Risikovurdering ved lovpålagte tilsyn med informasjonssikkerhet i helseforetak

Ali Mohammed Barzinje

Masteroppgave prosjektbeskrivelse
Master i informasjonssikkerhet
30 ECTS
Avdeling for informatikk og medieteknikk
Høgskolen i Gjøvik, 2010

Avdeling for
informatikk og medieteknikk
Høgskolen i Gjøvik
Postboks 191
2802 Gjøvik

Department of Computer Science
and Media Technology
Gjøvik University College
Box 191
N-2802 Gjøvik
Norway

Risikovurdering ved lovpålagte tilsyn med informasjonssikkerhet i helseforetak

Ali Mohammed Barzinje

Forord

Denne oppgaven markerer slutten på en flott studietid ved Høgskolen i Gjøvik. Oppgaven er utført vårsemesteret 2010.

Jeg vil takke min ektefelle som har støttet og oppmuntret meg, og mine tre barn som har vært tålmodige i løpet av studietiden.

Jeg vil rette en stor takk til min veileder Einar Snekkenes for god veiledning og inspirasjon gjennom oppgaven. Du har vært til god hjelp!

Jeg vil også takke assisterende helsedirektør Geir Sverre Braut for alt han har tilrettelagt for meg.

En ekstra takk går til alle intervjuobjektene og biblioteket i Helsetilsynet for all hjelp og tilgang til kilder, samt til min nærmeste leder Finn Pedersen som var snill og hjalp meg med korrekturlesing.

Dere har betydd mye!

Oslo, juni 2010
Ali Mohammed Barzinje

Sammendrag

Både Helsetilsynet og Datatilsynet har ansvar for tilsyn med informasjonssikkerheten i helsetjenesten. Denne oppgaven inneholder en analyse av Helsetilsynets arbeid med dette emnet og kommer med forslag til forbedringer av Helsetilsynets virksomhet.

Studien tar utgangspunkt i hvilke forventninger man i dag bør kunne stille til informasjonssikkerhet i større virksomheter og hvilke utfordringer det statlige tilsynet med informasjonssikkerheten stilles ovenfor. Det legges her vekt på resultater fra forsknings- og utviklingsarbeid knyttet til informasjonssikkerhet og risikoanalyser.

Videre er det gjennomført en studie av den praksis som Helsetilsynet i dag har når det gjelder tilsyn med informasjonssikkerheten i helsetjenesten. Det er lagt spesiell vekt på en vurdering av opplæring av tilsynsførere og gjennomføring av systemrevisjoner. Data er innsamlet gjennom intervjuer med nøkkelpersoner innenfor og utenfor Helsetilsynets organisasjon, spørreskjema til Helsetilsynets enheter i fylkene og dokumentanalyse av tilsynsrapporter.

Studien konkluderer med at Helsetilsynet har systematiske opplegg både for intern opplæring av tilsynsførere og gjennomføring av tilsyn. Men ingen av disse har et særlig fokus på informasjonssikkerhet. Dette avspeiles også i det faktum at informasjonssikkerhet ikke har noen tydelig plass i tilsynsrapportene som skrives.

I forlengelsen av studien tilrås det følgende tiltak:

1. Det etableres systematisk opplæring av tilsynsførere i informasjonssikkerhet.
2. Ved systemrevisjoner bør det benyttes en standardisert sjekkliste om informasjonssikkerhet.
3. Samarbeidet med Datatilsynet bør utvikles videre.

Abstract

Both Norwegian Board of Health and the Norwegian Data Inspectorate are responsible for supervising the security of information in health care. This paper contains an analysis of the Norwegian Board of Health work on this subject and coming with suggestions for improvements to the Norwegian Board of Health business.

The study is based on the expectations we today should be able to stand for information security in large enterprises and the challenges faced by the state audit of information security is set above. Emphasis here focuses on results from research and development related to information security and risk analysis.

Furthermore, it conducted a study of the practice as Board of Health today regarding an audit of information security in health care. It placed special emphasis on an assessment of the training of supervisory drivers and execution of system audits. Data were collected through interviews with key people within and outside the Norwegian Board of Health organization, questionnaire to Norwegian Board of Health units in the counties and document analysis of audit reports.

The study concludes that the Board of Health have systematic arrangements for internal training of supervisory drivers and conducting inspections. But none of these has a particular focus on information security. This is also reflected in the fact that information security has no obvious place in the audit reports as written.

As an extension of the study recommends the following measures:

1. It established a systematic training of supervisory drivers in information security.
2. The system audits should be used a standardized checklist of information security.
3. Cooperation with the Norwegian Data Inspectorate should be further developed

Contents

List of Figures

List of Tables

1 Introduksjon

Overgang til IT-løsninger for papirbaserte systemer innebærer en betydelig effektivisering i den daglige bruken av systemene, men også et økt nivå for en rekke trusler og sårbarheter. Dette gjør det vesentlig å komme fram til metoder som reduserer risikoen for tap eller utilgjengelighet av kritiske informasjon.

Bruken av elektronisk pasientjournal (EPJ) og andre kritiske IT-løsninger er økende innenfor helsevesenet. Innføring av EPJ i helsetjenesten representerer et fremskritt for alle parter. Det gir behandlerne raskere tilgang til pasientenes sykehistorie og tidligere behandling, og det letter pasientenes hverdag ved at de slipper å gjenta informasjon de allerede har gitt. Men den økte tilgjengeligheten skaper også utfordringer. Dette gjelder spesielt taushetsplikt og personvern som nå er under større press enn før.

Lovgivningen stiller krav om at 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. Journalforskriften inneholder bestemmelser om at virksomhet som yter helsehjelp må opprette pasientjournalsystem. Journalsystemet må organiseres slik at det både sikrer nødvendig tilgang til journalopplysningene og utlevering av journal, og verner opplysningene mot innsyn fra uvedkommende. Utveksling av taushetsbelagt informasjon mellom helsepersonell er basert på samtykke fra pasientene og kan kun skje når det er nødvendig for behandling og oppfølging av pasienten, eller der hvor det foreligger annet rettslig grunnlag for å gi slik informasjon. Tilleggene A.1 og A.2.

Statens helsetilsynet[1] og Datatilsynet gjennomførte i fellesskap i mai 2006 tilsyn med hvordan Helse Bergen HF Haukeland universitetssykehus ivaretok taushetsplikten og tilgjengeligheten ved bruk av pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS. Tilsynet omfattet både innhenting og utlevering av pasientinformasjon fra elektronisk pasientjournal og tilgangsstyring i forhold til elektronisk pasientjournal og det pasientadministrative systemet PIMS [18].
I juni 2006 gjennomførte Helsetilsynet og Datatilsynet et lignende tilsyn ved Akershus universitetssykehus HF. Temaet ved dette tilsynet var sikring av taushetsplikten og tilgjengeligheten til opplysninger ved bruk av det elektroniske pasientjournalsystemet DIPS [18].
Tilsynene ble gjennomført som systemrevisjoner og var av to dagers varighet. Ved tilsynene ble tiltak og praksis ved helseforetakene vurdert opp mot aktuelle krav i helselovgivningen, helseregisterloven og personopplysningsloven.

[1] Statens helsetilsyn kalles også Helsetilsynet

1.1 Tema oppgaven dekker

Valg av metode for en risiko- og sårbarhetsanalyse (ROS-analyse) er ofte basert på flere forskjellige faktorer som kan bli variert fra en sektor til annen. Noen slike faktorer kan være: ulike sikkerhetsaspekter, problemstilling, ressurser, tid eller juridiske begrensninger osv. For Helsetilsynet som et forvaltningsorgan med ansvar for tilsyn med helse, sosial og barnevern, hvor helseregisterloven og personopplysningsloven har en ledende funksjon, er systemrevisjon en sentral oppgave.
Med dagens utvikling av IT- og annen teknologi, er det kontinuerlige forandringer i IT-systemene i helsesektorene. Dette medfører vanskeligheter for tilsynsførere når de er på tilsynsbesøk. For eks en effektiv informasjonsutveksling og samarbeid mellom virksomheter reiser behov for juridiske avklaringer, gjennomgang av prinsipper for tilgangsstyring og autentisering samt integrasjon mellom EPJ og mange ulike fagsystemer internt i helseforetak.

Masteroppgaven tar utgangspunkt i spørreundersøkelser og intervjuer med sentrale personer i dette feltet, lager en oversikt over de mest vesentlige og/eller sårbare områder som Helsetilsynets tilsynsførere (som ikke er IT-eksperter) bør være oppmerksomme på når de er på tilsynsbesøk.

1.2 Nøkkelord

Risiko- og sårbarhetsanalyse, risikometode, informasjonssikkerhet, Helsetilsynet, tilsynsfører, sjekkliste, helseforetak, kompetanseheving og personvern.

1.3 Problembeskrivelse

Både Datatilsynet og Helsetilsynet har et tilsynsansvar i forhold til helseregisterloven. Både helseregisterloven og personopplysningsloven forutsetter at de ansvarlige har bygd sine sikkerhetssystemer på forsvarlige risikoanalyser.
Helseregisterloven stiller krav om at informasjonssystemet skal vurderes med hensyn til risiko med bakgrunn i fastsatte kriterier for akseptabel risiko. Det å gjennomføre en risikoanalyse er et verktøy for å bedre informasjonssikkerheten. En risikoanalyse vil peke på hvilken risiko som foreligger og hvilke tiltak som er nødvendig for å oppnå en akseptabel risiko. Den kan gi forslag til hvilke tiltak som bør prioriteres, slik at ledelsen får et bedre beslutningsunderlag for det videre arbeidet. En god ledelsesforankring av sikkerhetsarbeidet innebærer at det foretas grundige risikovurderinger ved innføringen av nye system, eller ved endring av f. eks systemene for elektronisk pasientjournal.

Både Statens helsetilsyn [2] og Datatilsynet [3] har ved gjentatte anledninger uttrykt uro for manglende sikring av skjermingsverdige opplysninger i IT-systemene i helsetjenesten. For Helsetilsynet som tilsynsmyndighet innebærer tilsyn med helsetjenestens bruk av IT-systemer ikke bare juridiske og helsefaglige utfordringer. Dette er tross alt forhold som de fleste av tilsynsførere er vant med å vurdere, både ved planlegging og gjennomføring av tilsyn. Derimot er tilsynsførere i liten grad trent i å vurdere risiko knyttet til selve

[2] http://www.helsetilsynet.no
[3] http://www.datatilsynet.no

IT-systemene.
De tilsynene som er foretatt har vist at helseforetakene ikke gjør grundige nok risikovurderinger ved innføring av, eller ved endring i systemene for elektronisk pasientjournal. Denne mangelen gjør at helseforetakene ikke får oversikt over egne systemers sårbarhet, og hvor stor risiko det er for ulike typer svikt. De går derved glipp av muligheten for å iverksette tilstrekkelige og målrettede forebyggende tiltak. Manglende risiko- og sårbarhetsvurderinger er en gjenganger innen alle deler av helsetjenesten.
Erfaringer viser at ledelsen i virksomheter som yter helsetjenester har et noe perifert forhold både til sikkerhetsstyringen og risikoanalysene som er nødvendige. Når i tillegg tilsynsførere ikke har så dyp IT-kunnskap, er det grunn til bekymring for at uforsvarlig risikohåndtering ofte ikke avsløres.

1.4 Forskningsspørsmålene

1. Hvilken kompetanse i informasjonssikkerhet har Helsetilsynet som grunnlag for å utføre tilsyn?
2. Hvilket behov har Helsetilsynet, særlig tilsynsførere, for kompetanseheving innen informasjonssikkerhet?
3. Hva er hensiktsmessig risikoanalysemetode ved tilsyn med informasjonssikkerhet i helseforetak?

1.5 Målet med oppgaven

Oppgaven har som mål å utarbeide en "sjekkliste" eller oversikt over de mest vesentlige og/eller sårbare områder som Helsetilsynets tilsynsførere bør være oppmerksomme på når de stiller spørsmål om hvilken styring ledelsen i kommuner eller helseforetak (sykehus) har med sikkerhet, sårbarhet og risiko i egne systemer.
I slutten av oppgaven skal det utarbeides et opplegg som Helsetilsynet skal kunne bruke om de skulle utvikle systemrevisjon på dette området. Opplegget skal inneholde hvilken type risikoanalysemetode det lønner seg for Helsetilsynet å velge i sitt tilsynsarbeid.

1.6 Begrensninger og valg i oppgaven

Oppgaven er avgrenset til å dekke lov om helseregistre og behandling av helseopplysninger (Helseregisterloven) [4] §§13, 13a, 14, 15, 16, 17, 18 og forskrift om behandling av personopplysninger (personopplysningsforskriften) [5] hele kapittel 2 og §3-1 Tilleggene A.1 og A.2.
Denne begrensningen er gjort pga. at ovennevnte lov og forskrift er i kjernefeltet for Helsetilsynets arbeid.

[4] http://www.lovdata.no/all/hl-20010518-024.html
[5] http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html

1.7 Oppgavens oppbygning

Oppgaven er delt inn i følgende kapitler:

Kapittel 1: Her er problembeskrivelse definert, oppgavens mål og bakgrunn kort gjort rede for, forskningsspørsmålene er definert, og noen begrensninger og valg i oppgaven er beskrevet.

Kapittel 2: Her er en introduksjon til risikostyring. Her er redegjort for IT-sikkerhetsrisikovurdering, definisjoner, klassifiseringsskjema for risikoanalysemetodikker, gitt eksempler av noen standarder og konkrete produkter av risikovurdering- og risikostyring

Kapittel 3: Her er Litteraturoversikt bl.a. lover og forskrifter, Tilsyn med informasjonssikkerhet i helsetjenesten, veiledninger og tidligere relevante arbeid beskrevet. Til slutt er det gitt et eksempel på bruk av risikoanalysemetodikk i en tilsynsvirksomhet.

Kapittel 4: Her er det gjort rede for alternative metoder for datainnsamling strukturert i forhold til forskningsspørsmålene. Først definerer jeg alternative metoder med rammer og begrensninger for hver metode, deretter velges de mest hensiktsmessige metodene.

Kapittel 5: Her er datainnsamlingen beskrevet, måtene dataene ble samlet inn på og hvordan jeg skrev rådataene. Jeg har sortert dem i forhold til måtene de ble innsamlet på.

Kapittel 6: Her er det dataanalyse og diskusjon. I begynnelsen er hvert forskningsspørsmål analysert for seg. Deretter er de viktigste funnene lagt inn, så behov for tiltak. Jeg har skrevet om de økonomiske og administrative konsekvenser av det jeg har funnet. Videre foreslår jeg noe tiltak for håndtering av identifiserte utfordringer. Til slutt tar jeg en enkel diskusjon.

Kapittel 7: Her presenteres tekstlig en utviklet sjekkliste som er et resultat av denne oppgaven. Sjekklisten er delt inn i flere områder og underområder. Disse områdene er beskrevet, viktigheten begrunnet og hvordan disse områdene kan sjekkes er forklart. Sjekklisten i form av spørsmål, er lagt som vedlegg.

Kapittel 8: Her er konklusjon, som er en kort oppsummering av min oppgave.

2 Introduksjon til risikostyring

I dette kapitlet vil jeg først forklare etablering av risikostyring og viktigheten av den. Deretter definerer jeg en del termer og begreper som brukes i dette området. Jeg skal presenter en modell for klassifisering av risikoanalysemetoder, samt beskrive noen metoder og standarder for risikovurdering og risikostyring innen informasjonsteknologi.

2.1 IT-sikkerhetsrisikostyring er en del av virksomhetsledelse

Det å etablere og vedlikeholde IT-sikkerheten i bedriften er en hel prosess:

- Oppnå en relevant, rolig og metodisk diagnostikk av informasjonssystemet, veiing av trusler og eiendeler for å identifisere de største risikoene på kjernevirksomheten.
- Gjennomføre nødvendig og tilstrekkelig beskyttende kontroller, i balanse med sine operative og økonomiske kostnader:
  - Bruke lov og forskrift for å redusere eksterne risikoer.
  - Sette opp en IT-sikkerhetsorganisasjon, i samsvar til bedriften.
  - Øke sikkerhetsbevissthet hos personalet gjennom kontinuerlig opplæring.
  - Implementere teknisk sikkerhetskontroller.
- Kontrollere nøyaktigheten av IT-sikkerhet gjennom revisjoner.
- Vedlikeholde informasjonssystemet og holde sikkerheten på tilstrekkelig sikkerhetsnivå.

For å etablere risikostyring, må man ha en støttende metode. Risikostyringsmetoder varierer fra enkle steg for steg tilnærminger til komplekse metoder som krever støtte av automatiserte verktøy.

Det første skrittet mot å håndtere IT-sikkerhetsrisikostyring er å vurdere viktigheten av organisasjonens informasjonseiendeler. Denne vurderingen gjøres i to steg [25], [37]:

1. Definere betydningen av forretningsprosesser for organisasjonen og miljø henholdsvis. Denne betydningen kan variere fra "høy" til "lav":
   - Prosesser med høy viktighet er de mest verdifulle eiendeler for organisasjonen (f.eks produksjonsprosessene). Avbrudd eller opphopning av slike prosesser fører til uakseptabel skade.
   - Prosesser med middels betydning representerer en moderat verdi for organisasjon. Avbrudd eller opphopning av slike prosesser fører til betydelig skade.
   - Prosesser med lav vekt er av mindre verdi for organisasjonen. Forstyrrelsen eller opphopning av slike prosesser fører bare til mindre skade.
2. Definere hvor avhengig forretningsprosesser er av informasjonssystemer:
   - Høy avhengighet: Forstyrrelse av informasjonssystemer resulterer i alvorlige hindrer eller opphopning av avhengige prosesser.
   - Middels avhengighet: Forstyrrelse av informasjonssystem fører til betydelig, men

ikke alvorlige hindre i avhengige prosesser.
- Lav avhengighet: Forstyrrelse av informasjonssystem fører til kun små hindrer i avhengige prosessen.

