevering av data til en annen helsevirksomhet). Datalagerløsninger med felles fysisk bildelager kan forenkle denne prosessen.

Fra Helseregisterloven og Helseforetaksloven følger det at deling av et felles bildelager mellom flere helseforetak hvor helseforetakene har tilgang til all informasjon i lageret er ulovlig. Uansett om det er snakk om lokale eller felles bildelager skal et helseforetak i utgangspunktet bare ha tilgang til data som de eier selv.

Tilgang til data i et felles datalager må skille på tilgang fra de ulike helseforetakene. Det at dataene ligger i et felles fysisk lager trenger ikke bety full tilgang til all informasjon i lageret. Selv om de lokale bildelagene blir samlet på et fysisk sted skal fortsatt hvert helseforetak bare ha tilgang til sitt lokale lager i en felles datalagerløsningen.

Personopplysningsloven gir ikke noen direkte retningslinjer med hensyn på tilgang og deling av data. Den sier derimot at det er den behandlingsansvarlige sitt ansvar å vurdere om sikkerhetsnivået er tilstrekkelig ved utlevering av informasjon til en motpart. Dette inviterer til at for eksempel regioner

samkjører implementering av felles systemer med tilhørende felles sikkerhetsmekanismer slik at en vet at mottakerne har tilfredsstillende informasjonssikkerhet.

5.2. Muligheter ved felles datalagerløsninger

En felles bildelagerløsning vil gi samlokalisering av data mellom flere ulike helsevirksomheter, for eksempel innen et regionalt helseforetak. Dette vil blant annet kunne gi reduserte drifts- og utstyrs kostnader. I helseregion Midt-Norge skjer det for eksempel en samkjørt innføring av PACS/RIS system for alle helseforetak med lagring av PACS/RIS informasjon i en felles datalagerløsning som er lokalisert til Trondheim.

Den mest opplagte muligheten som følge av en felles fysisk datalagerløsning er at helsevirksomhetene også har samarbeid om drift eller samordnet drift av det felles fysiske datalageret. Dette kan gi reduserte kostnader ettersom flere virksomheter benytter en felles datalagerløsning. Felles innsats rundt en sentral datalagerløsning vil sannsynligvis også kunne gi bedre resultater med tanke på informasjonssikkerheten enn dersom hvert helseforetak skulle hatt sin egen lagerløsning.

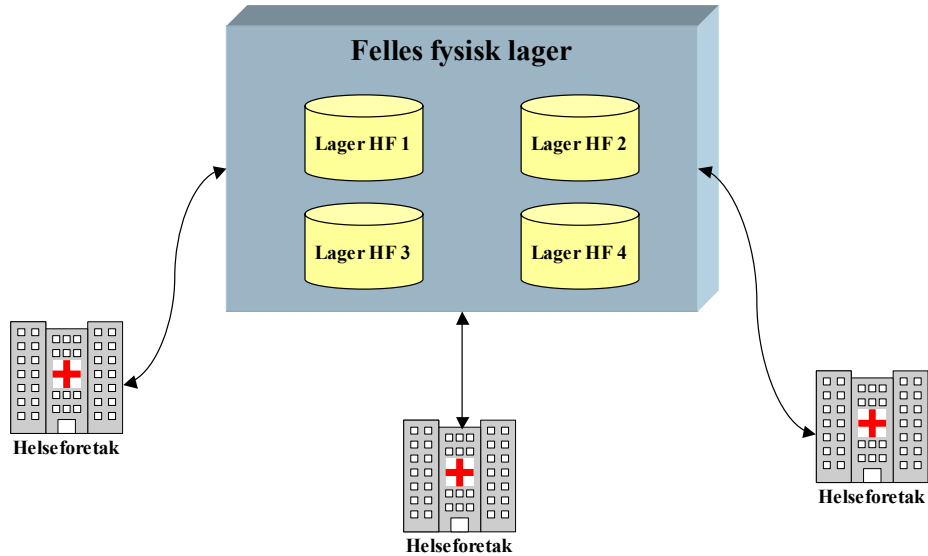
Felles systemløsninger

Felles systemløsninger for PACS og RIS mellom flere virksomheter er ikke en direkte følge av felles fysisk lager, men kan komme av at det etableres et samarbeid i forbindelse med anskaffelsen av felles datalagerløsninger. Felles systemløsninger ved brukerstedene vil kunne forenkle standardiseringen og samhandling og gi bedre muligheter for utveksling og kommunikasjon av informasjon.

Felles datalagerløsninger kan i midlertidig være uavhengige av hvilket PACS system som det enkelte helseforetaket velger å benytte seg av.

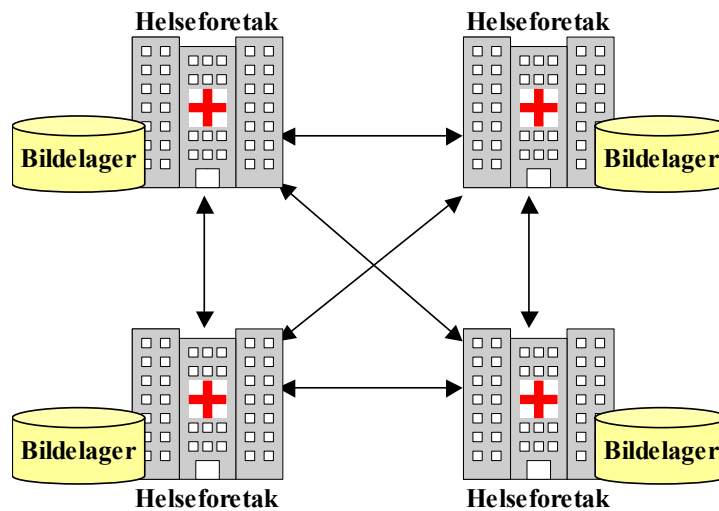
Bedre grunnlag for utveksling av data

Bedre grunnlag for utveksling av informasjon kan oppnås fordi data ligger samlet i et felles fysisk bildelagret og må ikke sendes fysisk fra et helseforetak til det andre når det skal utveksles.



Figur 7: Utsveksling via et felles fysisk lager

Utsveksling av informasjon på tvers av helseforetak kan skje ved at det gis tilgang til data som ligger i logiske lager i det felles fysiske lageret og at det hentes derfra til det aktuelle helseforetaket. Felles datalagerløsninger kan bidra til at en unngår at ulike implementeringer av PACS bildearkivene fører til problemer ved utveksling/tilgang til data på tvers av helseforetak.



Figur 8: Utsveksling direkte mellom HF

Figuren over viser hvordan utveksling av data foregår dersom en ikke har en løsning med fysisk felles bildelager mellom de ulike helseforetakene. I dette tilfellet må data gå direkte fra et helseforetak til et annet. Med flere helseforetak og kanskje private aktører inne i bildet vil det etter hvert bli mange mulige kommunikasjonsveier å forholde seg til.

Samarbeid mellom virksomheter

Felles fysisk bildelager kan danne grunnlaget for samarbeid mellom helsevirksomheter. Eksempel på dette er vaksamarbeid mellom helseforetak både innen og mellom ulike regionale helseforetak.