I tabellen nedenfor (Figur 1), illustrerer kritikalitet som kombinasjonen av IT-systemers avhengighet og viktigheten av en forretningsprosess. Dette kritikalitetet er den viktigste indikatoren for en IT- risikostyring, og vil vise IT-systemets bidrag til den samlede virksomheten i organisasjonen.

For eksempel, en svært viktig prosess (f. eks bestillingsprosessen) som er svært avhengig av et IT-system (f. eks et elektronisk skjema på webportalen til selskapet) må betraktes som meget kritisk for risikostyring (og som sådan må være gjenstand for risikostyring).

Viktigheten av prosess for virksomheten	Prosessens avhengighet av IT-systemet		
	Lav avhengighet	Middels avhengighet	Høy avhengighet
Lav viktighet	Ikke kritisk	Ikke kritisk	Lav kritisk
Middels viktighet	Ikke kritisk	Lav kritisk	Middels kritisk
Høy viktighet	Lav kritisk	Middels kritisk	Høy kritisk

Figure 1: Kritikalitet i risikostyring av et IT-system i forhold til dets bidrag til virksomheten.

(Tabellen hentet fra ENISAs report side 8) [25].

Den type IT-sikkerhetsrisikostyringsmetode man trenger, avhenger av kritikalitet som illustrert i cellene i tabellen ovenfor:

Hvis organisasjon har IT-systemer med middels eller høy kritikalitet, vil en risikostyring basert på en formell metode være hensiktsmessig. Hvis organisasjonen har IT-systemer med lav kritikalitet, vil en risikostyring basert på en enkel tilnærming være hensiktsmessig. En slik tilnærming kan være basert på allment akseptert beste praksis. Hvis det er nødvendig, kan i tillegg en enkel metode for risikostyring og risikoanalyse brukes.

Hvis organisasjonen har IT-systemer som ikke er kritiske, vil i så fall risikostyring bestå utelukkende i å implementere grunnleggende sikkerhetskontroller (f. eks grunnleggende beskyttelse). Utvalg av sikkerhetskontroller bør være basert på beste praksis.

2.2 Definisjoner

IT-sikkerhetsrisikostyring er en integrert del av et selskaps ledelsesprosess som handler om identifisering, behandling, kommunikasjon og aksept av IT-sikkerhetsrisikoer. Det innebærer valg og gjennomføring av tiltak som rettferdiggjøres ved at de identifiserer IT-sikkerhetsrisikoer og muliggjør reduksjon av risikoen til akseptabelt nivå. Det inneholder også kontinuerlig overvåking av risikoer og risikokommunikasjon.

En IT-sikkerhetsrisiko består av eiendel, trussel og sårbarhet: hvis et av disse elementene er irrelevante, så er det ingen risiko. Samling av alle single IT-sikkerhetsrisikoer

resulterer i total IT-risiko. Et sentralt skritt i risikostyringsprosessen er risikovurdering, og dette innebærer å vurdere hver IT-risiko så vel som den totale IT-risiko, og deretter gi dem prioriteringer.

I denne delen angir jeg definisjoner [1] basert på standarden ISO/IEC IS 13335-1, og vil gi eksempler på komponentene som inngår i IT-sikkerhetsrisikoer, nemlig: eiendel, trussel og sårbarhet:

Eiendel: alt som har verdi for organisasjonen. En eiendel er en konkret eller immateriell del av et informasjonssystem. Eiendeler kan være maskinvare, programvare, data, bygg, infrastruktur, men også produkter, kunnskapsressurser, kunderelasjoner eller omdømme. For å anslå risikoen, må først sikkerhetsbehovene til hver eiendel evalueres ved å ta hensyn til verdien. Eiendeler kan f. eks være kostnader til rekonstruksjon eller erstatning, eller dets verdi for virksomhetens funksjoner, verdien av tapte eller ødelagte data eller eiendom, eller verdien av den tapte forretningsmulighet.

Trussel: enhver handling eller hendelse med potensial til å forårsake skade. Trusler kan være av forskjellige typer, for eksempel:
Miljømessig (f. eks flom, lyn, stormer, jordskjelv osv.)
Organisatoriske underskudd (dårlig definert ansvar, etc.)
Menneskelige feil (feil e-postadresse, mangler kritiske datoer, noterte passord på klistremerker, feilslette filer, etc.)
Teknisk svikt (maskinvarefeil, kortslutninger, harddisk krasjer, etc.)
Bevisst handlinger (hacking, phishing, svindel, bruk av ondsinnet kode, tyveri, etc.)
Kilder for trusler kan være hærverk, spionasje eller bare menneskelige feil og ulykker. I de to første tilfeller kan styrken i trusselen avhenge av to viktige faktorer: motivasjon for trusselen og attraktiviteten til eiendelen.

Sårbarhet: en svakhet i en eiendel som kan utnyttes av en eller flere trusler. Sikkerhetsproblemer kan finnes i alle deler av et IT-system, f. eks i maskinvare eller programvare, i organisatoriske strukturer, i infrastrukturen eller hos personell. Det finnes ulike typer av svakheter, som:
Fysisk (ingen adgangskontroll, ingen vakter, osv.)
Logisk (ingen sikkerhetsoppdatering, ingen antivirus, etc.)
Nettverk (ingen nettverkssegmentering, ingen sikkerhetsporter, tilkobling til mistrodde parter, osv.)
Typiske sårbarheter som følge av organisatoriske forhold blir, f. eks dårlig definerte ansvar for informasjonssikkerhet eller mangel på revisjonsspor. Ustabil strømforsyning eller plassering i et område utsatt for flom er eksempler på svakheter forårsaket av miljøet og infrastruktur.

IT sikkerhetsrisiko: en potensiell hendelse hvor en trussel vil utnytte sårbarhet i en eindel og dermed forårsaker skade på organisasjonen og dens virksomhet.

Risikovurdering: En vitenskapelig og teknologisk prosess bestående av fire trinn, trusselidentifisering, trusselkarakterisering, eksponering og karakterisering av risikovurdering.

[1] Fullstendig definisjoner finnes i referanse-dokumenter [ISO / IEC IS 13335-1] og [EU-reg. 2004/460]

2.3 Klassifiseringsskjema for risikoanalysemetode

I dette avsnittet vil jeg presentere og forklare SANDIAs klassifisering av risikoanalysemetoder vist i tabellen nedenfor (figur 2)

Level		Approach		
		Temporal	Functional	Comparative
Abstract	Expert	① Engagement	④ Sequence	⑦ Principles
Mid-Level	Collaborative	② Exercise	⑤ Assistant	⑧ Best Practice
Concrete	Owner	③ Compliance Testing	⑥ Matrix	⑨ Audit

Figure 2: SANDIAs klassifiseringsmatrise

((Tabellen hentet fra SANDIAs rapport side 13)) [36].

Som illustrert i figuren, har SANDIA kategorisert metodene i 9 kategorier. Det er to akser i denne klassifiseringen, den ene er kompetanse som er nødvendig for å gjennomføre metoden, den andre aksen er grad av "realtime" eller hvor operativ metoden er. Her vil jeg beskrive kort kolonnene, radene og cellene i matrisen [36]

Ekspert bruekes her for å referere til en ekstern konsulent som er kunnskapsrik i evalueringsformer, men ukjent med systemet.
Eier brukes her for å referere til noen som ikke er kunnskapsrik i evalueringsformer, men er kjent med systemet.

Temporal
En temporal metode "stresser" et system: faktiske tester brukes. Disse "testene" presser nøkkelkomponenter i angrep, underlagt noen eksplisitte eller implisitte begrensninger. Ytelsen til system som følge av anvendelsen av disse testene er resultatet av metoden. Det kan være upraktisk å bruke testene på systemet selv. I mange tilfeller er det eneste valget å bruke en modell av systemet i stedet.

Funksjonell (Functional)
En funksjonell metode balanserer den temporale tilnærming, beskrevet over, og den komparative tilnærming, beskrevet nedenfor. Dette er grunnen til at den funksjonelle tilnærmingen vises i midterste kolonne i figur 2. Den funksjonelle tilnærmingen avhenger mindre av en forståelse av et system (eller modell) enn den temporale tilnærming og den bruker mer system-spesifikk forståelse enn komparativ tilnærming. Den funksjonelle tilnærmingen fokuserer på trusler og beskyttelse.

Komparativ (Comparative)
Den komparative tilnærmingen presenterer en eksplisitt standard. En eier sammenligner eierens system og / eller prosedyrer med standarden. Det er ikke noe eksplisitt system modell involvert her som det er i den temporale tilnærming. Det er heller ikke en eksplisitt liste over trusler og eiendeler som det er i den funksjonelle tilnærmingen. Modellen og listene er bare implisitt til stede i generisk form. Hver standard begrenser det som regnes å være det viktigste aspektet for alle systemene i en bred kategori som f. eks

en bestemt bransje. Standarden er utarbeidet og vedlikeholdes som resultatet av kontinuerlig utvikling, ekspertvurdering og erfaring i møte med et stadig skiftende miljø. En av styrkene til denne tilnærmingen er dens enkelhet. Komparative metoder kan være ideelle for organisasjoner som begynner å sette fokus på sikkerhet.

Engasjement (Engagement)
Et Engasjement består av eksperter på jakt etter hvilken som helst måte, innenfor gitte grenser, som kan invadere eiendeler. Et eksempel på denne metodetypen i informasjonssystemer er Red Team. Noen beskriver Red Teaming som genererer sonder som er "representative for faktisk trusler", eller som fokus på å finne sårbarheter og utnytte dem som en "hacker" kan forventes å gjøre.

Øvelse (Exercise)
En øvelse linker eksperter og eiere sammen for å teste beskyttelse på eiendeler bestemt til et gitt system. Vanligvis setter eieren grenser og vilkår, eventuelt gir innsideinformasjon og samarbeider med ekspertene. Et eksempel på denne metoden i informasjonssystemer er "penetrasjonstesting" med tre subtyper: fysiske, organisatoriske (eller prosedyremessige) og elektroniske.

Overensstemmelsetesting (Compliance testing)
Testene som inngår i metoder av denne typen er slik at eieren kan utføre dem selv uten hjelp av en ekspert. For eksempel kan eieren sjekke at døren låses i en gitt installasjon og faktisk hindrer oppføring, eller eieren kan kontrollere at Windows faktisk er låst.

Sekvens (Sequence)
En sekvensmetode består av en rekke trinn, vanligvis stilt som spørsmål, og noen ganger i en form så komplisert som et flytskjema. Denne typen ber brukeren om å følge trinnene. Utgangen av trinnene er resultatet av å bruke denne typen. For eksempel Kaplan & Garrick presentere en enkel sekvensmetode:
Hva kan skje (dvs. Hva kan gå galt?)? Hvor sannsynlig er det at det vil skje? Hvis det skjer, hva er konsekvensene?

Assistent (Assistant)
En assistentmetode holder styr på ting, detaljer, slik en god menneskelig assistent gjør. I dette tilfellet holder assisten styr på kombinasjoner av lister som trusler, sårbarheter og eiendeler.

Matrise (Matrix)
En matrisemetode er et tabell-oppslag. Denne typen ber brukeren å velge områder for n-dimensjoner. Informasjonen i cellene tilsvarende n- dimensjoner er resultatet av å bruke den typen. Et ekspertsystem er en implementering av denne typen, og er representant for funksjonell tilnærming.

Prinsipper (Principles)
En Prinsippmetodetype, som alle sammenliknende typer, er en liste. Denne typen ber brukeren om å la prinsippene gjelde for deres system. Anvendelsen av disse prinsippene

er resultatet av å bruke typen. Prinsipper er mer abstrakte enn Best Practice (beskrevet nedenfor) og har dermed større bredde.

Best Practice
En beste praksis-metodetypen er en liste, men den er mer spesifikk enn Prinsippiste. Beste Praksis listen kunne være basert på en standard, f. eks en Prinsippliste, eller det kan være sin egen standard. Den Beste Praksis -listen består av direktiver: Gjør dette, Ikke gjør det. Denne metoden ber brukeren om å sammenligne hva de gjør, deres nåværende praksis, med de beste praksis-listen: listen over forskjellene er resultatet av å bruke denne typen. Beste Praksis kan være industri eller programspesifikke, men er vanligvis for abstrakt til å være gjennomføringsspesifikk.

Revisjon (Audit)
En revisjonsmetodetype er en liste, men den er mer spesifikk enn en beste praksis- liste. Revisjonen er basert på en eksplisitt standard, f. eks en beste praksis- liste eller en liste prinsipper. Denne typen ber brukeren om å vurdere effektiviteten av kontrollene på plass gjennom å oppfylle hvert element i standarden. Settet av evalueringer for settet av elementer i standarden er et resultat av å bruke den typen. Revisjoner kan være implementerings eller systemspesifikke og kan ofte brukes av en eier. Revisjon blir mer konkrete enn Best Practice og har dermed større dybde.

2.4 Konkrete produkter av risikovurdering - og risikostyring

ENISA (European Network and Information Security Agency), beskriver 13 metoder [2] og standarder for risikovurdering- og risikostyring innen informasjonsteknologi. Her er en kort beskrivelse av disse metodene og standardene i alfabetisk rekkefølge [29]]:

2.4.1 Austrian IT Security Handbook

Den østerrikske IT-sikkerhetshåndboken består av to deler:
Del 1 gir en detaljert beskrivelse av IT sikkerhetsadministrasjonsprosessen, herunder utvikling av sikkerhetsrutiner, risikoanalyse, design av sikkerhetskonsepter, gjennomføring av sikkerhetsplan og oppfølgingsaktiviteter. Del 2 er en samling på 230 baseline sikkerhetstiltak. Et verktøy som støtter implementeringen er tilgjengelig som prototype [29].

2.4.2 CRAMM

CRAMM er en risikoanalysemetode utviklet av den statlige britiske organisasjonen CCTA (Central Communication and Telecommunication Agency), nå omdøpt til Office of Government Commerce (OGC). Et verktøy med samme navn støtter metoden CRAMM.
CRAMM metoden er ganske vanskelig å bruke uten CRAMM verktøyet [26] og [44].

2.4.3 Dutch A&K analysis

Metoden "Afhankelijkheids-en kwetsbaarheidsanalyse"(A & K-analyse) ble utviklet i utkast av det nederlandske offentlige selskapet RCC. Den nederlandske Ministry of Internal

[2] ENISA satt opp en gruppe i 2005 for opptelling av de mest kjente metodene og standardene

Affairs fullført utviklingen i 1996 og har utgitt en håndbok som beskriver metoden. Metoden har ikke blitt oppdatert etterpå [29].

2.4.4 Ebios

EBIOS er et omfattende sett av veiledere (pluss et gratis åpen kildekodeverktøy) dedikert til informasjonssikkerhetsrisikoledelse. Opprinnelig utviklet av franske myndigheter, er det nå støttet av en klubb av eksperter med ulike opphav. Denne klubben er et forum for risikostyring, aktiv i å opprettholde EBIOS guider. Det gir best praksis, samt applikasjonsdokumenter målrettet mot sluttbrukerne i ulike sammenhenger. EBIOS tilnærming består i en syklus i fem faser [46].

2.4.5 ISF metoder

ISF produkter refererer ofte til hverandre og kan brukes komplementært. Slike produkter er:
En Standard for god praksis for informasjonssikkerhet (The of Good Practice for Information Security), gir et sett med prinsipper og mål for informasjonssikkerhet på høyt nivå sammen med tilhørende eksempler på god praksis.
ISFs Informasjonssikkerhetsstatus.
FIRM (Fundamental Informasjonsrisikostyring) og den reviderte FIRM graderingskortet.
SARA (Forenkelt søk Risikoanalyse).
SPRINT (forenklet Prosess for Risikoidentifikasjon) [29].

2.4.6 IT-Grundschutz (IT Baseline Protection Manual)

IT-Grundschutz gir en metode for en organisasjon å etablere en Information Security Management System (ISMS). Det omfatter både generell IT-sikkerhetsanbefalinger for etablering en relevant IT-sikkerhetsprosess og detaljerte tekniske anbefalinger for å oppnå det nødvendige IT-sikkerhetsnivå for et bestemt domene [29].

2.4.7 Marion

Metoden Marion (Methodology of Analysis of Computer Risks Directed by Levels) kommer fra CLUSIF [3] og er sist oppdatert i 1998. Det handler om en metodikk for revisjon, som, som navnet indikerer kan anslå nivået på IT-sikkerhetsrisiko for et selskap gjennom balanserte spørreskjemaer som gir indikatorer i form av notater i ulike fag med fokus på sikkerhet.

Målet med metoden er å få et bilde av om selskapet som blir revidert har et nivå som kan betraktes som "korrekt", og sammenlignet med selskaper som allerede har besvart det samme spørreskjemaet. Sikkerhetsnivået er estimert etter 27 indikatorer fordelt på seks store fag, hver av dem velger en karakter mellom 0 og 4. Nivået 3 er nivået som skal nås for å sikre at en sikkerhetsvurdering anses som riktig. Resultatet av denne analysen, vil være en mer detaljert analyse for å identifisere risiko (trusler og sårbarheter) som selskapet er utsatt for [29].

[3] http://www.clusif.asso.fr/en/clusif/present/

2.4.8 Mehari

Mehari er en risikoanalysemetode, designet av sikkerhetseksperter ved CLUSIF. Mehari foreslår en tilnærming for å definere risikotiltak tilpasset organisasjonens målsettinger [35].

2.4.9 Octave v2.0 (and Octave-S v1.0 for Small and Medium Businesses)

Den operative kritiske trusselen, eiendel, og sårbarhetsevaluering (Octave-tilnærming) definerer en risikobasert strategisk vurdering og teknikk for planlegging av sikkerhet.

Octave er en "selfdirekted" tilnærming, noe som betyr at mennesker i en organisasjon selv tar ansvar for iverksetting av organisasjonens sikkerhetsstrategi [26] og [44].

2.4.10 SP800-30 (NIST)

Dette produktet er en av "Special Publikasjon 800"-serie rapporter. Det gir veldig detaljert veiledning og identifisering av hva som bør vurderes i en risikostyring og risikovurdering når det gjelder datamaskinssikkerhet. Det er noen detaljerte sjekklister, grafikk (inkludert flytskjema) og matematiske formler, samt referanser som i hovedsak basert på amerikanske regulatoriske forhold [24].