En utfordring som må håndteres ved denne typen samarbeid er hvordan tilgang til data skal gis på tvers av helseforetak. Ved vaksamarbeid må en kanskje ha rask tilgang til data (for eksempel ved ulykker), men dagens helselovgivning tillater ikke at helseopplysninger er tilgjengelige fra et annet helseforetak uten at tilgang gis eller materiale utleveres for hvert enkelt tilfelle. Prosedyrer og løsninger for gi rask tilgang til data må derfor utvikles, og disse må forholde seg til gjeldende lover og regelverk.

Informasjon raskt tilgjengelig

Dette punktet kan variere avhengig av hvilke løsninger som en velger å implementere. Informasjon også lagres lokalt på det aktuelle helseforetak selv om en har en felles datalagerløsning. Dette gjøres først og fremst for å kunne opprettholde lokal drift dersom en ikke skulle ha tilgang til det felles lageret.

Dersom PACS informasjon blir overført til det felles bildelageret vil det da kunne være tilgjengelig for tilgang fra andre helsevirksomheter omtrent umiddelbart etter at PACS bildene er tatt. Dersom det velges en løsning hvor informasjon ikke blir overført til det felles lageret før etter at det slettes fra det lokale lageret på det helseforetak vil en ikke kunne få de samme fordelene.

Samordning av nivå på informasjonssikkerheten

Som nevnt er den behandlingsansvarlige som må sørge for tilstrekkelig informasjonssikkerhet, dette gjelder også ved utlevering av informasjon til en annen helsevirksomhet. En løsning som inkluderer bruk av felles fysisk bildelager vil kunne forenkle en slik vurdering av motparten fordi en da vet hvilken sikkerhet motparten bruker i forbindelse med det felles fysiske lageret.

5.2.1. Ulemper med felles datalagerløsning

Selv om det er mange fordeler med felles datalagerløsninger finnes det også noen ulemper med slike løsninger. Tilgangskontroll og tilgangsstyring vil trolig bli blant de største utfordringene i forbindelse med en delt datalagerløsning. I kapittel 5.3 beskrives det nærmere problemstillinger rundt tilgangshåndtering til en sentral datalagerløsning.

Andre ulemper er at en gjør seg i stor grad avhengige av kommunikasjonslinjene til en felles datalagerløsning og kan være sårbare dersom disse ikke er tilgjengelige. Avhengighet til kommunikasjonslinjer og andre trusler mot informasjonssikkerheten blir behandlet under trusselvurderingene i kapittel 5.4-5.6.

5.3. Tilgangshåndtering

Tilgangskontrollen blir et sentralt punkt ved PACS/RIS løsninger som benytter seg av felles datalagerløsninger. Datatilsynet har i det siste hatt særskilt fokus mot helsevesenet og noe av det de påpeker er dårlig og manglende tilgangskontroll og at det nærmest blir gitt fri tilgang både innad og på tvers av helseforetak.

Tilgangskontrollen til et felles datalager må skille mellom tilgang fra de ulike helseforetakene. Brukere fra et helseforetak skal også bare ha tilgang til data som tilhører det aktuelle helseforetaket. En løsning som ikke skiller på brukertilgang fra de ulike helseforetakene vil komme i konflikt med gjeldene regelverk. I forbindelse med strategi for tilgangskontroll er det naturlig å se på hvordan det fysiske datalageret er bygd opp. Et datalageret oppdelt i logiske lager tilhørende de ulike helseforetakene som det er ”vanntette skott” mellom vil gjøre det enklere å få til en god styring med tilgangskontrollen.

Tilgang på tvers av helseforetak

Et aktuelt problemområde er hvordan tilgang til data på tvers av helseforetak håndteres. I følge Helseregisterloven og Helseforetaksloven kan ikke flere helseforetak dele på pasientinformasjon, og tilgang til informasjon må avtales i hvert tilfelle (blant annet loggføres). I tillegg til en faglig hjemmel og samtykke fra pasienten, kreves det også en aktiv handling for å få tilgang til pasientopplysninger på tvers av helseforetak. En kan langt på vei automatisere en slik handling (for eksempel en slags ”henvisning-svar” modell), men Datatilsynet legger stor vekt på at noen hos det databehandlingssansvarlige helseforetak gjør en vurdering av hver slik henvendelse. Eksempelvis kan

det tenkes at et tastetrykk er nok for å godkjenne tilgang fra et annet helseforetak, noe som er til dels mye lettere enn de manuelle prosedyrene som benyttes noen steder i dag.

5.4. Konfidensialitet

En løsning med et felles datalager vil kunne gjøre det enklere å få til en samordning av autorisasjon og tilgangskontroll til det felles datalageret. Ulike helsevirksomhetene vil da kunne benytte samordnet løsninger for autorisasjon og tilgangskontroll. Dette vil gjøre det enklere å integrere sikkerhetsløsninger på tvers av helsevirksomheter og oppnå et felles sikkerhetsnivå som gjelder for flere helsevirksomheter. Dette kan hjelpe til med å få en sikkerhetsløsning hvor det ikke finnes et svakt ”ledd” hos en av ulike helsevirksomhetene, men hvor alle punkter som foretar tilgangskontroll til et felles datalager har samme sikkerhetsløsning og samme sikkerhetsnivå.

Med en slik samordnet tilgangskontroll kan en for eksempel unngå at en dårlig sikkerhetsløsning hos et helseforetak gjør at noen får tilgang til opplysninger som tilhører andre helseforetak.

5.4.1. Trusler mot konfidensialiteten

Ved et felles fysisk bildelager er det først og fremst to grupper som kan utgjøre en trussel mot konfidensialiteten til PACS informasjon:

1. **Ansatte i helsevesenet** som utnytter sine rettigheter til å få urettmessig tilgang til sensitiv pasientinformasjon
2. **Utenforstående** som prøver å få tilgang til informasjon i en felles bildearkiv:
 - Avlytting av data ved overføring
 - Uautorisert tilgang til brukernavn og passord
 - Ondsinnet kode (for eksempel en trojansk hest som sender ut informasjon) som kan føre til at utenforstående får tilgang til informasjon lagret i en felles datalagerløsning.

5.4.2. Ansatte i Helsevesenet

Helsevesenet er en stor arbeidssektor med mange tusen ansatte. Eksempelvis har St Olavs Hospital (Universitetssykehuset i Trondheim) ca 5.500 ansatte og Helseregion Midt-Norge har ca 14.000 ansatte. Totalt dreier det seg altså om flere titusen ansatte i helsevesenet i Norge som kan ha tilgang til pasientinformasjon av ulik karakter.

Det er ikke noe grunnlag for å påstå at ansatte i helsevesenet med viten og vilje utnytter sin posisjon til å skaffe seg ukorrekt tilgang til sensitive pasientopplysninger. Det kan derimot heller ikke avvises at ansatte i helsevesenet skulle kunne bruke sine rettigheter til å skaffe seg urettmessig tilgang til pasientopplysninger. Med flere titusen ansatte i helsevesenet er sannsynligheten for at noen vil utnytte tilgangen de har til sensitive personopplysninger kanskje større enn man tror. Eksempelvis kan det tenkes at nysgjerrighet på naboer/familie fører til at man utnytter den tilgangen en har til helseopplysninger.