2.4.11 Sammenligning av ENISAs risikovurdering og risikostyringsmetoder

Tabellen nedenfor (figur 3) viser en sammenligning av ENISAs risikovurdering og risikostyringsmetoder.

Attributes / Products	Threat identification	Threat characterisation	Exposure assessment	Risk characterisation	Risk assessment	Risk treatment	Risk acceptance	Risk communication	Languages	Price (method only)	Size of organisation	Skills needed[5]	Licensing	Certification	Dedicated support tools
Austrian IT Security Handbook	••	•	•	••	•••	•••	•••	•••	GE	Free	All	**	N	N	Prototype (free of charge)
Cramm	•••	•••	•••	•••					EN, NL, CZ	Not free	Gov, Large	***	N	N	CRAMM expert, CRAMM express
Dutch A&K analysis	•••	•••	•••	•••					NL	Free	All	*	N	N	
Ebios	•••	•••	•••	•••	•••	•••	•••	•••	EN, FR, GE, ES	Free	All	**	Y	N	EBIOS version 2 (open source)
ISF methods	•••	•••	•••	•••	•••	•••	•••	•••	EN	For ISF members	All except SME	* to ***	N	N	Various ISF tools (for members)
ISO/IEC IS 13335-2 (ISO/IEC IS 27005)	••	••	••	••	••	•••	•••	•••	EN	Ca. €100	All	**	N	N	
ISO/IEC IS 17799	•					•			EN	Ca. €130	All	**	N	Y	Many
ISO/IEC IS 27001						•	•		EN, FR	Ca. €80	Gov, Large	**	Y	Y	Many
IT-Grundschutz	•••	•••	•••	•••	•••	•••	•••	•••	EN, GE	Free	All	**	Y	Y	Many
Marion (replaced by Mehari)	•••	•••	•••	•••					EN, FR	Not free	Large	*	N	N	
Mehari	•••	•••	•••	•••					EN, FR	€100-500	All	**	N	N	RISICARE (ca. € 10.000)
Octave	••	••	••	••	••	••	••	••	EN	Free	SME	**	N	N	
SP800-30 (NIST)	•••	•••		•••	•••	•••	•••		EN	Free	All	**	N	N	

Figure 3: ENISAs Sammenligningssammendrag av risikovurdering og risikostyringsmetoder

(Tabellen hentet fra Inventory of risk assessment and risk management methods side 56) [29]

2.5 Standarder

Her vil jeg forklare kort noe om de forskjellige standarder. Jeg valgte å skrive om følgende: ISO, NIST, COBIT, ITIL og CMMI

2.5.1 ISO

ISO (International Organization for Standardization) og IEC (International Electrotechnical Kommisjonen) danner spesialisert system for globalt standardisering. Nasjonale organer som er medlemmer av ISO eller IEC deltar i utviklingen av internasjonale standarder gjennom teknisk komiteer.
Følgende av ISO standarder innen informasjonssikkerhet er mest relevante [31]:

1. **ISO/IEC 13335**
   Denne standarden inneholder veiledning om forvaltning av IKT-sikkerhet. Den består av Informasjonsteknologi, Sikkerhetsteknikker og forvaltning av sikkerhet innen informasjons- og kommunikasjonsteknologi.
   Den er organisert i to deler:

Del 1 ISO / IEC 13335-1: Denne delen presenterer begreper og modeller for en grunnleggende forståelse av IKT-sikkerhet, og løser generelle administrative spørsmål som er viktige for vellykket planlegging, implementering og drift av IKT-sikkerhet. Det er ikke hensikten med denne standarden å foreslå en bestemt tilnærming til styring av IKT-sikkerhet. I stedet inneholder ISO / IEC 13335-1 en generell drøfting av nyttige begreper og modeller for styring av IKT-sikkerhet.
Del 2 ISO / IEC 13335-2 Sikkerhetsrisikostyring for informasjons- og kommunikasjonsteknolog. Denne delen beskriver sikkerhetsrisikostyring på en hensiktsmessig måte til bruk for de som er involvert med styring og ledelsesaktiviteter.

2. **ISO / IEC 27000- serien Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Grunnleggende ordforråd**
Serien inneholder det grunnleggende ordforråd og gir de beste praktiske anbefalinger om informasjonssikkerhetsledelse, risiko og kontroller innenfor rammen av en samlet (ISMS), med lignende design til styringssystemer for kvalitetssikring (ISO 9000-serien). Serien har bevisst bredt omfang som dekker mer enn bare personvern, konfidensialitet eller tekniske sikkerhetsproblemer. Serien har bl.a. følgende:

   (2.1) ISO/IEC 27001:2005 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Spesifikasjon for ISMS
   ISO 27001-standarden ble publisert i oktober 2005, i hovedsak erstatter den gamle BS7799-2 standarden. BS7799 ble selv lenge en stående standard, først utgitt på nittitallet som en anbefaling.
   ISO 27001 forbedret innholdet i BS7799-2 og harmonisert med andre standarder. En ordning er innført av ulike sertifiseringsorganer for konvertering fra BS7799 sertifisering til ISO27001 sertifisering.
   Målet med standarden i seg selv er å gi en modell for etablering, implementering, drift, overvåking, gjennomgang, vedlikehold og forbedring av et styringssystem i informasjonssikkerhet.

   (2.2) ISO/IEC 17799 (ISO/IEC 27002:2005) Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Anbefaling for ISMS
   ISO 27002-standarden er det nye navnet til ISO 17799-standarden, og er en anbefaling for informasjonssikkerhet. Den skisserer i utgangspunktet hundrevis av potensielle kontroller og kontrollmekanismer, som kan bli gjennomført, i teorien, i henhold til retningslinjer gitt i ISO 27001.
   Standarden etablerer retningslinjer og generelle prinsipper for igangsetting, gjennomføring, vedlikehold og forbedrer informasjonssikkerhetsledelsen i en organisasjon. De faktiske kontrollene oppført i standarden er ment å løse de spesifikke kravene som er identifisert via en formell risikovurdering. Standarden er også ment å gi en veiledning for utvikling av organisatoriske sikkerhetsstandarder og effektiv sikkerhetsadministrasjonspraksis og bidra til å bygge tillit mellom organisatoriske aktiviteter.
   Målet med ISO / IEC 27002:2005 er å gi informasjon til ansvarlige for gjennomføringen av informasjonssikkerhet innen en organisasjon. Den kan ses som

en beste praksis for å utvikle og opprettholde sikkerheten når det gjelder standarder og ledelsespraksis i en organisasjon, og for å forbedre stabilitet på informasjonssikkerhetsområdet. Standarden understreker betydningen av risikostyring og gjør det klart at det ikke er nødvendig å iverksette hver oppgitt retningslinje, kun de som er relevante. De veiledende prinsippene i ISO / IEC 27002:2005 er de første skritt for å implementere informasjonssikkerhet.

(2.3) ISO/IEC 27003:2010 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet- Implementeringsveiledning
Den beskriver prosessen med ISMS spesifikasjon og design fra begynnelse til produksjon og gjennomføringen av prosjektplaner, dekker forberedelser og planlegging før selve gjennomføringen, og tar for seg viktige elementer bl.a. som: Ledelsesgodkjenning, vurdering av informasjonssikkerhetsrisikoer og planlegging av riktig risikobehandlinger.

(2.4) ISO/IEC 27004: 2009 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Måling
Publisert i desember 2009, gir ISO 27004 veiledning om utvikling og bruk av tiltak og måling for vurdering av effektiviteten til et implementert ISMS og kontroller, som spesifisert i ISO 27001.

(2.5) ISO/IEC 27005:2008 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Risikostyring
ISO 27005 er navnet på den viktigste 27000-seriestandarden og dekker risikostyring av informasjonssikkerhet. Standarden gir retningslinjer for informasjonssikkerhetsrisikostyring (ISRM) i en organisasjon, spesielt støttes kravene i en ISMS definert av ISO 27001.
ISO 27005-standarden består av 55 sider, og gjelder for alle typer organisasjoner. Det gir eller anbefaler ikke en bestemt metodikk.

(2.6) l ISO 27006: 2007 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Krav til organer som gir revisjon og sertifisering av ISMS
Dette er den standard som gir retningslinjer for akkreditering av organisasjoner som tilbyr sertifisering og registrering med hensyn til en ISMS.

(2.7) ISO/IEC 27033-1: 2009 Informasjonsteknologi - Sikkerhetsteknikk - Administrasjon av informasjonssikkerhet - Nettverkssikkerhet
Gir en oversikt over nettverkssikkerhet og tilhørende definisjoner. ISO-standarden beskriver konsepter og gir veiledning vedrørende styring av nettverkssikkerhet. Standarden er relevant for de som eier, drifter og /eller bruker et nettverk: ledere, ikke-tekniske brukere samt ledere og administratorer som har spesifikt ansvar for informasjonssikkerhet og /eller nettverkssikkerhet, eller som er ansvarlige for organisatoriske sikkerhet og sikkerhetspolitikk. Standarden er også relevant for alle som er involvert i planlegging, utforming og gjennomføring av

arkitektoniske aspekter ved nettverkssikkerhet.

3. **ISO/IEC 31000**
   Den ble publisert som en standard i slutten av 2009. Formålet er å gi prinsipper og generelle retningslinjer for risikostyring, og generelle retningslinjer for design, implementering og vedlikehold av risikostyringsprosesser i hele organisasjonen. Omfanget av denne tilnærmingen til risikostyring er å aktivere alle strategiske, ledelse og operative oppgaver i en organisasjon gjennom prosjekter, funksjoner og prosesser som justeres til et felles sett av risikostyringsmål.

2.5.2 NIST standard

National Institute of Standards and Technologi har bl.a. følgende standarder om Risikostyring i Informasjonsteknologisystem, informasjonssikkerhetsvurdering og adgangskontrollsystem [12]:
NIST SP 800-16, NIST SP 800-30 [4], NIST SP 800-39, NIST SP 800-115 og NIST IR 7316 [5]

2.5.3 COBIT

COBIT er et internasjonalt samlet rammeverk som integrerer alle av de viktigste globale IT-standarder, inkludert ITIL, CMMI og ISO 17799.

COBIT og ISO/IEC 17799 er to kjente standarder. Disse to er komplementære, og det finnes en kopling mellom ISO/IEC 17799 og COBIT der hver prosess som er beskrevet i COBIT koples mot kontroller i ISO-standarden [40].

COBIT brukes globalt av de som har det primære ansvaret for forretningsprosesser og teknologi, de som er avhengig av teknologi for relevant og pålitelig informasjon. Den gir kvalitet, pålitelighet og kontroll av informasjonsteknologien.

Formålet med COBIT er å gi ledelsen og forretningsprosesseiere en styringsmodell som bidrar til å levere verdi fra IT og forståelse og håndtering av risiko forbundet med IT. Det er en kontrollmodell for å møte behovene for IT-styring og sikre integriteten av informasjon og informasjonssystemer [26] og [1].

Retningslinjene gir ledelsen et sett med verktøy som tillater egenvurdering for å ta valg for kontroll, gjennomføring og forbedringer av IT og måle oppnåelse av mål og korrekt gjennomføring av IT-prosesser. I retningslinjene for ledelsen er det inkludert modenhetsmodeller, viktige mål og beregninger, ansvarsbeskrivelser eller (RACI) diagrammer for å klargjøre roller og ansvar for å støtte ledelsesmessige beslutninger. For å oppsummere: IT-ressurser forvaltes av IT-prosesser for å oppnå IT-mål som reagerer på virksomheten krav. Dette er den grunnleggende prinsipp i COBIT rammeverket, som illustrer av COBIT kuben (Figur 4).

[4] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[5] http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf

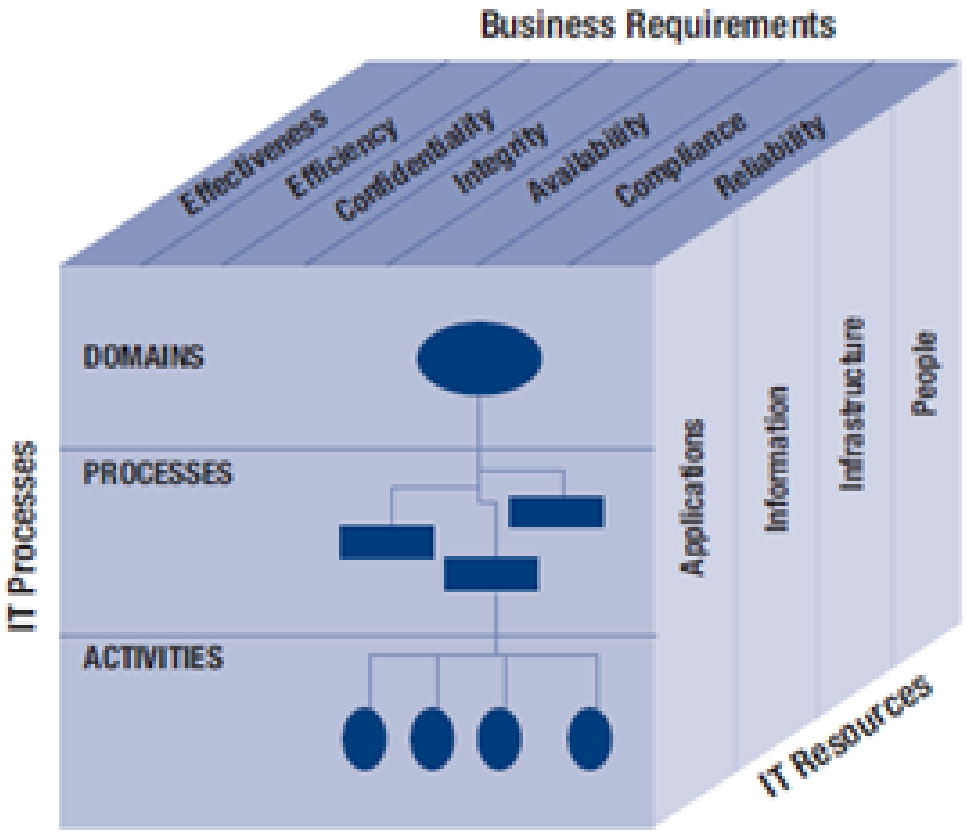

Figure 4: COBIT kube

(Figuren hentet fra [1]).

COBIT kan du se på som en 360 graders sirkel inndelt i 34 prosesser. Det er de prosesser som en IT-virksomhet bør består av. Hele COBIT er inndelt i fire område: planlegging (Plan and Organize), Tilegne og iverksette (Accquire and implement), Levering og støtte (Deliver and Support) og Overvåking og Evaluering (Moniter and Evaluate). Planlegging er inndelt til 11 prosesser, 7 under Tilegne og iverksette, 13 Levering og støtte og 5 Overvåking og Evaluering. Prosessnummer 1, IT-startegi, er den primære prosessen for å bestemme det videre løpet [26] og [1].

RISK IT ligger også inne i COBIT-familien. Den dekker risikostyring, evaluering og svarprosesser og aktiviteter. RISK IT er et rammeverk basert på et sett med veiledende prinsipper for effektiv styring av IT-risiko og den utfyller COBIT. Mens COBIT gir et sett med kontroller for å redusere IT-risiko, gir Risk IT et rammeverk for bedriftene for å identifisere, styre og håndtere IT-risiko. Enkelt sagt, gir COBIT midlene for risikostyring, Risk IT gir målene [34].

RISK IT gjør følgende:

- Gir et felles språk for å hjelpe kommunikasjon og forståelse mellom business, IT, risiko og revisjonsstyring
- Gir en ende-til-ende, omfattende oversikt over all risiko knyttet til bruk av IT og en tilsvarende grundig behandling av risikostyring, fra tonen og kulturen på toppen, til

operative spørsmål.

2.5.4 ITIL

ITIL (IT Infrastructure Library) er et strukturert rammeverk eller ontologi for kvalitetssikring av leveranse, drift og support innen IT-sektoren. ITIL går inn i organisasjonsstrukturen, og de faglige ferdigheter til en IT-organisasjon, ved å presentere et utførlig sett strynings prosedyrer som en organisasjon kan benytte til å styre sine IT-operasjoner. Disse prosedyrer er leverandøruavhengige og er relevante for alle aspekter av en It-infrastruktur [32].
ITIL-prosessene er følgende [8]: Brukersenter (Service Desk), Hendelsesstyring (Incident Management), Problemstyring (Problem Management), Endringsstyring (Change Management), Produksjonssetting (Release Management, Konfigurasjonsstyring (Configuration Management), Styring av tjenestenivå (Service Level Management), Kapasitetsstyring (Capacity Management), Tilgjengelighetsstyring (Availability Management) og Kontinuitetsstyring (Continuity Management).

2.5.5 CMMI

Capability Maturity Model Integration (CMMI) er en prosessforbedringsmodell først publisert i 1999, basert på prosessforbedringsrammeverket Capability Maturity Model. Pr. 2008 finnes det to varianter av CMMI [6]:
CMMI for Development (CMMI-DEV) som omfatter utviklingsprosesser for produkter og tjenester.

CMMI for Acquisition (CMMI-ACQ) som omfatter håndtering av forsyningskjeder, anskaffelser og outsourcing, og gjelder både offentlig og privat sektor. Grunnprinsippene i CMMI er Systematisk forbedring som krever repeterbarhet gjennom veldokumenterte prosesser, der man sørger for å lære av erfaringer.

Prosjekter styres i størst mulig grad gjennom fakta fremfor subjektive vurderinger. Forbedring skal baseres på innhenting og analyse av objektive data i prosjektene. Modellen forteller hva som skal tilfredsstilles, men ikke hvordan man løser det. Modellen tilbyr et veikart gjennom 5 ulike modenhetsnivåer slik at man bygger stein på stein. Nivå 2 er rett og slett basis prosjektledelse [39].

CMMI kan brukes i tre ulike områder: produkt- og tjenesteutvikling (CMMI for Development-modellen), Serviceetablering, forvaltning, og levering (CMMI for Tjenester modell) og i produkt og service kjøp (CMMI for kjøp modell).