Statistikker om datakriminalitet viser også i økende grad at egne ansatte utgjør en stadig større trussel mot informasjonssikkerheten i egen bedrift. Hos noen bedrifter utgjøre faktisk egne ansatte en større trussel enn trusler utenfor virksomheten.

Mulige tiltak

Det er vanskelig (for ikke å si umulig) å gardere seg mot at ansatte i en organisasjon utnytter den tilgangen de har til sensitiv informasjon. En kan innskrenke de ansattes tilgang til pasientinformasjon for å redusere sannsynligheten for at noen bruker informasjonen på en urettvis måte.

Ansatte må i midlertidig ha tilstrekkelige adgangsrettigheter til informasjon for å kunne utøve en effektiv og sikker behandling av pasienter. Innskrenkning av tilgangsrettigheter vil derfor bare delvis kunne fungere som et tiltak for å bedre konfidensialiteten.

Overgangen fra papir til elektronisk lagring av dokumenter gir mange fordeler, men det kan også gi ulemper. For eksempel kan en papirkopi bare leses av en person av gangen, mens nesten et ubegrenset antall personer kan i utgangspunktet lese elektronisk lagret informasjon. Det er derfor viktig med tiltak som loggføring og kontroll-/rapporteringsrutiner slik at eventuelle ”urettmessige” tilganger til pasientinformasjon kan oppdages og/eller spores tilbake dersom det blir behov for det.

5.4.3. Utenforstående

Utenforstående som av ulike grunner ønsker å få tilgang til data vil alltid være en trussel ved bruk av IT-systemer. PACS bilder med tilhørende RIS data kan være sensitiv personinformasjon slik at det er viktig at konfidensialiteten er godt bevart.

Mulige tiltak for å sikre konfidensialiteten kan være:

- Bruk av sterk autentisering i tillegg til at eventuelle brukernavn og passord bør krypteres
- Kryptering av innhold ved oversendelse av informasjon

- ❑ Bruk av ”lukket nettverk” som er sikret (VPN eller VLAN) og/eller som ikke er tilkoplek eksterne nettverk (for eksempel Internett)
- ❑ Benytte seg av viruskontroll og brannmur slik at eventuell ondsinnet kode ikke kommer inn i et nettverket som er tilknyttet en felles bildelagerløsning

PACS/RIS informasjon kan utgjøre store datamengder (et PACS bilde er ofte 5-10 MB) slik at kryptering på transportnivå kan kreve relativt store ressurser når en ser på antall PACS overføringer og datamengdene. Et mulig alternativ er derfor å benytte seg av sikre kommunikasjonskanaler (for eksempel VPN) slik at en unngår at mye ressurser går med til kryptering av dataene som skal overføres. Alternativt kan bare deler av informasjonen krypteres slik at koblingen mellom personidentitet og persondata forsvinner (se kapittel 3)

5.5. Tilgjengelighet

Det kan gi store konsekvenser dersom et felles datalager ikke er tilgjengelig og det er derfor viktig med en stabil driftsløsning. Dersom flere helseforetak går sammen om et felles datalager vil dette kunne gi løsninger med bedre tilgjengelighet enn dersom hvert helseforetak skulle drifte sin egen løsning. Høy tilgjengelighet krever ofte redundante løsninger, noe som kan bli kostbart dersom en krever tilnærmet 100% oppetid på systemet. At flere helsevirksomheter går sammen om felles drift av en sentral datalagerløsning kan trolig også gi en billigere løsning totalt sett.

5.5.1. Trusler mot tilgjengeligheten

Det settes generelt høye krav til tilgjengelighet for IT-systemer innen helsevesenet og dette blir ekstra viktig dersom en velger løsninger med felles datalagerløsninger for flere helsevirksomheter. En situasjon hvor en felles bildelagerløsning for en helseregion ikke er tilgjengelig er lite ønskelig og kan få store konsekvenser.

Aktuelle trusler mot tilgjengeligheten er:

- ❑ **Tjenestenektingsangrep** - dette er en type angrep som er en av de mest økende formene for datakriminalitet og vil kunne utgjøre en reell trussel.
- ❑ **Systemfeil i bildelager** - dette er feil som skjer i selve det fysiske bildelageret, noe som kan inkludere disk, strømforsyning, backup system eller andre komponenter.

- ❑ **Komponentfeil på kommunikasjonslinjer** – dette er feil som kan oppstå mellom det fysiske bildelageret og det enkelte helseforetak som er tilknyttet det felles lageret. Hvor kritisk en linjefeil er avhenger av hvor lenge data lagres på den lokale helsevirksomheten. Uansett vil en linjefeil føre til at utveksling av data til/fra det felles lageret og mellom helsevirksomheter ikke kan gjennomføres.

5.5.2. Tjenestenektingsangrep (DOS-angrep)

Det er i utgangspunktet ikke noe enkelt middel for å unngå DOS angrep fordi et slikt angrep i utgangspunktet benytter seg av lovlige midler, for eksempel å stresse en tjeneste med så mye data at hele tjenesten bryter sammen. Et mulig DOS angrep mot et felles bildelager kunne være å sende så mye data på kommunikasjonslinjene at eventuelle forsøk fra tilkoblede helsevirksomheter på å overføre data mislykkes.

Den mest effektive måten å redusere risikoen for DOS angrep er trolig å benytte seg av nettverk som har færrest mulig tilknytninger til andre nettverk og som ikke er tilknyttet eksterne nettverk (som for eksempel Internett). Ved å benytte nettverk som har streng tilgangskontroll utenfra og inn vil risikoen for å oppleve DOS angrep også kunne reduseres.

5.5.3. Feil i bildelager og linjer

Feil i det felles bildelageret kan være alt fra feil på disker eller backup-system til feil på rutere eller strømforsyning. Redundante løsninger er trolig den beste måten å unngå at feil på komponenter fører til at tilgang til lageret ikke er mulig. En slik løsning må være slik at komponentfeil i systemet ikke fører til at systemet bildelageret blir utilgjengelig (kjent som ”singel point of failure”).

Dette kan innebære at en må ha alternative kommunikasjonslinjer fra de ulike helsevirksomhetene og inn til det felles fysiske lageret. Et annet moment er at en bør bruke komponenter som er ”standardvare”, slik at det eventuelt er lett å få tak i nye reservekomponenter dersom noe skulle være feil.

Et annet viktig moment vil være hvordan backup systemet fungerer. Det vil være relativt store datamengder i et slikt felles bildelager slik at en gjenoppretting etter en feil må være effektiv med

tanke på de store datamengende som kunne måtte gjenopprettes. I Midt-Norge hvor det er etablert en felles fysisk datalagerløsning er det derfor valgt en backup løsning basert på RAID 1 med full speiling av dataene i bildelageret. Dette er ikke den enkleste og rimeligste løsningen, men de store datamengende kombinert med kravet til høy tilgjengelighet gjorde at en slik løsning med fullt ut speilet backup data ble valgt.