[6] Fra Wekipidia, http://www.wikipedia.org/

3 Litteraturoversikt

I dette kapitlet vil jeg forklare de områdene som jeg anser som relevant for min oppgave. Her vil jeg dele områdene som følger:
Lover og forskrifter, Tilsyn med informasjonssikkerheten i helsetjenesten, veiledninger (anbefalinger) og relatert arbeid i andre tilsynsorganer.

Når det gjelder lover og forskrifter, finnes det flere. Jeg vil nevne her lovverket som er mest relevant for Helsetilsynets arbeid innen informasjonssikkerhet. I og med at Helsetilsynet behandler sensitiv og taushetsbelagt informasjon, er Personopplysningsloven, Helseregisterloven, Personopplysningsforskriften og Forskrift om informasjonssikkerhet de mest relevante. De dreier seg om informasjonssikkerhet bl.a. sikring av konfidensialitet, integritet og tilgjengelighet, risikovurdering, sikkerhetsrevisjon, avvikshåndtering og tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon. Jeg lister her også "Norm for informasjonssikkerhet i helsesektoren" som har som formål å bidra til tilfredsstillende informasjonssikkerhet i helsesektoren.

Deretter vil jeg forklare tilsyn med informasjonssikkerheten i helsetjenesten og prøver å gi et bilde av det og hvordan tilsynet er organisert samt tilsynsoppgavene tildelt mellom forskjellige berørte etater i henhold til regelverket.

Jeg vil også peke på noen veiledninger og anbefalinger som man kan ha nytte av i denne sammenhengen. Pr. oppgavens skriving er det noen veiledninger som er på høring og de kan fort bli integrert i lovverket. I tillegg vil jeg nevne noen generelle anbefalinger som kan hjelpe og danne grunnlegende erfaringer. Til slutt i dette kapitlet vil jeg skrive litt om hvor langt andre tilsynsorganer har kommet i dette feltet for å løse sine oppgaver.

3.1 Lover og forskrifter

Lover og forskrifter etc. er i all hovedsak tilgjengelig via lovdata (www.lovdata.no). Det finnes flere lover og forskrifter om informasjonssikkerhet. Jeg lister opp de som (pr. i dag) er aktuelle for min oppgave.

- LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (Helseregisterloven). Her er §§13, 13a, 14, 15, 16, 17 og 18:
  http://www.lovdata.no/all/hl-20010518-024.html [Gjengitt i Tillegg A.1].
- Lov om behandling av personopplysninger (personopplysningsloven). Hele loven er tilgjengelig på siden:
  http://www.lovdata.no/all/nl-20000414-031.html
  §1. Lovens formål
  Formålet med denne loven er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger.
  Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende

personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.

- FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften), hele kapittel 2 omhandler emnet informasjonssikkerhet, og stiller blant annet krav til risikovurderinger og sikkerhetsrevisjoner. Den stiller krav til fysisk sikring av utstyr som brukes for å behandle personopplysninger, samt sikring av konfidensialitet,tilgjengelighet og integritet. Forskriften trådde i kraft 1. januar 2001 [Gjengitt i Tillegg A.2].
  http://www.lovdata.no/for/sf/fa/xa-20001215-1265.html
- FOR 2001-07-01 nr 744: Forskrift om informasjonssikkerhet. Hele Forskriften gjelder informasjonssikkerhet og er tilgjengelig på siden:
  http://www.lovdata.no/cgi-wift/ldles?doc=/sf/sf/sf-20010701-0744.html
- LOV 1999-07-02 nr 61: Lov om spesialisthelsetjenesten m.m. (spesialisthelsetjenesteloven). Med tilhørende forskrifter.
  http://www.lovdata.no/all/hl-19990702-061.html
  Krav til informasjonssikkerhet
  Konfidensialitet Jf. §3-2 skal journal- og informasjonssystemene være forsvarlige. Det er videre krav om å hindre at utenforstående får tilgang eller kjennskap til journal. Jf. §6-1 har enhver som utfører tjeneste eller arbeid for helseinstitusjon taushetsplikt etter Forvaltningsloven §§13 - 13e.
  Tilgjengelighet Foruten det generelle kravet om forsvarlige journal- og informasjonssystemer er det krav om å sikre Helsetilsynet tilgang til opplysninger som tilsynsorganet finner nødvendig, herunder opplysninger om personskade på pasient - jf.§§6-2 og 3-3. Iht. §3-4 skal helseinstitusjonens kvalitetsutvalg også ha tilgang til nødvendige opplysninger. Jf. §3-11 skal pasienter gis tilgang til opplysninger etter Pasientrettighetsloven. Allmennheten skal - i medhold av samme bestemmelse - sikres tilgang til informasjon for å ivareta rettigheter, bl.a. etter Pasientrettighetsloven §§2-1 - 2-5. I medhold av §6-1 skal også andre forvaltningsorgan ha tilgang til opplysninger - for å løse oppgaver etter loven, eller for å forebygge vesentlig fare for liv eller helse. Dessuten skal kommunehelsetjenesten ha tilgang til nødvendige opplysninger om helsemessige forhold - jf. §6-3.
  Integritet Krav om opplysningenes integritet følger av det generelle kravet om at journal- og informasjonssystemer må være forsvarlige.
- LOV 1999-07-02 nr 64: Lov om helsepersonell m.v. (helsepersonelloven)
  http://www.lovdata.no/all/tl-19980320-010-001.html
  Loven stiller krav om informasjonssikkerhet. Krav om taushetsplikt er definert svært presist, inklusive tilfeller hvor taushetsplikt ikke er påkrevet. Videre stiller loven krav om dokumentasjon, dvs. plikt til å føre journal. Det tillates både papirbaserte og elektroniske journalløsninger. Det skal være mulig å spore hvem som har oppdatert journalen, noe som igjen stiller krav om autentisering av brukere (i tilfeller med bruk av elektronisk journal). Det er også stilt krav om etablering av internkontroll i virksomheten.
- FOR 2000-12-21 nr 1385: Forskrift om pasientjournal (Journalforskriften)
  http://www.lovdata.no/for/sf/ho/xo-20001221-1385.html

Krav til informasjonssikkerhet omfatter konfidensialitet, tilgjengelighet og integritet i §10.

- LOV 1998-03-20 nr 10: Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven) http://www.lovdata.no/all/hl-19980320-010.html
  Loven stiller omfattende krav til både administrative, fysiske, organisatoriske og systemtekniske forhold i forbindelse med behandling av skjermingsverdig informasjon. Kravene er spesielt knyttet opp mot konfidensialitet, men også integritet og tilgjengelighet er omhandlet.
- Norm for informasjonssikkerhet i helsesektoren [13].
  Normen er utgitt av Sosial- og helsedirektoratet. Den er utarbeidet av representanter for sektoren, herunder fra Den norske legeforening, representanter for de regionale helseforetak, Norsk Sykepleierforbund, Norges Apotekerforening og Kommunenes Sentralforbund. I tillegg har Datatilsynet, Helsetilsynet, Rikstrygdeverket og Sosial- og helsedirektoratet deltatt i arbeidet. Normen angir det nivå som anses nødvendig for å oppnå tilfredsstillende informasjonssikkerhet og er i utgangspunktet et veiledende dokument, Men vil være juridisk bindende for de som tilknyttes Norsk Helsenett.
  Normen er også ment å være et hjelpemiddel i den enkelte virksomhets arbeid med informasjonssikkerhet. Normen er først og fremst basert på personvern- og helselovgivningens krav til å etablere tilfredsstillende informasjonssikkerhet for systemer inneholdende helse- og personopplysninger, jf. personopplysningsloven §13, helseregisterloven §16 og personopplysningsforskriften kapittel 2.

3.2 Tilsyn med informasjonssikkerhet i helsetjenesten

I dette kapitlet vil jeg strukturere Tilsyn med informasjonssikkerhet i helsetjenesten i to deler, hvor den første er "Statlig tilsyn" og den andre er "internkontroll". Under Statlig tilsyn vil jeg forklare det legale grunnlaget for både Statens helsetilsyn og Datatilsynet.

3.2.1 Statlig tilsyn

Både Datatilsynet og Statens helsetilsyn har etter bestemmelser i lovgivningen både plikt og rett til å føre tilsyn med informasjonssikkerheten i helsetjenesten. Hovedhjemlene for Datatilsynets tilsyn finnes i kapittel VIII i lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven)[1]. Personopplysningsloven §42 fastsetter Datatilsynets myndighet slik:
Datatilsynet er et uavhengig forvaltningsorgan administrativt underordnet Kongen og departementet. Kongen og departementet kan ikke gi instruks om eller omgjøre Datatilsynets utøving av myndighet i enkelttilfeller etter loven. Datatilsynet skal:

1. *føre en systematisk og offentlig fortegnelse over alle behandlinger som er innmeldt etter §31 eller gitt konsesjon etter §33, med opplysninger som nevnt i §18 første ledd jf. §23,*
2. *behandle søknader om konsesjoner, motta meldinger og vurdere om det skal gis pålegg der loven gir hjemmel for dette,*

[1] http://www.lovdata.no/all/nl-20000414-031.html

3. *kontrollere at lover og forskrifter som gjelder for behandling av personopplysninger blir fulgt, og at feil eller mangler blir rettet,*
4. *holde seg orientert om og informere om den generelle nasjonale og internasjonale utviklingen i behandlingen av personopplysninger og om de problemer som knytter seg til slik behandling,*
5. *identifisere farer for personvernet, og gi råd om hvordan de kan unngås eller begrenses,*
6. *gi råd og veiledning i spørsmål om personvern og sikring av personopplysninger til dem som planlegger å behandle personopplysninger eller utvikle systemer for slik behandling, herunder bistå i utarbeidelsen av bransjevise atferdsnormer,*
7. *etter henvendelse eller av eget tiltak gi uttalelse i spørsmål om behandling av personopplysninger, og*

Datatilsynet har også hjemmel spesielt rettet inn mot helsetjenesten gjennom §31 i lov av 18. mai 2001 nr. 24 om helseregistre og behandling av helseopplysninger (helseregisterloven) som lyder slik:

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 Helsetilsynet i fylket etter lov 30. mars 1984 nr. 15 om statlig tilsyn med helsetjenesten. Tilsynsmyndighetene kan kreve de opplysninger som trengs for at de kan gjennomføre sine oppgaver. Tilsynsmyndighetene kan som ledd i sin kontroll med at lovens regler etterleves, kreve adgang til steder hvor det finnes helseregistre, helseopplysninger som behandles elektronisk og hjelpemidler for slik behandling av opplysninger. Tilsynsmyndighetene kan gjennomføre de prøver eller kontroller som de finner nødvendig, og kreve bistand fra personalet på stedet i den grad dette må til for å få utført prøvene eller kontrollene. Retten til å kreve opplysninger eller tilgang til lokaler og hjelpemidler i henhold til annet og tredje ledd gjelder uten hinder av taushetsplikt. Tilsynsmyndighetene og andre som utfører tjeneste for tilsynsmyndighetene, har taushetsplikt etter §15. Taushetsplikten omfatter også opplysninger om sikkerhetstiltak. Kongen kan gi forskrift om unntak fra første til fjerde ledd av hensyn til rikets sikkerhet. Kongen kan også gi forskrift om dekning av utgiftene ved kontroll. Skyldige bidrag til dekning av utgiftene er tvangsgrunnlag for utlegg.

Helsetilsynet er organisert med en sentral enhet (Statens helsetilsyn) og lokale enheter i hvert fylke (Helsetilsynet i fylket). Helsetilsynet i fylket er administrativt underlagt Fylkesmannen, men tilsynsfaglig underlagt Statens helsetilsyn. Hovedhjemmel for det statlige tilsynet med helsetjenesten finnes i lov av 30. mars 1984 nr. 15 om statlig tilsyn med helsetjenesten (helsetilsynsloven) . I §§1 og 2 første og annet ledd er tilsynsoppgavene beskrevet slik:
§1 Tilsynsmyndighetene
Statens helsetilsyn har det overordnede faglige tilsyn med helsetjenesten i landet og skal utøve myndighet i samsvar med det som er bestemt i lover og forskrifter. Statens helsetilsyn ledes av en direktør. Direktøren utnevnes av Kongen på åremål. I hvert fylke skal det være en fylkeslege. Fylkeslegen er tillagt myndighet som " Helsetilsynet i fylket " i lover og forskrifter og er da direkte underlagt Statens helsetilsyn. Forøvrig er fylkeslegen underlagt fylkesmannen. Fylkeslegen utnevnes av Kongen. Kongen kan bestemme at en fylkeslege skal ha mer

enn ett fylke i sin embetskrets. Statens helsetilsyn kan gi den enkelte fylkeslege oppgaver som omfatter et større geografisk område enn eget fylke.

§2 Helsetilsynet i fylket og Statens helsetilsyns oppgaver Helsetilsynet i fylket skal føre tilsyn med alt helsevesen og alt helsepersonell i fylket og i tilknytning til tilsynet gi råd, veiledning og opplysninger som medvirker til at befolkningens behov for helsetjenester blir dekket. Helsetilsynet i fylket skal holde Statens helsetilsyn orientert om helseforholdene i fylket og om forhold som innvirker på disse.

Disse bestemmelsene gjelder for offentlige så vel som private tjenesteytere. I annen lovgivning (f. eks helsepersonelloven, spesialisthelsetjenesteloven og kommunehelsetjenesteloven) er tilsynsoppgavene ytterligere spesifiserte, uten at dette endrer på prinsippene som beskrives i helsetilsynsloven. Når hjemlene for Datatilsynet sammenholdes med hjemlene for Helsetilsynet, jf. særlig §31 i helseregisterloven, er det gjennom lovgivningen etablert en grensedragning mellom tilsynsoppgavene til Datatilsynet og Helsetilsynet. Datatilsynet skal konsentrere sitt arbeid om sikkerheten i informasjonssystemene. Helsetilsynets arbeid skal være konsentrert om ytelsen av helsetjenester og helsepersonellets aktiviteter. I grenseflaten mellom disse skal da Datatilsynet ha sin oppmerksomhet mot det spesielle ved sikkerheten i informasjonssystemene, mens Helsetilsynet skal se på informasjonssystemene og informasjonshåndteringen som en del av det totale helsetjenestesystemet.

Denne tette grenseflaten tilsier at de to tilsynsetatene bør ha god kjennskap om hverandres arbeid. Ikke minst bør Helsetilsynets tilsynsførere ha kunnskap om informasjonssikkerhet fordi dette er en så viktig del av helsetjenestens styring av kvalitet og sikkerhet. En svikt på dette området vil være en alvorlig trussel i forhold til befolkningens tillit til helsetjenesten. Informasjonssikkerhet i helsetjenesten er ikke noe som kan behandles og forstås uavhengig av sikkerhet og kvalitet ved ytelsen av helsetjenestene. Det er en del av sikkerhet og kvalitet ved selve tjenesteytelsen i helsesektoren.
Det er ikke etablert en nærmere spesifisert samarbeidsavtale om denne grensedragningen mellom Datatilsynet og Helsetilsynet. Statens helsetilsyn har slike samarbeidsavtaler med noen andre statsinstitusjoner, f. eks Petroleumstilsynet. Selv om det ikke er en egen samarbeidsavtale mellom de to tilsynsetatene, har de hatt et samarbeid om planlegging og gjennomføring av noen større tilsyn. Det er også vanlig praksis at Datatilsynet informerer Helsetilsynet i fylket når de gjennomfører tilsyn med informasjonssikkerheten i helsetjenesten. Det hender også at tilsynsførere fra Helsetilsynet i fylket deltar sammen med Datatilsynet ved slike tilsyn.

3.2.2 Internkontroll

Prinsippet om internkontroll (egenkontroll) ligger til grunn både for de ulike helsetjenesteyteres styring av informasjonssikkerheten og for deres styring av ytelsen av helsetjenester. Dette prinsippet er hjemlet som lovkrav i §17 i helseregisterloven [Gjengitt i Tillegg A.1], §14 i personopplysningsloven og §3 i helsetilsynsloven. Det er ikke noen vesentlig forskjell på dette prinsippet enten det er hjemlet i personopplysningslovgivningen eller i helsetjenestelovgivningen.

Det er heller ikke noe i lovgivningen som tilsier at virksomhetene skal bygge opp

separate internkontrollsystemer for å ivareta kravene i de ulike lovene. Virksomhetenes internkontrollsystem kan med fordel omfatte alle de ulike lovene der det stilles krav om internkontroll, jf også det som er nevnt ovenfor om informasjonssikkerhet som en viktig del av den totale sikkerhet og kvalitet ved ytelsen av helsetjenester. Dette vil både lette virksomhetenes egen styring og det åpner for et nært samarbeid om tilsyn fra de statlige tilsynsetatenes side.

3.3 Veiledninger / anbefalinger

Her vil jeg dele veiledninger i to grupper hvor den ene er på høringer dvs. enda ikke gjeldende og den andre er generelle anbefalinger Følgende veiledninger som pr. oppgavens dato er på høring:

3.3.1 På høring

Følgende veiledninger som pr. oppgavens dato er på høring:

- Høring av forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre.I denne forskriften er lagt stor vekt på å få frem et regelverk som er godt balansert mellom hensynet til rask tilgang til relevante pasientopplysninger når det er nødvendig for å yte helsehjelp til pasienten, og hensynet til pasientens rett til vern om opplysningene [6].
  http://www.regjeringen.no/nn/dep/hod/Dokument/Hoyringar/Hoyringsdokument/2010/Horing-av-forslag-til-forskrift-om-informasjonssikkerhet-tilgangsstyring-og-tilgang-til-helseopplysninger-i-behandlingsrettede-helseregistre/Horingsbrev.html?id=604374
- Kompetansekrav for bruk av IKT i helse- og omsorgssektoren [9].
  Dett er et dokument som utgitt av KITH (Kompetansesenter for IT i helse- og sosialsektoren AS). Kompetansekravene spesifiserer sentrale områder som helsepersonell skal være orientert om, ha kunnskap om eller forståelse for når de benytter eHelsesystemer. Disse kompetansekrav er grunnleggende for bruk av IKT i helse- og omsorgssektoren.
- Norsk helsenett SF strategi [14].
  Dette er et konkret og kortfattet strategidokument med utgangspunkt i overordnede nasjonale rammer/føringer og formelle stiftelsesdokumenter utgitt av Norsk Helsenett SF. Norsk Helsenett har tre prioriterte virksomhetsområder: drift, utvikling og støttefunksjoner. Hvert virksomhetsområde består av tre til fem hovedstrategier.