Etablering av Nasjonalt Helsenett som et transittnett for helseinformasjon kan være med på å redusere risikoen for at feil i nettverk fører til at en felles bildelagerløsning ikke er tilgjengelig.

5.6. Integritet

Ved et felles fysisk datalager vil det kunne være naturlig at de involverte helsevirksomheter nytter seg av et eget dedikert nettverk til PACS/RIS kommunikasjon fra/til det fysiske lageret. Et slikt eget nettverk vil være med på kunne opprettholde høy tilgjengelighet, men vil også kunne hindre utenforstående i å få tilgang til dataene i nettverket.

Ved å benytte seg av et dedikert ”lukket” PACS nettverk vil en også kunne redusere risikoen for at ondsinnet kode eller DOS-angrep (eller andre ondsinnede angrep) skal ødelegge integriteten til dataene og også opprettholde tilgjengeligheten til nettverkslinjene.

5.6.1. Trusler mot integriteten

Aktuelle trusler mot integriteten er:

- ❑ **Ondsinnnet kode** - dersom for eksempel virus eller trojanske hester kommer inn i nettverket hvor informasjon blir sendt til/fra det sentrale bildelageret, kan dette slette eller endre dataene.
- ❑ **Feil i lagringsenhet** - dersom det skulle skje en feil i bildelageret (disker, backup rutiner) kan dette føre til at informasjonen går tapt eller blir endret
- ❑ **Avlytting av informasjon** - dersom noen avlytter kommunikasjonslinjene som er tilknyttet bildelagret kan det være mulig å ”snappe” opp data og endre de før de sendes videre til bildelageret.
- ❑ **Uautorisert innlogging** - dersom noen som ikke er autorisert for tilgang greier å logge seg inn på systemet kan disse for eksempel slette eller foreta endringer i dataene i det felles bildelageret.

5.6.2. Ondsinnet kode

Ondsinnet kode er en de mest vanlige formene for datakriminalitet og mange virksomheter med IT-utstyr opplever dette i dag. Det er vanskelig å sikre seg 100 % mot ondsinnet kode, men det er kanskje spesielt to tiltak som kan redusere risikoen ondsinnede angrep. Det ene er å benytte seg av virusprogramvare og den andre er ha så få tilknytninger til eksterne nettverk som mulig.

5.6.3. Feil i lagringsenhet

Feil i lagringsenheten er nevnt tidligere og som da er løsningen her å benytte seg av redundante løsninger som gjør at en feil i komponent ikke fører til at data blir tapt eller endret. Igjen presiserer vi at en redundant løsning må omfatte alle komponenter som inngår i systemet for det felles fysiske bildelageret. Det er for eksempel ingen nytte i at selv bildelageret er fullt ut redundant dersom en ruter svikter slik at en helsevirksomhet ikke får tilgang til lageret.

5.6.4. Avlytting av informasjon

Det sikreste og enkleste måten å unngå at noen avlytter informasjonen som blir sendt over nettverket er å ikke tilknytte det noen eksterne nett slik at kommunikasjonslinjene som benyttes er isolerte. Et annet tiltak er å benytte seg av sikre linjer (som er krypterte) slik at ingen får nytte av dataene dersom de skulle greie å avlytte data på kommunikasjonslinjene.

5.6.5. Uautorisert innlogging

Uautorisert innlogging kan trolig best unngås ved å bruke bedre autentisering enn bare brukernavn/passord av brukere som skal logge seg inn på systemet. Andre tiltak kan være krav til passord (for eksempel krav til både tall og bokstaver) og ev. bruk av sterk autentisering som for eksempel bruk av smartkort. Kryptering av brukernavn/passord ved innlogging til systemet vil også kunne hindre uautoriserte i å få tak i gyldige brukernavn/passord.

5.7. Sporbarhet til data

En felles fysisk datalagerløsning kan gi en samlet oversikt over all PACS/RIS informasjon innen for eksempel en helseregion. Kombinert med loggføring og kontrollrutiner vil dette kunne gi god sporbarhet til bruk av informasjonen som lagres i en sentral datalagerløsning.

Det stilles krav om at tilgang til opplysninger som er gitt til et annet helseforetak skal kunne føres inn i pasientjournalen til aktuell pasient. En må derfor kunne spore hvem som har hatt tilgang til informasjonsobjekter for å kunne se om tilganger for eksempel er gjort på tvers av helseforetak.

Ved å bruke for eksempel sterk autentisering eller digitale signaturer kan en på en sikker måte vite hvem som har hatt tilgang til data. På denne måten kan en også sikre seg at en forespørsel om utlevering eller tilgang til sensitiv informasjon faktisk kommer fra en sikker kilde (for eksempel et annet helseforetak)

Trusler mot sporbarheten

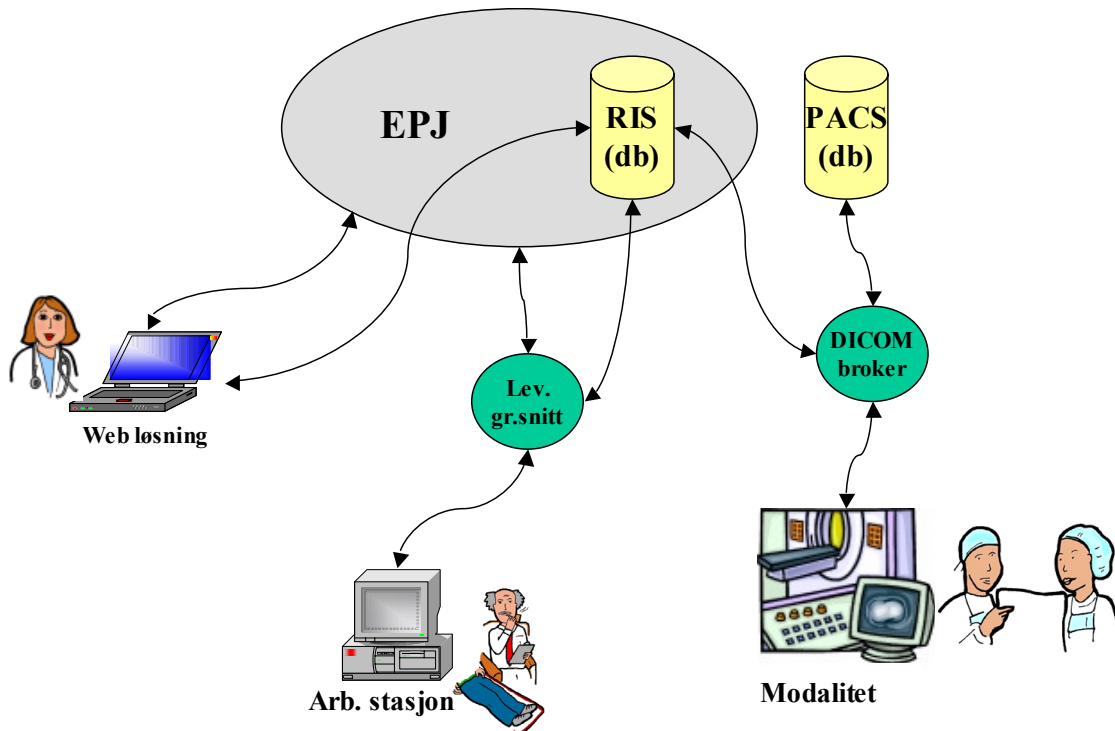
Det er vanskelig å identifisere noen klare trusler mot sporbarheten til informasjon. Det er i midlertidig klart at manglende funksjonalitet for å kunne spore tilbake hva som faktisk har skjedd svekker sporbarheten til informasjonen.