3.3.2 Generelle anbefalinger

Følgende dokumenter gir anbefalinger til å ta nytte av:

- IT-revisjon med fokus på sikkerhetsrevisjon [7].
- En veiledning om internkontroll og informasjonssikkerhet [3].
- Veiledning til §5-1 gjennomføring av konfigurasjonskontroll [23].
- Veiledning i risiko- og sårbarhetsanalyse ROS [20].
- Veiledning i sikkerhetsadministrasjon [21].

- Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner [19].
- Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven [16].
- Risikoanalyse - Metodegrunnlag og bakgrunnsinformasjon [15].

- Veiledning lover og regler med betydning for informasjonssikkerhet [22].

3.4 Risikoanalysemetodikk i Norge

Risikoanalysemetodikk brukes i Norge i forbindelse med tilsyn bl.a. av Finanstilsynet. Finanstilsynet som tidligere het Kredittilsynet ble etablert i 1986. Det nye navnet (Finanstilsynet) reflekterer bedre at tilsynet omfatter både bank, forsikrings- og verdipapirtilsyn og andre oppgaver. Finanstilsynet er et selvstendig tilsynsorgan som bygger på lover og vedtak fra Stortinget, Regjeringen og Finansdepartementet og på internasjonale standarder for finansielt tilsyn. Finanstilsynet har tilsyn med banker, finansieringsforetak, e-pengeforetak, forsikringsselskap, pensjonskasser, verdipapirforetak, verdipapirfondsforvalting og markedsadferd i verdipapirmarkedet, børser og andre regulerte markeder, oppgjørssentraler og verdipapirregister, eiendomsmeglingsforetak, inkassoforetak, regnskapsførere og revisorer. I tillegg har Finanstilsynet kontroll med den finansielle rapporteringen til børsnoterte foretak [4].

3.4.1 IT-tilsyn

Finanstilsynet utfører IT-tilsyn basert på internasjonal standard. Det ble i 2009 gjennomført 22 IT-tilsyn, enten separat eller i samband med ordinære tilsyn i foretakene. I tillegg ble det utført 21 forenklede IT-tilsyn [2]. I figur 2 er det et eksempel på en del av skjemaet som Finanstilsynet bruker i sitt tilsynsarbeid. De har forskjellige type skjemaer etter virksomhetstype og prosesstype som gjennomføres.

[2] I henhold til Finanstilsynets årsmelding 2009 side 32

Grad av viktighet, rangering 1 til 34	PO9 IT-Prosesser	Kontroll-spørsmål		Sårbarhet		
				H	M	L
	Vurdere risiko	Ja	Nei			
	1. Har foretaket inkludert vurdering av IT-risiko og styring og kontroll av IT-virksomheten i foretakets øvrige rammeverk for risikohåndtering?					
	2. Har foretaket etablert en prosess for risikoanalyser av IT-virksomheten?					
	3. Har foretaket etablert retningslinjer / metode for hvordan ny risiko skal identifiseres?					
	4. Har foretaket etablert ansvarsfordeling for gjennomføring og oppfølging av risikoanalysen?					
	5. Har foretaket fastsatt kriterier for akseptabel risiko forbundet med bruk av IT-systemene?					
	6. Er det etablert tiltak som sikrer at det blir gjennomført systematiske vurderinger av forskjellige typer risiko som f. eks. innføring av ny teknologi, endringer, single point of failure, sikkerhet, lover, beredskap, organisasjon og grensesnitt?					
	7. Har foretaket etablert tiltak som sikrer at risikoanalyse av IT-virksomheten gjennomføres minst årlig og ved større endringer?					

Figure 5: En del av IT-tilsynsskjema for Finanstilsynet

Figuren hentet fra side 6 på:

http://www.finanstilsynet.no/Global/Temasider/IT-tilsyn/Op_risk_forenklet%20_i_mal.pdf

3.4.2 Noen viktige funn fra IT-tilsyn

I sin årsrapport Risiko- og sårbarhetsanalyse (ROS) - 2007 og 2008 [3] , hevder Finanstilsynet at i løpet av hvert av disse årene, ble det gjennomført 20 stedlige IT-tilsyn. I tillegg var det 35 foretak som i forbindelse med ordinær inspeksjon leverte egenevalueringsskjema for foretakets IT-virksomhet og ble vurdert i henhold til prosedyre for forenklet IT-tilsyn. Følgende er viktige funn fra IT-tilsynene som ble gjennomført i 2007 og 2008:

- Manglende eller ufullstendige ROS-analyser.
- Kompetanse til gjennomføring av ROS-analyser er et gjennomgående problem.
- Manglende styring og kontroll ved gjennomføring av større IT-prosjekter.
- Fortsatt problemer knyttet til endringshåndtering, samt for dårlig grunnlag ved beslutning om å iverksette drift av nye løsninger.
- Mer oppmerksomhet må rettes mot infrastruktur og felles løsninger - kompetansen i det enkelte foretaket kan svekkes når oppgaver ivaretas utenfor foretaket.
- Problematisk å opprettholde tilstrekkelig nøkkelkompetanse ved utkontraktering og på områder med manglende industristandarder.

[3] http://www.finanstilsynet.no/

- Mangelfulle prosessbeskrivelser og dokumentasjon i foretak med stor grad av egenutvikling.
- Ikke tilstrekkelig kontroll med og test av katastrofeløsninger.
- Utilstrekkelig konfigurasjonsstyring.
- Manglende etterlevelse av egne endringsprosesser.

4 Metode

I det følgende kapitlet vil jeg redegjøre for den fremgangsmåten jeg har valgt for å belyse min problemstilling. Her vil jeg synliggjøre hvordan jeg har kommet frem til metoden og hva som jeg har vurdert som riktig metode for mine forskningsspørsmål. Forskningsdesign er en strategi for å innhente informasjon fra virkeligheten [38].
Designet er bindeleddet mellom de spørsmål man ønsker å få svar på, og innhenting av data som skal belyse den aktuelle problemstillingen. Forskningsdesign kan sies å være de reglene og prosedyrene som kreves for å innehente informasjon om forskningsspørsmålet.
Et forskingsarbeid kan foretas på mange måter. Det metodiske valget en tar er avhengig av hvilke data man ønsker å samle inn, samt hvilken fremgangsmåte som er relevant i forhold til forskingsarbeidet man gjør.
Nedenfor vil jeg presentere og identifisere hvilken metode som er mest hensiktsmessig for hvert av forskningsspørsmålene. Tankerekken er sortert som følger:

- *Forskningsspørsmål.*
- *Sammendrag av de metodene som kan tenkes å være aktuelle for å få frem kunnskapen*
- *Rammebetingelsene som setter begrensninger på friheten i valg av metode på grunn av resurser og rammer for gjennomføring, for eksempel datatilgjengelighet, tid, ressurser, konfidensialitet, kompetanse etc.*
- *Metodevalg ut fra pålitelighet, gyldighet i forhold til problemstillingen dvs. for hvert av forskningsspørsmålene, en vurdering av i hvilken metode som kan være egnet.*
- *Konklusjon: hvilken metode/metoder er mest hensiktsmessig basert på resonnement ovenfor.*

4.1 Forskningsspørsmål nummer 1

Hvilken kompetanse i informasjonssikkerhet har Helsetilsynet som grunnlag for å utføre tilsyn?
For å kunne besvare dette hovedspørsmålet, må jeg ha besvart flere avledede forskningsspørsmål. Hvis man velger en analytisk fremgangsmåte, kan man starte med
Hva er kravene til helseforetakene med hensyn på informasjonssikkerhet?
Dette må etableres først. Deretter kommer et underspørsmål:
Hvilke informasjonssikkerhets tiltak må helseforetakene gjennomføre for at de kravene skal være tilfredsstilt?
Og så må man finne ut hvilke tiltak som må gjennomføres for at kravene skal tilfredstilles. For å kunne avgjøre om disse tiltakene er gjennomført, må man vite:
Hvilken kompetanse må man da ha for å kontrollere dette?
Videre kommer enda et underspørsmål til:
Hvordan skal man teste at Helsetilsynets tilsynsførere har denne kunnskapen?

De metodene som tenkes for å besvare de avledede forskningsspørsmålene kan være

følgende:

- Å teste tilsynsførere ved å lage et Quiz i informasjonssikkerhet i form av spørreskjema. I denne quizen kunne jeg ha spurt om hva betyr et virus, hva sikkerhetspolicy betyr, hva tilgangsstyring eller loggføring betyr, om du er kjent med tilgangsreglene i din organisasjon osv.
  Begrensninger går her på gyldighet og pålitelighet fordi psykologisk sett er folk veldig forsiktige med å si at de ikke kan noe som helst eller at de kan alt. Jeg regner med at mange antakelig ville ha sagt at de kunne litt og jeg kunne fått samling mot midten. Det er klart at jo mer indirekte spørsmål, jo mer problematisk er gyldigheten.
  Denne metoden er ikke vanskelig å gjennomføre, men datatilgjengelighet kan også være et problem i denne metoden fordi jeg kanskje ikke ville fått nok svar og folk er redde for konsekvenser av besvarelsene.
- Å ha sjekket CV'er til ansatte som er involvert i tilsyn gjennom personalkontoret i administrasjon. Formåle med dette ville være å få vite om hva slags bakgrunn disse ansatte har og om de har tilegnet seg noe kompetanse innen informasjonssikkerhet.
  Her er noen rammer og begrensninger pga. konfidensialitet da CV'er også inneholder personlige opplysninger i tillegg til at det er tidskrevende både for meg og personalkontoret å samle disse dataene for et antall tilsynsførere som er spredt i ulike deler av landet. Det er både resurskrevende og tidskrevende å få oppdaterte CV-opplysninger som betyr at datatilgjengelighet også kan være problematisk.
- Å lage en enkel spørreundersøkelse som fylles ut av alle Helsetilsynet i fylkene. Formålet med denne spørreundersøkelsen er å kartlegge hvor stort behovet er for kompetanseøkning, og hvilke områder det er størst utfordringer innen informasjonssikkerhet. Dette er en enkel måte, da skjemaene kan sendes pr. e-post. Men datatilgjengelighet er ikke lett på denne måten fordi svarprosenten kan bli for lav.
- Å velge kvalitativ metode ved å intervjue personer. Et intervju kan være en rask måte å samle mye informasjon på fra den som blir intervjuet [42] og [45]. Man velger gjerne nøkkelpersoner som er nært knyttet til emnet, og som dermed har kunnskap om og (kjennskap til) den aktuelle problemstillingen.
- Velge trianguleringsmetode. Triangulering betyr å peile inn et punkt fra tre kanter, og i samfunnsvitenskapen betyr det å se ting fra flere perspektiver. Altså at forskeren samler inn og analyserer data ved hjelp av flere forskjellige teknikker. Holme & Solvang lister opp en rekke fordeler ved å bruke triangulering, blant de viktigste finner vi at gyldigheten til metoden testes og at tillitten til analyseresultatene styrkes når ulike metoder fører til samsvarende konklusjoner [33].
  Sammenlignet med rene kvalitative eller kvantitative metoder, er metodetriangulering en forholdsvis ny tilnærming og utformingen av denne er fremdeles under utvikling.
- Nedskrivning av mine egne erfaringer og min innsikt fra mitt arbeid innen IT i Helsetilsynet i mer enn 13 år. Jeg vil bruke meg som en kilde for data. Begrensningene her går på pålitelighet og gyldighet.
- Litteraturstudium

Konklusjon:
De metodene som er mest hensiktsmessige basert på resonnement ovenfor, og som jeg har tenkt å bruke, er følgende: Min hovedmetode er å bruke trianguleringsmetode. Triangulering kan styrke troverdighet, man kompenserer for svakheter ved å kombinere forskjellige analytiske tilnærminger. Forskeren bruker enten flere metoder, ulike datakilder eller flere uavhengige forskere for å styrke troverdigheten. Metodetriangulering kategoriseres vanligvis i tre kategorier. Det er triangulering mellom kvalitative metoder, triangulering mellom kvalitative og kvantitative metoder, samt triangulering mellom kvantitative metoder. Et intervju kan foregå på mange måter hvor en av måtene kan være telefonintervju.

Metoden som jeg tenker å bruke er basert på å engasjere min overordnede sjef, assisterende helsedirektør, til å ringe sin underordnende i noen utvalgte Helsetilsynet i fylkene for å få oversikt over kompetansenivået innenfor informasjonssikkerhet hos tilsynsførerne hos Helsetilsynet i fylket [Spørsmålene er gjengitt i Tillegg E].
Selv om man i et telefonintervju mister noen spesielle ting, for eksempel muligheten til å notere eller legge merke til kroppsspråket til objektet, er denne måten en veldig rask måte å hente kunnskap, særlig med tanke på når objektene er spredt over store deler av landet. Når det gjelder gyldighet og pålitelighet, dreier det seg om små miljøer der leder har god oversikt over kompetanseprofilen.

I tillegg til dette og i samarbeid med den samme engasjerte personen skal jeg benytte en enkel spørreundersøkelse. Formålet med denne spørreundersøkelsen er å kartlegge behovet for kompetanseøking innen informasjonssikkerhet gjennom kvantitative data. Dette gjør jeg i tillegg for å styrke påliteligheten av dataene. I en trianguleringsmetode ser man på dataene som er innsamlet og sammenligner dem med hverandre [Spørsmålene er gjengitt i Tillegg B]. Jeg skal også samle data via intervju, litteratur og mine egne erfaringer som er basert på min lange praksis i Helsetilsynet.

4.2 Forskningsspørsmål nummer 2

Hvilket behov har Helsetilsynet, særlig tilsynsførere, for kompetanseheving innen informasjonssikkerhet?
Her må jeg finne ut hva tilsynsførere har behov for å kunne og hva de kan. Jeg må se på forskjellen mellom det og avstanden mellom hva de kan og hva de burde kunne. Gapanalyse med hensyn på kunnskapsnivå om informasjonssikkerhet baserer seg på forskjellen mellom der du er nå og dit du ønsker å gå eller å være. Dette betyr at jeg må få etablert minimumskunnskapskravet innen informasjonssikkerhet til tilsynsførere i Helsetilsynet.

De metodene som kan tenkes for å få vite minimumskravet om kunnskapsnivå er:

- Ved å ta et intervju med en nøkkelperson dvs. en leder i Helsetilsynet og spørre hva denne tror tilsynsførere trenger av ekstra kunnskap. Denne måten egner seg fordi du fritt kan spørre om hva du vil. Begrensninger og rammer her er kanskje manglende kompetanse. Dette betyr at spørsmålene og måten du spør på, dvs. direkte eller indirekte spørsmål, i stor grad vil avgjøre hvilke data du får og hvor gode de er. Datatilgjengeligheten er enkel på denne måten.

- Å gå inn i lover og regler som Helsetilsynet forvalter eller se på oppdragsdokumentene til Helsetilsynet og deretter gjøre en vurdering av hva slags kunnskap tilsynsførere bør ha. Hvis det ikke ligger formelle krav til disse tilsynsførere, kan man lage en "eksamen i informasjonssikkerhet", teste tilsynsføreres kunnskap i dette feltet for å finne ut hva de kan og se på differansen.
- Selvvurdering av tilsynsføreres kunnskap er en metode for å finne ut hva de kan. Dette baseres på min erfaring i organisasjonen og kjennskap til en del av tilsynsføreres kunnskap. Datagyldighet eller troverdigheten av dataene er svært liten ved bruk av denne måten.

Konklusjon:
Metoden jeg vil brukfor for å finne ut hva de trenger av opplæring, er gapanalyse. Når jeg tenker gyldighet, så ville jeg si at gapanalyse er mer troverdig enn selvevaluering. Selv om en form for selvvurdering kanskje inngår i gapanalyse, blir i hvert fall analysen utført av meg.

4.3 Forskningsspørsmål nummer 3

Hva er hensiktsmessig risikoanalysemetode ved tilsyn med informasjonssikkerhet i helseforetak?
For å kunne besvare dette spørsmålet, må jeg ha besvart flere avledede forskningsspørsmål som:

1. Hva er status nå?
2. Hvilken metode brukes nå?
3. Hvor godt fungerer denne metoden?

Deretter må jeg for å finne en hensiktsmessig metode, klargjøre rammene for metoden dvs. å identifisere metodekravene. Her kommer flere avledende forskningsspørsmål som:

1. Hva er metodekravene for å føre tilsyn? Dette omfatter flere underspørsmål som:

1.1 Hva er nødvendig kunnskapsnivå/opplæring for å bruke metoden?

1.2 Hva er nødvendig tid for å bruke metoden dvs. hvor raskt kan metoden gjennomføres?

1.3 Hvor nøyaktighet må metoden være dvs. hvor mye feil kan tolereres?

Når metodekravene er identifisert, er tiden kommet for å se på aktuelle metoder. De metodene som tenkes for å besvare avledede forskningsspørsmålene kan være følgende:

- Intervju med nestleder i Helsetilsynet.
  En leder i virksomheten vet, basert på erfaringer, hvilken type kompetanse som trenges for å gjøre et tilsyn. Dette dreier seg om tilsynsføreres kompetansenivå, om de må ha høgskole eller universitets -utdanning i tillegg til relevant arbeidserfaring. I tillegg til dette vet en leder hvor raskt tilsynsbesøk kan gjennomføres dvs. hvor mye tid som er budsjettert for det, for eksempel 10, 20 eller 40 timers arbeid. Videre hvor mye og hva slags feil som kan avdekkes i et tilsyn. En leder vet også om det fungerer godt eller ikke med dagens metode. En fordel med dette er datatilgjengelighet, dvs. en rask gjennomføring av intervju og mye data, avhengig av hvilken type spørsmål

og på hvilken måte du spør. En ting som kan påvirke resultatet er hvor god kontakt lederen har med sine ansatte, og om lederen har full oversikt over hva som skjer på saksbehandlernivå.

- Helsetilsynets oppdragsdokument/ de mest relevante myndighetskrav
  Her kan man se på lovverket dvs. hva slags krav settes av loven når det gjelder metode, om loven setter noen rammer og begrensninger for metoden. Det som er vanskelig her er fortolkning og hvorvidt loven dekker de tingene som man lurer på.
- Litteraturstudium
  Dette gjøres ved å se på kravene til metoden ved å gå gjennom tidligere tilsynsrapporter, om det finnes noen svakheter, er det mulig de har oversett noe, har tilsynsrapporter preg av tilsynsførere, om de skjønner det de driver med eller om de har vært grundige nok. Det er en bra metode for å vurdere om ting er blitt riktig gjort. Denne metoden er tidskrevende når en må analysere flere tilsynsrapporter.
  Her er fordeler og rammebetingelse. Fordelene er at jeg har ferdig utførte tilsynsbesøk. Dataene er innsamlet fra forskjellige vinkler bl.a. dokumenter, intervjuer, møter..etc. Jeg skal studere dem og komme med en vurdering av metode og finne frem svakheter eller generelle konklusjoner om hva som kan forbedre arbeidet. Begrensningen her er at dette er resurskrevende.
- Spørreundersøkelse som sendes til alle Helsetilsynet i fylkene
  Formålet med undersøkelsen er å få vite hvor store utfordringer organisasjonen er utsatt for i tilsynsarbeidet med informasjonssikkerhet. Dette betyr hvor godt fungerer dagens risikoanalysemetodikk hvis de har det pr. i dag. Dette er en enkel framgangsmåte, men datatilgjengelighet er et problem fordi at du muligens ikke får nok svar for danne et riktig bilde av virkeligheten.
- Nedskrivning av min egen vurdering basert på mine erfaringer og kunnskap fra mitt arbeid innen IT i Helsetilsynet i mer enn 13 år. Jeg kan bruke meg selv som en kilde for data. Begrensningene her går på pålitelighet og gyldighet.

Konklusjon:
De metodene som er mest hensiktsmessige er flere. De jeg har tenkt å bruke er følgende:

- Jeg vil ta et intervju med Helsetilsynets ledelse (assisterende helsedirektør) og vil benytte intervjuet til å få et bilde av dagens metodebruk og kunnskap om metodekravene [Spørsmålene er gjengitt i Tillegg G].
- Spørreundersøkelsen som nevnt ovenfor i forskningsspørsmål 1, for å få et bilde av dagens utfordringer med hensyn på evt. valg av ny risikoanalysemetodikk [Spørsmålene er gjengitt i Tillegg B].
- Nedskrivning av min egen erfaring, min egen innsikt og dokumentasjon av egen arbeidserfaring. For eksempel på svar om det brukes noe risikoanalysemetodikk pr. i dag.
- Helsetilsynets skriftlige materiale for å finne ut bl.a. hvor godt dagens metode fungerer.

Opptak

I de fleste bøker som omhandler kvalitativ metode beskrives ulike hjelpemiddel som forskeren kan benytte seg av under et intervju. En kan enten notere det som blir sagt, eller en kan spille inn intervjuene ved hjelp av ulike typer av innspillingsmedia. På denne måten trenger en ikke å fordele oppmerksomheten på flere ting, det vil si, stille spørsmål, registrere det som blir sagt, samt, notere svarene. Det er ofte lett å bli distrahert under slike forhold, og intervjuene blir oppstykket og mister dynamikk. Ved opptak kan også intervjuene gjengis i stor detalj, i motsetning til dersom en støtter seg bare på notater [[43] side 123-124]. I situasjoner der opptak brukes kan intervjuet påvirkes i den grad at informantene blir oppmerksom på at samtalen blir innspilt, og dermed endrer oppførsel deretter, ettersom en da blir påminnet om at intervjuet ikke er en uformell samtale. Opptak medfører også et etisk ansvar, dette kommer an på forskningens innhold [[30] side 209]. I dette prosjektet skal jeg ta lydopptak, gjort med informantenes samtykke, på alle mine intervjuer.

Transkribering

Alle intervjuer skal transkriberes i etterkant. Transkriberingsprosessen er svært tidkrevende. Likevel er transkribering essensielt, fordi det er en prosess som gir deg kjennskap til datamaterialet. Ved å høre igjennom materialet kan en velge ut hvilke intervju som er relevant, og hvilke intervju som ikke er relevant. Et intervju inneholder så mye data at det vil være svært vanskelig å analysere dem dersom de ikke har blitt konvertert til en tekst [[28] side 73]. Intervjuene som ble foretatt var på ca. en times varighet. I samtaler som strekker seg over et slikt tidsrom blir det sagt mange ting. Det var derfor fordelaktig å anvende opptak. I etterkant ble det skapt manuskript av intervjuene med den hensikt at de skulle brukes som en basis for videre analyse.

5 Datainnsamling

I dette kapitlet vil jeg forklare de metodene som er brukt for datainnsamling. Først vil jeg forklare litt om metoden, deretter vil jeg si noe om dataene som ble samlet og til slutt vil jeg diskutere gyldighet og pålitelighet av dataene.
Hovedsakelig besto datainnsamlingsmetodene av fire måter:

1. Spørreundersøkelse: Sendt alle Helsetilsynet i fylkene.
2. Intervju: som deles i to typer: telefonrundespørring og tilstedeintervju.
3. Litteraturstudie: fra både Statens helsetilsyn og Datatilsynet.
4. Jeg som en ansatt i Statens helsetilsyn i mer enn 13 år, brukte mine relaterte erfaringer for å evaluere data til alle forskningsspørsmålene.

Når det gjelder spørreundersøkelsen, er den sendt til alle Helsetilsynet i fylkene (18 kontorer) for å samle inn data til forskningsspørsmålene 1 og 3.

Når det gjelder telefonrundespørring (telefonintervju), var det min overordnete sjef "assisterende helsedirektør" som ringte en del utvalgte kontorer og stilte spørsmål [Spørsmålene og resultatene gjengitt i Tillegg E].

Når det gjelder "tilstedeintervju", har jeg tatt tre intervjuer [Tillegg C] og formålet med disse intervjuene var å samle inn data. Jeg tok intervjuer med følgende personer:

1. Med en erfaren tilsynsrådgiver i Datatilsynet som har ledet en rekke av kontrollene, for å samle inn data til alle forskningsspørsmålene. [Spørsmålene gjengitt i Tillegg D].
2. Med en leder i Helsetilsynet, assisterende helsedirektør, for å samle inn data til alle forskningsspørsmålene [Spørsmålene gjengitt i Tillegg G].
3. Med en tilsynsrådgiver i Finanstilsynet for å samle inn data om måten de har løst sine oppgaver innen dette feltet. Dette vil jeg fortelle mer om under "Relatert arbeid" på slutten av dette kapitlet [Spørsmålene gjengitt i Tillegg F].

Litteraturstudiene ble brukt for å samle inn data til alle forskningsspørsmålene.

5.1 Spørreundersøkelse

Jeg har lagd et enkelt spørreskjema. Formålet med denne spørreundersøkelsen var å kartlegge behovet for kompetanseøking innen informasjonssikkerhet og for å få vite i hvor stor grad organisasjonen er utsatt for utfordringer i tilsynsarbeidet med informasjonssikkerhet. Skjemaet inneholdte 20 spørsmål hvor alle var relatert til informasjonssikkerhet. Jeg la også inn et åpent felt hvor det var mulig å legge til noen linjer med informasjon om respondenten mente det var relevant.
Spørreundersøkelsen ble sendt sammen med et brev som et vedlegg pr. e-post til alle

Helsetilsynet i fylkene [1] [Et eksemplar av skjemaet og brev gjengitt i Tillegg B].
Skjemaet var delt inn i to deler og alle svarfeltene var i form av avkrysningsbokser for å gjøre besvarelsen lettere:
Del 1 gjaldt *organisasjonens utfordringer i tilsynsarbeidet*. Denne delen inneholdt 10 spørsmål knyttet til hvor ofte saker der man må ta en vurdering, forekommer i tilsynsarbeid. Det var tre svaralternativer: Aldri vært aktuelt, Sjelden (ca. årlig) og Hyppig (> månedlig).

Del 2 av skjemaet gjaldt *organisasjonens kompetanse og opplevelse av behov for kompetanseøkning* dvs. hvordan Helsetilsynet i fylket opplever sin egen kompetanse når det gjelder tilsynsmessig vurdering. Besvarelsesalternativene bestod av tre kolonner som hetet (Ingen kompetanse), (Bør bli bedre) og (Tilfredsstillende kompetanse).

Etter svarfristens utløp, hadde jeg fått kun 8 svar av 18 utsendte. Jeg måtte sende en påminnelse pr. e-post og forlenge svarfristen i to uker til. Til slutt fikk jeg svar fra 10 kontorer.

Når det gjelder gyldighet og pålitelighet av dataene, kan jeg ikke vite hvem som fylte ut skjemaene, men jeg antar at det ble fylt ut av fylkeslegen som er den øverste lederen i Helsetilsynet i fylket. Kun ett av fylkeslegekontorene ga tilbakemelding om at de ville diskutere dette på avdelingsmøte. Om fylkeslegen har full oversikt over sine ansatte og ansattens kompetanse på dette bestemte området, er det vanskelig å si noe om, selv om det er snakk om små arbeidsmiljø ved disse kontorene. Noe som kan påvirke pålideligheten er for eksempel at de ikke fyller ut hundre prosent riktig fordi de tenker at konsekvensene blir at det avslører at det sitter ukompetente folk der. For å styrke pålideligheten av dataene, bestemte jeg å samle samme type data med fokus på kompetanse hos tilsynsførere via en telefonrunde til fylkeslegene. Dette vil jeg si mer om under "Telefonintervju" senere i dette kapitlet.

5.2 Telefonintervju

Når det gjelder intervju, gjorde jeg dette på to måter. Telefonintervjuene ble foretatt av assisterende helsedirektør, mens tilstedeintervjuene foretok jeg selv. I begge måtene ble intervjuobjektene informert og ga forhåndsamtykke. Nedenfor vil jeg forklare nærmere måten intervjuene ble tatt på, hvilke data som ble samlet inn, og diskutere gyldighet og pålitelighet av dataene.

Som nevnt ovenfor, har jeg involvert en tredje part til å gjennomføre telefonintervjuene. Dette inngår i del av trianguleringsmetoden som jeg snakket om i metodekapitlet. Her er min ledelse i Helsetilsynet involvert ved å ta en telefonrundspørring. Formålet med denne måten var å få bekreftet eller avkreftet dataene som jeg fikk fra spørreundersøkelsen som nevnt ovenfor. Det ble foretatt en rundspørring til et utvalg av kontorer. Dette skjedde i perioden 15.04.2010 til 20.04.2010 da assisterende helsedirektør ringte fem av de største Helsetilsynet i fylkene og et mindre embete. I telefonintervjuene ble det innledningsvis kort forklart at dette gjelder å få en oversikt over kompetanse innenfor informasjonssikkerhet hos tilsynsførere hos Helsetilsynet i fylket [Spørsmålene gjengitt i Tillegg E].

[1] Sendt til e-postadressen til fylkeslegen sammen med vedlagt brev den 22.02.2010

Etter innledningen ble det spurt om antall personer (ikke årsverk) som er involvert i planlagt tilsyn (systemrevisjoner) med helsetjenestene, og svaret var totalt 70 personer. På svar på spørsmål 2, hvor mange av disse som har gjennomgått opplæring innenfor informasjonssikkerhet, ser vi at ingen av dem hadde gjennomgått opplæring innenfor informasjonssikkerhet (kurs, seminarer, studier eller lignende).
På svar på spørsmål 3, om ansatte ved kontoret får annen opplæring eller bevisstgjøring innenfor informasjonssikkerhet (ut over det som er nødvendig for ivaretakelsen av interne rutiner og systemer (Arkivsystemet ePhorte, taushetsplikt etter forvaltningsloven), var det ingen som hadde det, bortsett fra to av kontorene som hadde ansatte som deltok på fellestilsyn med Datatilsynet og lærte mye av det. På et av kontorene hadde de hatt tilsyn fra Datatilsynet på egne systemer og lærte mye av det.

Når det gjelder gyldighet og pålitelighet av dataene innsamlet på denne måten, er det to punkter her man bør konsentrere seg om. Det første er når en underordnede leder svarer på spørsmålene fra overordnet leder, er han/hun på en eller annen måte under en form for psykiske press. Her er sjef-ansatte forhold inn i bildet og en ansatt vil i liten grad ønsker å innrømme at han/hun har gjort en dårlig jobb og det kan mulig være en feilkilde. Det andre punktet er at hvor stor oversikt en leder har over sine ansatte og deres kompetanser, men her dreier det seg om små miljøer der leder har god oversikt over kompetanseprofilen.
Når jeg ser på svarene som jeg har fått på denne måten og sammenligne dem med det som jeg har fått fra spørreundersøkelsen, har jeg grunn til å tro på dem, fordi i begge tilfellene viser det seg at kunnskapsnivået er veldig lavt.

5.3 Tilstedeintervju

Intervjuet i Datatilsynet og i Finanstilsynet tok ca. en times tid for hver. I begynnelsen av intervjuene presentert jeg meg, min bakgrunn, min masteroppgave og formålet med den. Deretter ba jeg intervjuobjektene om å presentere seg, sin stilling i organisasjonen, arbeidsoppgaver og sin erfaring i feltet. Intervjuet i Helsetilsynet tok halvannen time.

5.3.1 Kunnskap om informasjonssikkerhet hos tilsynsførere

Når det gjelder kunnskapsnivået i informasjonssikkerhet hos tilsynsførere og hva de trenger av ekstra kunnskap, fikk jeg opplyst fra ledelsen i Helsetilsynet at:

1. Tilsynsførere skal kjenne til hva som er en god standard i en risikoanalyse, hva som er en god risikoanalyse av sikkerhet i et IT-system. De skal ikke nødvendigvis kunne gjøre den selv fordi dette blir for mye og for omfattende for tilsynsførere, men de skal få vite hva som er karakteristisk for en god risikoanalyse. Kanskje de skal kjenne allmennt brukte standarder for gjennomføring av risikoanalyse, slik at de kan si om en risikoanalysen er gjennomført i forhold til denne standarden og er akseptabel.
2. De skal og vite noe om de teknologiske mulighetene til å sperre tilgang, for retting og endring i journalsystem, for kommunikasjon inn og ut av et teknisk eller elektronisk informasjonssystem, de skal vite om hvordan ulike elektroniske pasientjournalsystem for eksempel kan sperres slik at deler av en pasientjournal blir gjort utilgjengelig.

> Helsetilsynet har for eksempel sett saker der folk har sagt at de ikke kan sperre, fordi har du tilgang til noe, så har du tilgang til alt. Det stemmer ikke, fordi i EPJ-systemene kan man gradere tilgang etter ulike behov. Mange tilsynsførerne vet ikke at det faktisk går an å sperre bruk av usb-porter, om kryptering av lagringsmedium og hva som er mulig å verne med kryptering, hva som er mulighetene når det gjelder å verne data i en database. Tilsynsførere må føler seg trygge på den kunnskapen de har slik at de skal kunne stille noe nysgjerrige spørsmål som gjør dem i stand til å gå litt dypere på de påstandene som de møter.

Standarder for risikoanalyse og teknologimuligheter for tilgangskontroll er to sånne ting som en rent konkrete kunne ønske at tilsynsførere visste mer om. Dette betyr at en del helt basale ting ønsker Helsetilsynet at dets tilsynsførere kan få vite mer om.

5.3.2 Dagens metode og tilsynsmetodekrav

Ut i fra mine erfaringer har Helsetilsynet ikke noen metoder for å føre tilsyn med informasjonssikkerhet pr. i dag. Dette er også bekreftet av ledelsen i Helsetilsynet.
For å kunne finne en hensiktsmessig metode for Helsetilsynet, må vi vite tilsynsmetodekravene. Dette gjelder kravene til en tilsynsfører, tiden som trenges for å føre tilsyn og hvor nøyaktig en tilsynsmetode må være.

Gjennom intervjuet med nestleder i Statens helsetilsyn fikk jeg opplyst følgende:
Om krav til en tilsynsfører, mener ledelsen i Helsetilsynet at en tilsynsfører vanligvis skal ha høyskole eller universitetsutdanning innenfor relevant fagfelt, for eksempel helse og sosialfag eller jus. I tillegg til utdanningen kommer kravet om yrkeserfaring, for eksempel ved at man må ha jobbet i helsetjeneste eller sosialtjeneste, eller jobbet med forvaltningssaker, slik at man vet hvordan dette foregår i praksis. Deretter kommer kravet om deltakelse i et ukes innføringskurs i systemrevisjon og revisjonsteknikk før man deltar som ordinær revisor ved tilsyn. Pr. i dag inneholder ikke dette kurset noe om informasjonssikkerhet, men det skal settes opp et heldags kurs for dette i fremtiden.
Videre tilføyer ledelsen at fram til nå er det ikke blitt stilt krav om spesielle kvalifikasjoner innenfor informasjonssikkerhet. Noe av den kunnskapen som tilsynsførerne trenger for å vurdere informasjonssikkerhet er sammenfallende med den kunnskapen de vanligvis har når det gjelder taushetsplikt og vern av informasjon om helsemessige og andre personlige forhold. Han sier "*Men kunnskap som handler om hvordan informasjonssystemer er bygget opp og fungerer har fram til nå ikke hatt spesiell oppmerksomhet ved rekruttering og opplæring av tilsynsførere i Statens helsetilsyn*" .

Når det gjelder *tid som trenges* for en godt planlagt og gjennomført systemrevisjon, tror Helsetilsynet at det trenger minst to personer til å dra ut og de bruker 2-3 dagers arbeid. Dette betyr at det går minst 40 timer på det. Av denne tiden kan det settes en hel dag for å føre tilsyn med informasjonssikkerhet.