En svakhet med dagens PACS systemer er at de ikke har funksjonalitet for historikk når en mottar data fra andre PACS systemer. Dette har sammenheng med at dagens PACS systemer kun har støtte for interne arbeidsprosesser og ikke eksterne.

Etter hvert som elektronisk utveksling og samhandling mellom helseforetak blir mer utbredt blir sporbarheten til informasjonen mer viktig. Dette blant annet for å kunne dokumentere hvilken informasjon en hadde tilgang til under en behandling. Det vil også være behov for vite hvor den originale informasjonen ligger og gjøre de endringer som behøves der.

6. Løsninger med felles fysisk datalagring

Det forsøkes her å gi en oversikt over hvordan et PACS system kan fungere mot en løsning som benytter seg av en felles datalagerløsning. Her presenteres det en løsning med utgangspunkt i at det finnes en integrert PACS/RIS løsning der det benyttes et felles bildelager med et eller flere andre helseforetak.



Figur 9: Eksempel på PACS/RIS system

Illustrasjonen over viser et eksempel på et PACS system. Løsningen er bygd opp slik at PACS og RIS informasjon ligger i egne databaser. PACS bilder som er relevante for journalen til pasienten kan også lagres i selve pasientjournalen.

Helsepersonell som jobber på røntgenavdelingen har direkte tilgang til PACS bilder gjennom ulike modaliteter som benytter seg av DICOM standarden for håndtering av PACS informasjon. Dette vil si at de ikke går via EPJ eller andre helseinformasjonssystemer. Røntgenpersonellet kan også ha tilgang til RIS informasjon gjennom de ulike DICOM-modalitetene. Dette krever i midlertidig at DICOM modalitetene har RIS grensesnitt.

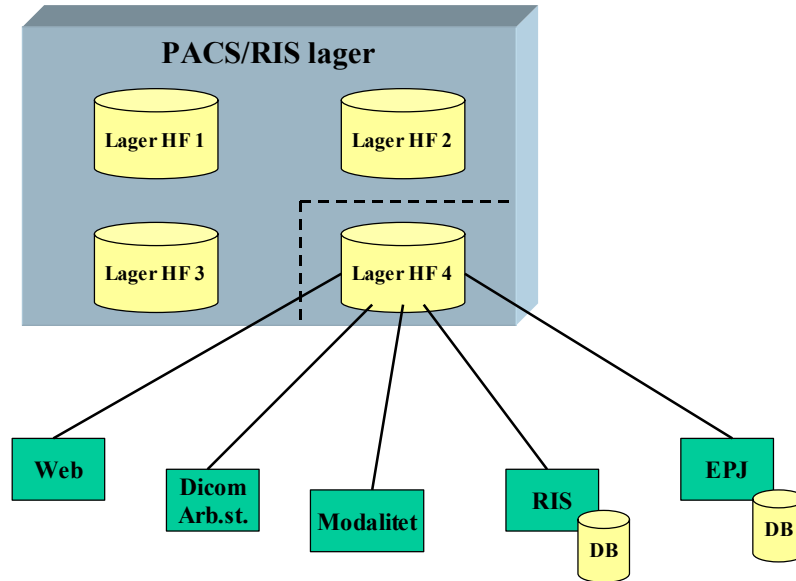
DICOM brokieren fungerer som en bro mellom PACS og RIS systemene og er ofte nødvendig fordi RIS (og eventuelt andre pasientinformasjonssystemer) systemer ikke forholder seg til DICOM-standard.

En DICOM broker er programvare utviklet spesielt med tanke på informasjonsutveksling mellom RIS, PACS og PACS-modaliteter for å støtte arbeidsflyten. Den knytter pasient- og undersøkelsesdata til PACS-bilder, muliggjør overføring av arbeidslister fra RIS til PACS-modaliteter, støtter visning av svarrapport ved granskning, trigger ”prefetching” (henter inn informasjon på forhånd), oppdaterer RIS med informasjon fra PACS-modaliteter etter en undersøkelse, og oppdaterer status mellom systemer.

Brukere utenfor røntgenavdelingen som skal ha tilgang til PACS/RIS informasjon kan gjøre dette via aksess gjennom et tradisjonelt leverandørgrensesnitt (levert for eksempel fra Sectra, DIPS, Agfa eller andre). Dette kan være tilgang både gjennom EPJ og tilgang til et eget RIS system. Gjennom en slik løsning får disse brukerne bare tilgang til PACS/RIS informasjon for den pasienten som brukeren har valgt i det aktuelle systemet. Det kan også tenkes at tilgang til EPJ og/eller RIS kan skje via et webgrensesnitt, noe som leverandører kan levere løsninger på i dag.

6.1. Kobling mot felles lager

Som nevnt tidligere sier Helseregisterloven at deling av pasientopplysninger mellom helseforetak ikke er tillatt. Bruk av felles datalager betyr at en må kunne skille mellom data tilhørende to helseforetak og at tilgang til data i andre helseforetak må kunne kontrolleres i hvert enkelt tilfelle.



Figur 10: Kobling mot felles lager

Som figuren over viser kan det være flere ulike metoder for aksess til PACS/RIS data i et sentralt lager:

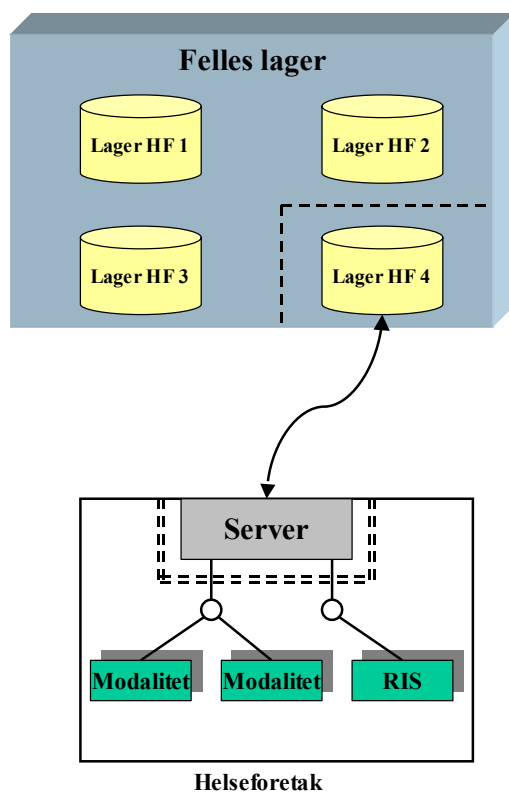
- ❑ **EPJ** - gjennom den elektroniske pasientjournalen som kan være koblet opp mot RIS (og også PACS) data
- ❑ **RIS** - gjennom RIS systemet kan en få tilgang til RIS og PACS data
- ❑ **Modaliteter** - gjennom ulike modaliteter kan en få direkte tilgang til PACS informasjon
- ❑ **DICOM arbeidsstasjoner** - gjennom ulike arbeidsstasjoner som jobber ved hjelp av DICOM standarden kan en få tilgang til PACS data
- ❑ **Web** - gjennom et webgrensesnitt kan en for eksempel få tilgang til EPJ som igjen kan være linket opp mot PACS/RIS informasjon