Om et tilsyn avdekker feil eller hvor nøyaktig tilsynets metode bør være dvs. hvor mye feil kan tillates, er viktig. Ledelsen mener at en feil som gir grunnlag for avvik ikke kan tillates. Dette betyr at det må være null feil på de områdene som kan føre til lovbrudd.

5.3.3 Samarbeid mellom Helsetilsynet og Datatilsynet

Datatilsynet fører tilsyn med personvern bl.a. innen helse- og omsorgssektoren. I og med at informasjonssikkerhet er en sentral del av personvernet, kan man ikke se bort fra behovet for samarbeid mellom Helsetilsynet og Datatilsynet. I tillegg til dette, fikk flere av tilsynsførerne på fylkesnivå god kunnskap og bevisstgjøring om informasjonssikkerhet da de samkjørte tilsyn med Datatilsynet.

Helsetilsynet og Datatilsynet har størst behov for å være synkronisert når det gjelder tilgangsstyring, spesielt §13 [Gjengitt i tillegg A.1]. Her møter taushetspliktbestemmelsen sikkerhetsbestemmelsene, og helselovgivningen og Helsetilsynet setter rammene for hva som er godt nok, og i hvilken grad taushetsplikten ikke er overholdt i forhold til tilgangsstyring. Begge tilsynsorganene trenger tverrfaglig kompetanse knyttet til både behov for tilgjelighet og taushetsplikten på den helsefaglige side, hva som er god nok sikring av konfidensialitet på sikkerhetssiden.

Helsetilsynet og Datatilsynet gjennomførte i mai 2006 i fellesskap tilsyn med hvordan Helse Bergen HF Haukeland universitetssykehus ivaretok taushetsplikten og tilgjengeligheten ved bruk av pasientjournalsystemet Doculive og det pasientadministrative systemet PIMS. Tilsynet omfattet både innhenting og utlevering av pasientinformasjon fra elektronisk pasientjournal og tilgangsstyring i forhold til elektronisk pasientjournal og det pasientadministrative systemet PIMS [18].

I juni 2006 gjennomførte Helsetilsynet og Datatilsynet et lignende tilsyn ved Akershus Universitetssykehus HF. Temaet ved dette tilsynet var sikring av taushetsplikten og tilgjengeligheten til opplysninger ved bruk av det elektroniske pasientjournalsystemet DIPS [[18]].
Disse tilsynene fungerte på en vellykket måte, men det ble ikke flere lignende fellestilsyn.

Gjennom mine intervjuer med både Helsetilsynet og Datatilsynet, kommer det fram at samtaleklima både på ledernivå og på tilsynsførersnivå mellom dem er veldig bra og de betrakter hverandre som organisasjoner som lett kan snakke med hverandre. Det har vært veldig god kontakt mellom tilsynsførere fra Datatilsynet og fra Helsetilsynet. Tilsynsføre har jobbet godt sammen i de tilsynene som var samkjørte. De føler at de snakker samme juridisk språk når de møter hverandre. Det som har gjort at de ikke har fulgt opp videre er at bl.a. sykehusene og dels også Helse- og omsorgsdepartementet mente Helsetilsynet var for streng i fortolkningene av gjeldende regelverk.
Både Helsetilsynet og Datatilsynet har felles forståelse av at de har lyst til å jobbe sammen med hverandre. De har felles forståelse av hva regleverket krever og hva regleverket burde kreve.

De avvikene som de fant i Bergen og på A-hus er ganske like med de man antar å kunne finne mange andre plasser i landet. Helsetilsynet har derfor ikke funnet grunnlag for å gjennomføre ytterligere felles tilsyn på dette feltet før regelverket er revidert slik at unødige hindre er ryddet bort.

5.3.4 Gyldighet og pålitelighet av dataene ved denne metoden

Når det gjelder intervju med en leder, kommer spørsmål om hvor stor gyldighet/pålitelighet dataene har som kommer fra slike intervjuer. Dette har tre siders: hvor den ene er at det ikke er lett for en leder å innrømme at de sitter med titals tilsynsførere som har dårlig kompetanse i et viktig område "informasjonssikkerhet". Dett vil kunne skape en type tvil hos tjenestemottakere. Den andre dreier seg om et ønske om forbedring på dette området, og derfor vil en leder være opptatt av å gi riktige opplysninger. Det tredje er om lederen har god nok kontakt med saksbehandlere dvs. om en leder hvet hva slags diskusjon som foregår på saksbehandlernivå.

5.4 Skriftlige kilder

Jeg har gått gjennom mye skriftlige kilder fra både Helsetilsynet og Datatilsynet. Jeg valgte Datatilsynet også fordi de gjør tilsyn med Personvern i helse- og omsorgssektoren. I og med at informasjonssikkerhet er en sentral del av personvernet, kan man ikke utelate å se på forholdet mellom Helsetilsynet og Datatilsynet.

5.4.1 Helsetilsynet

Jeg har gått gjennom listen over gjennomførte systemrevisjoner fra de tre siste årene (2007-2009). Rapportene fra alle systemrevisjoner publiseres på internett [2] . Ingen av rapportene har et særlig fokus på informasjonssikkerhet. Jeg har videre gått grundigere gjennom mer enn 15 tilfeldige valgte tilsynsrapporter (systemrevisjoner) for Helsetilsynet i disse årene for å se om informasjonssikkerhet er tatt med blant andre temaer. Ved denne gjennomlesingen har jeg funnet at de ikke inneholder spesielle spor av vurdering av informasjonssikkerhet.

I rapportene er det mye snakk om forsvarlighet og taushetsplikt. Dette er selvsagt temaer som til en viss grad kan innbefatte informasjonssikkerhet. Men for eksempel taushetsplikt blir ikke knyttet opp til en bredere vurdering av rutinene for informasjonssikkerhet i virksomheten. Likeledes inneholder vurderingen av forsvarlighet ikke elementer av informasjonssikkerhet. Helsetilsynets rapporter legger stor vekt på ledelsens ansvar for å ha gode systemer for forsvarlig drift og opprettholdelse av taushetsplikt, men likevel er det vanskelig å få øye på ledelsesforankringen av informasjonssikkerhetsansvaret.

Jeg mener derfor å kunne slå fast at informasjonssikkerhet i perioden 2007-2009 ikke har hatt en selvstendig plass som vurderingstema i Helsetilsynets systemrevisjoner.

5.4.2 Datatilsynet

Gjennom intervjuet med Datatilsynet [Spørsmålene gjengitt i Tillegg D] og skriftlig tilgjengelig materialer [17] har jeg fastslått at Datatilsynet har følgende funn innen helse- og omsorgssektoren:

[2] På Helsetilsynets hjemmeside: http://www.helsetilsynet.no

- *Sviktende tilgangsstyring* har vært avdekket ved samtlige tilsyn med dette som tema ble foretatt i perioden 2005 - 2008. Kontrollvirksomheten har avdekket at helseforetakene ikke sikrer at taushetsbelagte personopplysninger i de elektroniske pasientjournalsystemene er forsvarlig vernet mot innsyn fra ansatte som ikke har tjenstlig behov for opplysningene.
- *Tilsyn har avdekket at muligheten for å avdekke snoking er utilfredsstillende*. Det store antallet oppslag, små kontrollressurser og svake kontrollrutiner gjør at ansatte ved kliniske avdelinger som kikker i pasientjournaler uten å ha tjenestelige behov, har meget lav risiko for å bli avslørt. Loggkontroll, slik det fremstår i dag, er derfor vurdert av tilsynsmyndighetene til å være et lite effektivt hjelpemiddel til å avdekke misbruk.
- *Mangelen på grundige risikovurderinger* ved innføring av nye systemer har vist seg å være en gjennomgående svakhet avdekket i tilsyn hos helseforetakene. Denne mangelen gjør at helseforetakene ikke får oversikt over egne systemers sårbarhet, og hvor stor risiko det er for ulike typer svikt. De går dermed glipp av muligheten for å iverksette tiltrekkelige og målrettede forebyggende tiltak. Mangelen på systematiske risikovurderinger i forhold til sikring av konfidensialitet og tilgjengelighet til elektroniske pasientjournaler har vært avdekket ved flere tilsyn foretatt i perioden 2005 - 2008, blant annet ved St. Olavs Hospital HF, Akershus Universitetssykehus HF og Sykehuset i Vestfold HF.
- *Risiko for konfidensialitet- og integritetsbrudd*: Manglende tilgangsstyringen ble vurdert slik at den ikke ga tilfredsstillende konfidensialitetssikring etter Helseregisterloven. En verifikasjon viste for eks. at det var mulig å bytte identitet ved skriving i journalen. Dette innebar at en kunne utgi seg for å være en annen ansatt når en skrev i journalen.
- *Tilgang til person- og helseopplysninger*: Dette omfatter tilgang med hensyn til populasjon, tilgang med hensyn til opplysningsmengde om enkeltperson, tilgang med hensyn til tid og tilgang til IPLOS-informasjon [3].
- *Usikker forsendelse av helseopplysninger*: Under verifikasjonen fremkom det at personopplysninger mellom ulike avdelinger i kommunen ble sendt i identifiserbar form på usikret telefaks.
- *Virksomhetens bruk av logger*: kommunen hadde iverksatt logging - herunder logging av oppslag. Rutiner for gjennomgang av loggene var ikke etablert. De enkelte oppslag som den ansatte gjorde, ble ikke logget. Det var følgelig ikke etablert rutiner for gjennomgang av logger.

Datatilsynets kontroller har vist at både helsepersonell og andre ansatte i helsesektoren gjennomgående har alt for vid tilgang til å tilegne seg pasientopplysninger i den elektroniske journalen. Samtidig er virksomhetens kontroll med hvilke opplysninger den enkelte ansatte faktisk tilegner seg, alt for svak.

[3] IPLOS er et nasjonalt helseregister men med tilsvarende lokale data i de lokale fagsystemene. Det omtale her tilgang til lokale data

5.5 Relatert arbeid

Risikoanalysemetoden brukes i Norge i forbindelse med IT-tilsyn bl.a. i Finanstilsynet. Siden Finanstilsynets virksomhet er relevant og beslektet, har jeg valgt å fokusere på det. Dette kapitlet er basert på et intervju med en tilsynsrådgiver i Finanstilsynet. Formålet med dette intervjuet var å bli kjent med hvordan de har løst sine oppgaver innen dette området [Spørsmålene er gjengitt i Tillegg F].

5.5.1 Finanstilsynets opplegg om IT-tilsyn

Intervjuobjektet har vært med på etableringen av tilsynsopplegget som nå benyttets når de fører tilsyn. Dett går tilbake til 2002 da de først måtte lage en IKT-forskrift for Finanstilsynets tilsynsområder. Det er en forskrift som bestemmer det regimet som finansforetak må implementere for å drive IT-virksomhet. De bruker COBIT, ITIL, ISO og CMMI i sitt arbeid. De tok utgangspunktet i COBIT og ITIL da de begynte å skrive forskriften paragraf for paragraf. Innen de 15 paragrafene som forskriften består av, finner man alle de 34 prosessene som COBIT har. For eksempel ligger det fire til fem prosesser under §2 i forskriften. Til slutt sjekket de alle paragrafene og det viste seg at forskriften dekket alle de 34 prosessene. I tillegg tok de ITIL som er et tilsvarende rammeverk som går mer på operasjon og drift av IT-systemer. I forskriften har de sjekket at det er samsvar både med COBIT og ITIL.

Gjennom intervjuet fikk jeg opplyst at før forskriften ble godkjent i 2003, lagde de spørreskjema som begynte med prosessnummer 1. Tilsynet har 11-12 skjema som de ber virksomheten som er utsatt for tilsyn om å fylle ut. Hvis det er første gang, bruker de det store skjemaet med 34 prosesser, ca. 180 spørsmål. Finanstilsynet sender ut spørreskjema til foretaket en måned på forhånd. I COBIT er det kontrollpunkter som veileder deg til å stille de riktige spørsmålene. I prosessnummer 1 er det IT-strategi som er den primære prosessen for å bestemme det videre løpet, fordi den forteller hvor god du er. Ved å bruke COBIT finner de ut om de har ting på plass og ved å bruke ITIL finner de ut kvaliteten mer detaljert, samtidig som de har IKT-forskriften i bakhånd. Gjennom dette opplegget er informasjonssikkerhet veldig godt ivaretatt.

Når det gjelder tilsynsprosess, fikk jeg opplyst at det velges først tilsysobjektet dvs. foretaket som skal utsettes for tilsyn. Deretter sender Finanstilsynet et skriftlig varsel til foretaket hvor de ber om spesifisert dokumentasjon av IT-virksomheten. I tillegg blir foretaket bedt om å fylle ut egenevalueringsskjema med ca 180 kontrollspørsmål med ja/nei-svar. Dette skjemaet er basert på COBIT. Egenevalueringsskjemaet har kontrollspørsmål knyttet til hver prosess i de 34 prosessene i COBIT. Når Finanstilsynet mottar dokumentasjonen og det utfylte egenevalueringsskjemaet, blir dette gjennomgått som en del av tilsynsforarbeidet.

Det finnes også en forenklet versjon av egenevalueringsskjemaet som dekker 12 av de 34 COBIT-prosessene med ca 75 kontrollspørsmål. Som ledd i ordinære tilsyn med finansforetak gjennomført av andre seksjoner i Finanstilsynet, blir foretaket bedt om å svare på det forenklede egenevalueringsskjemaet om foretakets IT-virksomhet. IT-tilsynsgruppen får de ferdig utfylte skjemaene til vurdering og kan gi tilbakemeldinger til fagavdelin-

gene som tar dette med i sin rapport. Dette kalles forenklet IT-tilsyn. IT-tilsynsgruppen analyserer informasjonen fra de forenklede egenevalueringsskjemaene før det blir vurdert om det skal gjøres et IT-tilsyn med den aktuelle bedriften førstkommende år.

I egenevalueringsskjemaet skal virksomheter svare på spørsmålene knyttet til hver COBIT-prosess, og hver prosess skal ROS-analyseres så virksomheten kan svare på om sårbarheten i den utvalgte prosessen. Alle kontrollspørsmål som er besvart med nei er i utgangspunktet å anse for avvik, og betyr ofte at bedriften må iverksette forbedringstiltak.

Alle svarene registreres i en database og analyseres ved hjelp av verktøyet ISAP. Selv om dette gir kvantitative mål på resultatet av egenevalueringen, diskuterer IT-tilsynet nytten av denne informasjonen. Ofte viser det seg (gjennom det stedlige tilsynsmøtet) at det foretaket svarer på egenevalueringsskjemaet, fremstår med annen sikkerhet enn det som virkelig gjelder. Årsaken til denne uoverensstemmelsen kan være misforståelser og ulik oppfatning av hvordan spørsmålene skal tolkes. Egenevalueringsskjemaet er uansett viktig, fordi det krever svar fra foretaket på alle deler av IKT-virksomheten, og det er utgangspunkt for diskusjon om temaene på tilsynsmøtet.

Intervjueobjektet fortalte om outsourcing og kvalitetssikring av risikoanalyse: "*Vi ser også på infrastruktur og topologi. Vanligvis ber vi om å få en oversikt over systemarkitektur. Vi har våre egne vurderinger om dette er bra, eller ikke bra nok. Hvis organisasjonen bruker outsourcing, fører vi tilsyn der IT-systemet er. Det betyr ingenting om de fører det selv eller andre steder*".
"*Vi spør om virksomheten har risikoanalyse, hvis svaret er ja så går vi til neste skjema som kvalitetssikrer operasjonen, som i dette tilfellet er risikoanalysen*" .

Når det gjelder samarbeid mellom Finanstilsynet og Datatilsynet, fungerer dette utmerket fordi rollene er veldig klare. Intervjuobjektet fortalte at "*Datatilsynet har det med Personvern å gjøre, men vi har alt. Innenfor en banks datasystem kanskje personvernbiten kan være konsentrert om en database som har alle kundeopplysninger. Mens alt de andre som har med det å drive bank å gjøre, er vårt ansvar. Datatilsynet har en liten, men viktig, del av jobben, men vi har resten*" .

5.5.2 Finanstilsynets erfaringer med COBIT

Finanstilsynets erfaring med COBIT er bare positiv og de betrakter dette rammeverket som en grunnmur for å være sikkert på at alle prosessene er på plass. Intervjueobjektet fortalte følgende om modulen deres:
"*Vi satte COBIT på plass som et grunnlag, så tok vi ITIL som har god kvalitet opp i COBIT og på tredje nivå kom ISO 27002. Denne modellen tilfredsstiller kravene som ISO setter.*
COBIT er brukerdrevet av veldig mange foretak. For eksempel kan jeg være med i en programgruppe eller utviklingsgruppe innefor COBIT og utvikle nye ting. Så det er brukerdrevet og det er ikke noen som eier det på en måte. Derfor er det god utvilkling og det gode for oss er at vi slipper å endre forskriften når det kommer ny teknologi som for eks."cloud computing"

[4]. *Vi behøver ikke å forholde oss til alt det. Det blir håndtert gjennom bruken av COBIT, ITIL og ISO. Hvis du har veldig god virusbeskyttelse, men change kontrollbiten av den er dårlig, da hjelper det veldig lite*" .

Denne modulen som Finanstilsynet har, passer ikke bare for finans, den kan også passe for helse, industri og andre områder.

[4]Cloud computing: http://no.wikipedia.org/wiki/Nettskyen

6 Dataanalyse og diskusjon

I dette kapitlet vil jeg analysere dataene som ble samlet inn. Jeg skal ordne dem i forhold til forskningsspørsmålene og vil oppsummerer de viktigste funnene. Jeg vil skrive noe om behovet for tiltak for å komme videre med de utfordringene disse funnene avdekker. I og med at dette er en forvaltningsoppgave, vil jeg skrive noe om økonomiske og administrative konsekvenser av disse funnene. Jeg vil i tillegg også foreslå noe tiltak for å håndtere de utfordringene som jeg syns er viktige for fremtidig arbeid for Helsetilsynet. På slutten av dette kapitlet vil jeg ta en diskusjon.