Det viktige er at ingen av de ulike metodene for aksess felles lager gjør at det kommer i strid med lovverket (spesielt Helseregisterloven). Tilgang som er knyttet mot en enkelte pasient (gjennom EPJ eller andre helseinformasjonssystemer) håndteres bra fordi tilgangen til PACS/RIS informasjon er da koblet mot den pasienten som er inne på i det aktuelle helseinformasjonssystemet. En har med en slik løsning ikke tilgang til annen informasjon enn det som hører til den aktuelle pasient. En unngår dermed eventuelle problemer i forhold til regelverket om at en har ”fri” tilgang til et felles lager mellom flere helseforetak.

Det er vanskeligere å håndtere tilgang gjennom DICOM systemer fordi en da ikke knyttet opp mot en spesiell pasient, men har i realiteten tilgang til all PACS/RIS informasjon (dette blir diskutert under).

6.2. Håndtering av DICOM kommunikasjon

DICOM standarden gir mulighet for å autentisere mellom DICOM applikasjoner (for eksempel portnummer, IP-adresse og DICOM_AE_TITLE, se i kapittel 3). Dette kan benyttes til å knytte PACS informasjon opp mot ulike modaliteter som benytter DICOM standarden. På denne måten kan tilgang til et felles datalager gjennom DICOM applikasjoner skille på tilgang fra ulike helseforetak.



Figur 11: Tilgang fra DICOM applikasjoner

Som vi ser av figuren er alle modaliteter (eller annet utstyr) som benytter DICOM applikasjoner knyttet til en server som håndterer DICOM kommunikasjon. Denne serveren kan sørge for at all informasjon som blir sendt (eller ”pushet”) inn til lageret får riktig ID (kan for eksempel være

DICOM_AE_TITLE), og at kun informasjon med riktig ID blir hentet inn fra lageret og til helseforetaket. Det kan også tenkes at hvert helseforetak har sin egen foretaksidentifikator ("foretaksID") som kan benyttes til å knytte informasjon til riktig helseforetak.

En annen løsning er det sentrale datalageret holder rede informasjonen til de ulike helseforetakene. Datalageret må da sørge for å lagre data under riktig "foretaksnode" og tilby informasjon i det logiske lageret som tilhører denne noden. Hva som brukes for å identifisere en foretaksnode er ikke så viktig så lenge det sentrale datalageret vet hvilken foretaksnode det kommuniserer med.

Dette kan løse noe av problemet med at klinikerne (røntgenavdelingen) som benytter DICOM applikasjoner i utgangspunktet har tilgang til all informasjon i et PACS lager og er dermed i strid med lovverket.

DICOM gir mulighet for at en kan benytte seg av TLC (Transport Layer Security) og ISCL (Integrated Secure Communication Layer) for sikker autentisering av to parter. Dette kan benyttes slik at en på en sikker måte vet hvilket helseforetak som ønsker å få tilsendt data i fra det felles bildelageret.

En slik løsning vil ikke kunne autentisere brukere, men kun kommunikasjonen mellom to ulike DICOM applikasjoner. Eventuell autentisering av brukere av DICOM applikasjonene må foregå på annet vis.

Bruk av ISCL (eller alternativt TLS/SSL) gjøre at tilgang på tvers av helseforetak via DICOM applikasjoner til et sentralt lager ikke er mulig uten videre. Dersom en velger å bruke DICOM attributtene for autentisering krever dette en server (DICOM broker) som håndterer denne funksjonaliteten.

7. Konkusjon og anbefalinger

Denne rapporten har hatt fokus på regionale datalagerløsninger for digital røntgen og sett på hvilke muligheter og farer dette kan gi med tanke på informasjonssikkerheten.

Både aktuelt lovverk og dagens teknologi muliggjør regionale datalagerløsninger for digital røntgen mellom helseforetak. Den største utfordringen er trolig hvordan slike løsninger skal utformes med tanke på utveksling og/eller tilgang til informasjon på tvers av helseforetak. Som nevnt tillates ikke fri deling av pasientopplysninger mellom helseforetak. Skal pasientinformasjon utveksles eller gis tilgang til må dette avtales for hvert aktuelle tilfelle. Dette for å sikre blant annet at informasjon bare blir gitt tilgang til/utlevert når det er hjemlet i forbindelse med behandling og at pasienten har gitt sitt samtykke.

Mekanismer og prosedyrer for utlevering/tilgang til informasjon bør på plass for å sikre lovmessig korrekt utlevering/tilgang til pasientinformasjon mellom helseforetak.

Regionale datalagerløsninger må skille mellom informasjon fra de ulike helseforetakene. Det finnes flere metoder dette kan gjøres på, men det viktige er at informasjon knyttes opp mot ett helseforetak. Det er også viktig at informasjon tilhørende et helseforetak ikke kan aksesseres av et annet helseforetak uten at det er gitt særskilt tillatelse til det.

En av de største truslene med regionale datalagerløsninger er avhengigheten en gjør seg av tilgang til en regional datalagerløsning. En slik datalagerløsning med tilhørende kommunikasjonslinjer bør utformes med redundante løsninger for å sikre seg tilnærmet 100% oppetid på et PACS-nettverk. Risikovurderinger kan (og bør) være grunnlag for de løsninger en velger med tanke på blant annet redundans for felles datalagerløsninger.

En annen stor trussel er det store antallet helsearbeidere som i teorien kan skaffe seg tilgang til pasientinformasjon. I forbindelse med dette er det ikke bare viktig med gode kontrollrutiner på tvers av helseforetak, men også innad i hvert enkelt helseforetak.

Referanseliste

- DICOM DICOM webside: <http://medical.nema.org/>
- SHDir ”Igangsetting av behandling av opplysninger i helseforetak”, Sosial- og
Helsedirektoratet - 15. september 2002
- SHDir ”Ansvar for personvern og informasjonssikkerhet i helseforetak”, Sosial- og
Helsedirektoratet - 15. september 2002
- HIG Høyskolen i Gjøvik - videreutdanning for radiografer:
<http://www.hig.no/at/radiograf>

Vedlegg B: Referat fra workshop

KITH arrangerte den 19. november 2002 en workshop hvor hovedtema var informasjonssikkerhet og PACS løsninger. Det var nærmere 30 personer tilstede på workshopen, inkludert personer fra KITH. Workshopen ble gjennomført med fire hovedbolker med et fokusområde under hver bolke.

Roald Bergstrøm fra KITH åpnet workshopen ved å si litt om bakgrunnen for Paraplyprosjektet, som var hovedårsaken til at workshopen ble holdt. Det ble også gitt en kort innledning om digital røntgen i Norge og hva som er status for utviklingen av PACS i Norge.

Etter dette gav Tor Olav Grøtan fra KITH en introduksjon til innhold og hensikten med workshopen. Grøtan begynte med at på den ene siden har en dagens teknologi og hvilke muligheter denne gir med tanke på ulike PACS løsninger. På den andre siden har en lovverk som setter begrensninger for hvordan teknologien kan brukes. Dette gapet mellom teknologi og lovverk må på en eller annen måte tettes og med denne workshopen vil en trekke frem noen punkter som kan være med på tette gapet.

Fokusområde 1: Helselovverk og forskrifter

Bjarte Aksnes holdt en kort presentasjon av de viktigste punktene i helselovgivningen som er relevant i forhold til PACS løsninger. Dette ble gjort fordi en trodde at mange innen helsevesenet ikke var helt kjent med hvilke lover og forskrifter som er relevante for PACS løsninger. Det er også et nytt lovverk som gjør at kanskje ikke alle deler av lovverket er kjent eller forstått.

I tillegg ville en at workshopen ikke skulle bli en diskusjon om lovverket er bra eller dårlig, men heller at workshopen skulle fokusere på hvilke problemstillinger som lovverket gir i forhold til aktuelle løsninger.

Hovedpunkter av presentasjon fra Bjarte Aksnes:

- ❑ Helseregisterloven
 - Databehandlingsansvarlig
 - Behandlingsansvarlig
 - Regionale og lokale helseregister
 - Sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet
- ❑ Personopplysningsloven - POL
 - Personopplysningsforskriften (kap. 2 om informasjonssikkerhet)
- ❑ Helsepersonelloven
 - Utlevering av informasjon til samarbeidende personell
- ❑ Pasientrettighetsloven
- ❑ Helseforetaksloven

Konklusjoner:

- ❑ EPJ skal være knyttet til ett og bare ett helseforetak
 - Gjelder også PACS bilder
- ❑ Bør være mulig å benytte en driftsleverandør
- ❑ Flere helseforetak bør kunne benytte samme databehandler, men dette krever risikovurderinger og dokumentasjon

Diskusjon

Etter presentasjonen ble det holdt en åpen diskusjonsrunde hvor alle deltakerne hadde sjansen til å komme med synspunkter, spørsmål eller andre kommentarer.

Noen viktige punktene var:

- ❑ Hvilket foretak skal ha eierskap til en journal når pasienten forflytter seg?

- Skal opplysningene følge pasienten?
- Tilgang på tvers av helseforetak
 - Fysisk handling og vurdering hver gang info skal overføres?
- Lovverk (innen teleradiologi) som sikrer kvaliteten på informasjon som sendes
 - Behandlingsansvarlig må være sikker på at den får info med god kvalitet
- Spørsmål om hvorfor er det så stor skille i lovverket mellom behandling innen og mellom ulike HF (et HF kan jo bestå av flere sykehus), ofte samarbeider jo flere HF i en behandlingssituasjon for å få utført ulike tjenester?

Det var tydelig at den nye helselovgivningen verken var fullstendig kjent eller forstått ute i helsesektoren, og det var meninger om at det nye lovverket ikke er tilpasset den strukturen helse Norge har fått med sine fem regioner og inndeling i helseforetak. Det ble også påpekt at Datatilsynet har en informasjonsrolle i henhold til å gjøre lovverket kjent ute i sektoren som de kunne ha utøvd på en bedre måte.

Konklusjon

Etter den ”åpne” diskusjonsrunden ble deltakerne delt inn i grupper hvor de skulle komme frem til de tre største utfordringene i regelverket i forhold til aktuelle PACS løsninger. Dette ble presentert i plenum hvor en underveis prøvde å gruppere de ulike utfordringene.

Nedenfor er det listet opp hvilke utfordringer som deltakerne mente var de vanskeligste å oppfylle:

- Ikke lov å ha felles logisk Databaser mellom HF (med felles tilgang)
- Autentisering av oppslag i journal (logging av oppslag)
- Tilgang til all relevant pasienthistorikk (nasjonalt register)
- Beslutning bak utlevering av info (helseregisterloven)

- ❑ Logging og sporbarhet for tilgang til felles lager mellom HF
- ❑ God tilgangskontroll
 - ikke mer tilgang enn nødvendig
- ❑ Personvern

- ❑ Utfordring å gjøre data tilgjengelig på en lovlig måte (for eksempel fysisk handlig ved utlevering)
- ❑ Konfidensialitet til dataene
- ❑ Integriteten til dataene, flere skriver på journalen

- ❑ Autorisasjons og tilgangskontroll
- ❑ Felles drift av løsninger, sikre tilgjengeligheten til dataene
- ❑ Beslutningstaking for tilgang til data (aktiv handling)

- ❑ Lik tilgangsstrategi for ulike systemer og mellom ulike virksomheter
- ❑ Beslutning om tilgang til data
- ❑ Praktisk håndtering av samtykke

- ❑ Hvem har eierskap til pasientopplysningene (sannsynligvis pasienten selv)?
- ❑ Spørsmål om samtykke fra pasienten
- ❑ Tilgjengelighet av data der hvor behandlingen skal skje

- ❑ Relasjonen mellom pasienten som forflytter seg og et og bare ett HF som skal ha eierskap til opplysningene
- ❑ Godkjenning av tilgang til informasjon - finne praktiske løsninger/ordninger for dette
- ❑ Sporbarhet og det å kunne oppdage uønskede hendelser

Etter hvert så en at en kunne gruppere de ulike argumentene som gikk på mye av de samme tingene. De viktigste bestemmelsene (i betydningen størst utfordring i å oppfylle) i regelverket syntes å være:

1. Løsninger med felles databaser (eller datalager) mellom HF
2. Håndtering av samtykke og tilgang på tvers av HF
3. Logging og sporbarhet
4. Autentisering

Fokusområde 2: Akseptkriterier

Utviklingen av akseptkriterier er et viktig del av det handlingsrommet et helseforetak har i forhold til regelverket som forvaltes av Datatilsynet. Dette tar utgangspunkt i at det er det ulike helseforetakene som selv må sørge for at de har tilstrekkelig informasjonssikkerhet. Dette vil si at helseforetakene selv skal avgjøre hva som er tilfredsstillende informasjonssikkerhet og begrunne hvorfor de mener at de har god nok informasjonssikkerhet (som oftest gjennom risikovurderinger).

Tor Olav Grøtan holdt en kort presentasjon hvor han tok for seg akseptkriterier og hvilke muligheter som ligger ved å bruke disse på en fornuftig måte.

Hovedpunkter av presentasjon fra Tor Olav Grøtan:

- ❑ Sikkerhetsbehov knyttet til:

- Tap av liv og helse
- Økonomi (i betydningen ”individets” økonomi)
 - En kan ikke argumentere for at å senke nivået for personvernet gjør at en sparer penger
- Personvern
- Akseptkriterier
 - Informasjonssikkerheten (konfidensialitet, integritet og tilgjengelighet) som operasjonalisering av sikkerhetsbehovene
- Risikovurdering
 - Informasjonssikkerheten
- Ansvarlig er den databehandlingsansvarlige
 - En ledelsesbeslutning
 - Skal inngå i sikkerhetsmål/prioritering
- TV-506, kapittel 2
 - Konfidensialitet teller mer enn tilgang (eksempel)

Diskusjon

Diskusjonsrunden fokuserte på følgende:

- Diskusjonen rundt PACS er egentlig en del av diskusjonen rundt journal generelt
- En må få helhetlige løsninger for ulike systemer

Det virket som om muligheten til å bruke akseptkriterier for å forsvare eller begrunne det valgte sikkerhetsnivå var delvis ny og ukjent for de fleste. Selv om akseptkriterier gir et visst handlingsrom var det også enighet om at akseptkriterier ikke kan brukes som en generell ”trylleformell” for å legitimere det sikkerhetsnivået som er valgt.

Konklusjon

- ❑ Fornuftig tilnærming dersom den brukes riktig (i henhold til intensjonen)
- ❑ Tilgjengelighet - bør begrunnes
 - For hvem
 - Hva
- ❑ Komme i gang med å utarbeide fornuftige argumenter
 - Samordning mellom HF (og kanskje også mellom RHF) - hvert enkelt HF kan ikke utarbeide sine "egne" kriterier uavhengig av de andre HF'ene
- ❑ Det koker ned til hvilke teknologiske løsninger har en for hånden i dag!!
 - En må bruke de teknologiske løsningene som finnes på en fornuftig måte i forhold til behov og regelverk som finnes i dag
 - Hva er mulig å få til i dag?
- ❑ Har flere behandlingsmuligheter enn det økonomien tillater i dag
 - Utnytte ressursene på en fornuftig måte
- ❑ Internasjonale lover
- ❑ Integritet og kvalitet

Fokusområde 3: PACS løsninger

Her gav Magnus Alsaker en kort presentasjon av to ulike modeller for PACS løsninger, en med en felles systemløsning med et felles bildelager innen en helseregion, mens den andre løsningen var at hvert HF hadde sin PACS løsning med tilhørende bildelager. Det ble kort tatt opp fordeler og ulemper med begge løsningene. Bakgrunnen for dette var å vise spennet i de løsninger som finnes i dag og fordeler og ulemper med de ulike løsningene.

Diskusjon

- ❑ Felles løsninger er et grunnlag for å kunne samordne og samhandle mellom virksomheter
- ❑ Lokale PACS løsninger m/lager er ikke noe å satse på!
- ❑ Til færre enheter og systemer involvert til enklere er det
- ❑ Tilgangsstyring gjennom EPJ
 - Midt-Norge bruker denne løsningen
- ❑ Fokus på standardisering på tvers av RHF - spesielt for region Sør og Øst som har mange transaksjoner mot HF utenfor sin egen region
- ❑ Trenger mer samordning og standardisering!

Diskusjonen gikk egentlig på at en trenger standardisering av metoder slik at utveksling av informasjon kan skje mellom to vilkårlige HF i Norge. Det er ikke nok at en velger samme løsning innenfor en region, dette løser ikke kommunikasjon mot en annen region med en annen PACS løsning.

Diskusjonen gikk raskt over mot temaet som skulle være i bolk fire, nemlig at en trenger et ”standardisert” rammeverk skal en få til samhandling mellom PACS systemer på tvers av systemer og helseforetak.

Konklusjon

Det ble ingen klare konklusjoner om hvilken løsning som er best, men flere mente at en strategi med felles systemløsning mellom flere HF er det mest fornuftige med tanke på å kunne få til samordning og utveksling av informasjon.

Det ble også tatt frem at felles løsninger er det som troligst gir den billigste og mest effektive løsningen.

Fokusområde 4: Rammeverk

I den siste bolken ble det satt fokus på rammeverk for hvordan en håndterer PACS (og RIS) informasjon slik at uveksling mellom ulike PACS systemer går enklere. Bakgrunnen for å se på rammeverk er at det finnes flere ulike PACS systemer i Norge i dag som fungerer på ulike måter. Å kommunisere ren PACS informasjon (bilder) går i de fleste tilfeller greit, men det er problemer med hvordan tilhørende RIS informasjon håndteres. Det finnes i dag ikke noen felles standard eller ”RIS-melding” som leverandørene kan benytte for å sende RIS informasjon.

Hovedpunkter av presentasjon fra Olaf Trygve Berglinh:

- Utviklingen har vært teknologidrevet
 - Må sette fokus på brukerbehov og organisasjon
 - Deretter kan en se på teknologi

Diskusjon

Det ble en god diskusjonsrunde som viste at det ikke er et enkelt spørsmål å skulle utvikle et rammeverk for PACS, blant annet fordi det er en komplekse arbeidsprosesser og kompleks arbeidsflyt som foregår i forbindelse med bruk av PACS løsninger.

Her er noen av tingene som ble tatt opp under diskusjonen:

- PACS data går greit, men RIS informasjon må sendes manuelt (kanskje pseudonymisert)
- Logikken bør være tilstede uansett om det er snakk om et felles (Midt-Norge) eller flere systemer (Sør)
- Database er logisk oppdelt, men på søk får du tilgang til hele databasen. I praktisk bruk har bare et HF tilgang til sine data, men juridisk holder det ikke (fordi et søk gir tilgang til hele databasen).
- Brukerne (kundene) må sette krav til de systemene som skal innføres (for eksempel til sikkerhet og lovverk)

- I en oppstartsfase vil det være naturlig at systemene ikke er fullstendige og kanskje ikke har alle sikkerhetsmekanismer implementert
- ”Utprøving” av lovverk vil være naturlig
- systemet må være ”åpent” (og kanskje ulovlig) i starten slik at brukerne liker det (skaper tillit hos brukerne)
 - Direktoratet påpekte at en slik ”åpen” løsning er en helt uakseptabel og feil strategi
- Lovverket bør tenkes på fra første stund - ikke etter at et system er satt i drift
- Regelverk og funksjonalitet bør ”møtes” på midten i en felles ”løsning”
- Mangler definerte arbeidstransaksjoner
- Trenger å spikre fast noen tekniske ”knagger” slik at ulike system kan fungere mot hverandre
 - Datamodellen for PACS kan være et utgangspunkt (utviklet av KITH for noen år siden)
- Sende all data (PACS bilde, henvisning og RIS) i en pakke, for eksempel i en EDI melding eller i en e-post (forsøk gjort mellom NST og Haukeland)
 - Slipper unna DICOM standarden
- Manglende funksjonalitet i dagens PACS systemer for å håndtere PACS/RIS mottatt fra et annet PACS system
 - PACS/RIS systemene støtter ikke historikk (følger ikke IHE standard)
 - Støtter interne arbeidsprosesser
 - Trenger støtte for eksterne arbeidsprosesser
 - Mangler sporbarheten for PACS dataene
- Trenger å vite hvor originalen ligger og noterer de endringer en gjør
 - Det er ikke alltid nok med en kopi

- En må kunne dokumentere hvilken informasjon en hadde for eksempel under en behandling

Konklusjon

Det ble ikke noen entydig konklusjon, men noen sentrale elementer var:

- Rutiner som fungerer i stor skala
- Standardisert utveksling til mottaker/avsender også utenfor en felles løsning