6.1 Forskningsspørsmål nr. 1

Hvilken kompetanse i informasjonssikkerhet har Helsetilsynet som grunnlag for å utføre tilsyn?

Før jeg tar en stilling til dette spørsmålet, må jeg ha kjennskap til kravene til helseforetakene med hensyn på informasjonssikkerhet. I Helseregisterloven er kravene tydelig definert. §13 som lyder slik [Gjengitt i Tillegg A.1]:
"*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. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt."

Videre i samme lov, §13 a som lyder slik:
"*Forbud mot urettmessig tilegnelse av helseopplysninger*
Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift"

I §16 legges vekt på sikring av konfidensialitet, integritet, kvalitet og tilgjengelighet:
"*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*".

Personopplysningsloven utgjør den viktigste rettskilden innen personvern. Loven stiller noen grunnkrav til all behandling av personopplysninger. Hele kapittel 2 i Forskrift om behandling av personopplysninger gjelder informasjonssikkerhet [Gjengitt i tillegg A.2].

Hvilke informasjonssikkerhetstiltak må helseforetakene gjennomføre for å tilfredsstille disse kravene? Jeg kan ikke svare på dette spørsmålet før vi bli kjent med tiltakene

som må gjennomføres for at kravene skal tilfredstilles. Og for å kunne avgjøre om disse tiltakene er gjennomført, må vi vite hvilken kompetanse man må ha for å kontrollere det. For å få vite om tilsynsførere har den kunnskapen, måtte vi teste og kartlegge kunnskapen deres.

Når jeg ser på dataene som ble innsamlet i forrige kapittel [Tillegg E], kan jeg ikke se at tilsynsførere har den nødvendige kompetansen for å kontrollere at tiltakene er gjennomført eller ikke. Vi har sett at av 70 tilsynsførere som er involvert i tilsynsarbeid, hadde ingen av dem gjennomgått opplæring innenfor informasjonssikkerhet. Det var ingen som hadde fått annen opplæring eller bevisstgjøring innenfor informasjonssikkerhet, bortsett fra to av kontorene hvor noen av de ansatte hadde deltatt på fellestilsyn med Datatilsynet og lærte mye av det.

Når det gjelder data fra spørreundersøkelsen, er det litt forskjell mellom dem og fra telefonrundspørringen, men stort sett peker de i samme retning. Tallene fra spørreundersøkelsen viser at 50% av deltakerne svarte at det aldri hadde vært aktuelt med opplæring av ansatte i informasjonssikkerhet i organisasjonen. På spørsmål om opplæring av ansatte i informasjonssikkerhet med svaralternativene (Ingen kompetanse, Bør bli bedre, Tilfredsstillende kompetanse), svarte 60% av deltakere at opplæringen bør bli bedre, 20% besvarte ingen kompetanse mens 20% besvarte tilfredsstillende kompetanse.

Ut fra funnene som ble gjort ved spørreskjemaundersøkelsen og telefonrundspørring om tilgjengelig kompetanse innenfor informasjonssikkerhet, og det opplevde behovet for slik hos Helsetilsynet i fylket, er det grunn til å anta at denne er svært lav. Dette betyr at kunnskapsnivået i dette feltet pr. i dag er veldig lavt.

6.2 Forskningsspørsmål nr. 2

Hvilket behov har Helsetilsynet, særlig tilsynsførere, for kompetanseheving innen informasjonssikkerhet?

Det er viktig at tilsynsførere i Statens helsetilsyn eller hos Helsetilsynet i fylket har nok kjennskap til informasjonssikkerhet. Hovedgrunnen til dette er at veldig mye av tilsynet handler om å avdekke mulig svikt i forhold til pasientbehandling. To ting er spesielt viktig: Den ene er at taushetsplikt blir ivaretatt og den andre er at behandling blir faglig forsvarlig og effektiv. Det betyr at de må ha tilgang til nødvendig informasjon der og da når de trenger informasjon, både for å verne pasientintegritet og for å sikre at helsepersonell har nødvendig tilgang til nødvendig informasjon. Viss informasjonen er nødvendig når de behandler pasienten, så er informasjonssikkerhetskunnskap nødvendig.
I gårsdagens samfunn var informasjonssikkerhet definert ved den fysiske tilgjengeligheten til pasientjournalen. I den maskinskrevne journalen, eller kanskje håndskrevne notat, hos allmennlegen, var det en veldig lett og umiddelbart tilgang til informasjon. Enten fant du journalen eller så fant du ikke journalen. Fant du journalen så hadde du det som var aktuelt. I dag er ikke tilgang til journalen umiddelbar, den går gjennom en komplisert infrastruktur. Hvis du jobber i en poliklinikk så ligger kanskje dataene egentlig lagret på en server i Ullevål sykehus, i fremtiden kanskje lagret på en server på Gjøvik eller hvor som helst. Derfor, for å forstå tilgangen til data som er viktig med hensyn til pasient, så

må tilsynsførere ha et minstemål av kunnskap om infrastruktur.

Videre, for å forstå hvordan det kan være lekkasje av opplysninger må tilsynsfører forstå infrastrukturen. I gamle dager var det nok for tilsynsfører å forstå hvordan journalen ble låst inne i et skap for å vurdere om opplysningene var sikret.. I dag må en kjenne sikringsrutine i en infrastruktur som ikke bare handler om et kontor, men kanskje handle om hele helseNorge, for å kunne vurdere graden av beskyttelse.

Når Helsetilsynet skal verne om pasientintegritet og sikre forsvarligheten i pasientbehandlingen, er både integriteten og forsvarligheten avhengig av informasjonsteknisk infrastruktur. Da må tilsynsføreren kjenne et minstemål av det som ligger bak grenseflaten, det er ikke nok å forstå grenseflaten. Helsetilsynets arbeid skal være konsentrert om ytelsen av helsetjenester og helsepersonellets aktiviteter. I grenseflaten mellom disse skal Datatilsynet ha sin oppmerksomhet mot det spesielle ved sikkerheten i informasjonssystemene, mens Helsetilsynet skal se på informasjonssystemene og informasjonshåndteringen som en del av det totale helsetjenestesystemet.
For å kunne føre tilsyn innen helse- og sosial på en tilstrekkelig og forsvarlig måte, er kunnskap om informasjonssikkerhet nødvendig.

Ut fra funnene som ble gjort ved intervju med Helsetilsynets ledelse og studiet av skriftlig materiali, vises at det er behov for kompetanseøking innen informasjonssikkerhet hos tilsynsførere i Helsetilsynet.

Ut fra funnene som ble gjort ved intervjuene med ledelse i Helsetilsynet og Datatilsynet om samarbeid mellom dem, vises at det ikke er godt nok.

6.3 Forskningsspørsmål nr. 3

Hva er hensiktsmessig risikoanalysemetode ved tilsyn med informasjonssikkerhet i helseforetak?
Vi ble kjent med at pr. i dag bruker Helsetilsynet ikke noen metoder for tilsyn med informasjonssikkerhet. Det er et spørsmål om hvor godt det fungerer å ikke bruke noen metoder. Ut i fra min analyse av tilsynsrapportene, sett i forhold til de avvikene som gjelder tilgangsstyring som Datatilsynet finner ved helseforetakene, ser man at det fungerer svært dårlig. Jeg har oppdaget at det ikke fantes noe spor av informasjonssikkerhet i disse rapportene, og i intervju med ledelsen i Helsetilsynet, uttrykte de bekymringen over at informasjonssikkerhet ikke er integrert på en god måte i deres tilsynsarbeid. Ut i fra svarene fra spørreundersøkelsen om de opplevde utfordringer i tilsynsarbeidet med hensyn på informasjonssikkerhet, varierte svarene slik at ca. halvparten mente at de opplever dette "ofte månedlig", men halvparten svate "sjelden årlig)".

Da er det behov for at man må gjøre noe med dette. Jeg har samlet data om kravene til evt. ny metode dvs. har identifisert metodekravene. Jeg kan ikke si noe om hvilken metode som er mest hensiktsmessig før jeg skjønner hvilke krav som skal stilles til den metoden. Metodekravene består i at det må være en enkel og billig metode fordi brukere ikke har mye tekniske kompetanse og erfaringer i dette feltet. Metoden må være rask,

billig og enkel og ikke kreve mye opplæring.

Som jeg forklarte i kapittel 2, er det i SANDIA rapporten 9 grove kategorier av metoder i risikoanalyse. For å adressere de kravene som jeg har identifisert, vil jeg se på hvor gode disse kategoriene er, f. eks om noen av metodene krever veldig mye tekniske kunnskap og erfaring. Det betyr at hvis jeg har krav om at metoden skal være lett å bruke, så er de metodene som krever mye tekniske kunnskap uaktuelle. Det handler også om lovkrav som gjelder disse metodene som skal brukes f. eks en virksomhet som har vært gjennom flere tilsyn kan det hende allerede ha fått pålegg fra andre om å bruke bestemte metoder. I så fall vil det være naturlig kanskje i hvert fall å vurdere om en skal stille krav til ny metode eller om man bare skal ha tilleggskrav til bruk av metoden som brukes allerede.

Jeg kommer frem til den konklusjon at en sjekklistebasert metode er den mest hensiktsmessige metode for Helsetilsynet.

Sjekklistebasert metode krever relativt liten innsikt for de som skal bruke den, og kan være relativt rask å gjennomføre. En sjekkliste med veiledning kan innholde hva det er de skal sjekke når det gjelder informasjonssikkerhet. For eksempel hvilket tilsyn er utført, hvor gode vurderinger har de tatt, hvorfor har det gått feil. Dette betyr at sjekklisten må være basert på kvalitetskontroll av eksisterende tilsyn. Det må lages en liste over ting som de må sjekke bedre og grundigere, og forklares hvordan denne sjekken skal gjøres. Da har de fått et verktøy for å gjøre bedre tilsyn og tilsynskvaliteten forbedres.

6.4 Sammendrag av de viktigste funn

- Kompetansenivået er for dårlig
  Pr. i dag er kompetansenivået innen informasjonssikkerhet for dårlig.
- Kompetanseøking er nødvendig
  Det må gjøres noe med kompetanseøking i form av systematisk skolering eller obligatorisk kurs.
- Ingen spor av informasjonssikkerhet i Helsetilsynets tilsynsrapporter
  I fremtiden bør tilsynsrapportene inneholder noe om informasjonssikkerhet fordi konfidensialitet og tilgjengelighet er to sentrale ting i Helsetilsynets arbeid når de gjør tilsyn.
- Lite samarbeid mellom Helsetilsynet og Datatilsynet
  Helsetilsynet har i liten grad hatt et særlig fokus på et systematisk tilsyn med informasjonssikkerheten i helsetjenesten. Det er blitt gjennomført to fellestilsyn mellom Helsetilsynet og Datatilsynet som avdekket til dels store mangler. Både Helsetilsynet og Datatilsynet har tatt disse funnene opp med Helse- og omsorgsdepartementet. Ut over dette er det ikke særlige spor etter vurdering av informasjonssikkerheten i revisjonsrapportene fra Helsetilsynet. Helsetilsynet blir orientert fra Datatilsynet om de tilsynene som de gjennomfører, og i noen grad deltar de også som observatører ved slike tilsyn.
  Samlet sett er Helsetilsynets innsats i forhold til systematisk tilsyn med informasjonssikkerheten liten. Dette kan jeg til dels forklare med en viss usikkerhet om hvilke krav

som kan stilles overfor helseforetakene ut fra gjeldende helselovgivning. Men dette er bare en mulig forklaring. En annen forklaring som jeg kan se, som er minst like viktig, er at Helsetilsynets tilsynsførere ikke har nok kompetanse innenfor dette feltet.

6.5 Behov for tiltak

Jeg mener at følgende tiltak er nødvendig::

6.5.1 Opplæring

Det må holdes en form for systematisk skolering for kompetanseheving (et løpende kurs) til tilsynsførere. Innholdet i dette kurset bør dekke følgende områder:

- Basiskunnskap om hva som er de vanligst brukte systemene ut i helsetjenesten og vanlige EPJ system f. eks DIPS, slik at de vet hvordan disse fungerer ren teknisk operasjonelt.
- Forholdet mellom Helsetilsynet og Datatilsynet slik at det ikke er i tvil om hvor grenseflaten går. Datatilsynet bør inviteres til å være med for å fortelle om sitt selvbilde og Helsetilsynet om sitt.
- Presentere en modell for risikoanalyse med sjekkliste for informasjonssikkerhet som arbeidsverktøy.

6.5.2 Rekruttere personer med kompetanse

Helsetilsynet har gode erfaringer med systemrevisjoner og de setter sammen revisjonsteam med tverrfaglig kompetanse, en som kan mye om tilsyn, en som kan mye om helsetjenesten og en jurist. Dette er en typisk sammensetting av et tilsynsteam. Det kan godt tenkes at den som kan mye om tilsyn f. eks og skal være en person som kan mye om IT, eller at den som kan mye om helse og skal være en person som har fått en basisutdanning i informasjonssikkerhet. Helsetilsynet ønsker ikke å dele tilsyn i to deler: en helsefagligdel og en informasjonssikkerhetsdel, men sørge for at tverrfaglig team har nødvendig kompetanse til å gjøre en anstendig jobb på informasjonssikkerhet. Dette betyr at de bør rekruttere flere personer med nødvendige kompetanse.

6.5.3 Skrive retningslinjene for systemrevisjonen på nytt

En systemrevisjon er en revisjon der det undersøkes om styringssystemet sikrer etterlevelse av myndighetskravene. En revisjon er en systematisk, uavhengig og dokumentert prosess for å fremskaffe revisjonsbevis og bedømme om revisjonskriteriene er oppfylt.
Systemrevisjon gjennomføres for å få et bilde av hvorvidt og på hvilken måte virksomheten har innrettet seg for å etterleve kravene, skriftlig dokumentasjon gjennomgås, og ledere og ansatte intervjues. Tilsynet vil også, gjennom stikkprøver (verifikasjoner) avklare om rutiner og prosedyrer er kjent og etterleves i praksis, og om de er effektive i forhold til oppgaven eller problemet som skal løses. I tillegg til å avdekke svikt på tilsynstidspunktet, kan tilsynet avdekke uheldige forhold som på sikt kan medføre et problem for rettssikkerhet eller forsvarligheten i tjenesten, og dermed forebygge brudd på lover og forskrifter.

Systemrevisjonen inneholder ikke noe om informasjonssikkerhet pr. i dag, men den inneholder en god del om forsvarlighet og taushetsplikt. Informasjonssikkerhet må bli en naturlig integrert del av tilsynet. Dette betyr at retningslinjene for systemrevisjonen må skrives på nytt slik at det inneholder en egen del om informasjonssikkerhet. Helsetilsynets tilsynsmaler må inneholde en enkel sjekkliste med veiledning som gjør det enkelt for folk å etterspørre de rette tingene, slik at de slipper å tenke dem ut selv hele veien. Denne sjekklisten som er et resultat av denne oppgaven kunne være et slikt enkelt hjelpemiddel eller verktøy. Sjekklisten kan være et vedlegg til systemrevisjonsmalen. I de situasjonene der det er naturlig å se på informasjonssikkerhet, skal denne legges til grunn.

6.5.4 Systematisk samarbeid mellom Datatilsynet og Helsetilsynet

Når det gjelder arbeidsdeling mellom de to tilsynsetatene, er det som foregår inn i systemet Datatilsynets sitt ansvar, for å si det slikt, men det som kommer ut av det systemet, måten helsepersonelle forholder seg til tastatur og skjermbilde på, det er Helsetilsynets tilsynsansvar. Hvilke personer som kan komme inn på et gitt skjermbilde eller i en gitt database er Helsetilsynets tilsynsansvar. Men når opplysningene er inne i systemet er det Datatilsynet sitt tilsynsansvar.
Til en viss grad er Datatilsynet og Helsetilsynets tilsynsansvar overlappende. Men for å få utnyttet samlet kompetanse er et mer systematisk samarbeid viktig.

Helsetilsynet og Datatilsynet har størst behov å være synkronisert overfor hverandre når det gjelder tilgangsstyring, spesielt §13 [Tillegg A.1] hvor taushetspliktbestemmelsen møter sikkerhetsbestemmelsene, og hvor det er helseforvaltningene og Helsetilsynet som kan sette rammene for hva som er godt nok og hvor langt taushetsplikten går i forhold til tilgangsstyring. Begge tilsynsorganene trenger tverrfaglig kompetanse knyttet til både behov for tilgjelighet og taushetsplikten på den helsefaglige side, hva som er god nok sikring av konfidensialitet på sikkerhetssiden.

6.6 Økonomiske og administrative konsekvenser av funnene

Informasjonssikkerhet blir viktigere og viktigere. Vi har sett i de siste årene at mange virksomheter begynner å ta dette på alvor. Regleverket blir mer og mer omfattende, men også mer dekkende for ulike risikomomenter i dette feltet.

Helsetilsynets oppgaver innenfor tilsyn med helsetjenesten er krevende og omfatter også informasjonssikkerheten. Men det må gjøres noe for å forbedre Helsetilsynets innsats på dette området.

Jeg vil tilrå at etaten begynner å integrere informasjonssikkerhet i sitt ordinære tilsyn. Man da må de nok gjøre noen endringer i sine prosedyrer både for opplæring av tilsynsførere og gjennomføring av tilsyn.

Etaten må gjøre et løft for kompetanseheving for sine tilsynsførere. Dette kan medføre at de må ansette noen tilsynsførere som har gode erfaringer eller bakgrunn fra IT i tillegg

til den generelle relevante kompetansen som en tilsynsfører må ha.

Fra nå og fremover bør etaten vurdere å stille noe ekstra krav om kunnskaper om informasjonssikkerhet når de ansetter folk for å jobbe med tilsyn. Dette er et tiltak som i og for seg ikke medfører ekstra kostnader, ut over at kanskje slike personer vil kreve noe høyere lønn enn det som tilbys i dag til tilsynsførere.

Men utfordringen kan også løses ved at det lages et opplegg for kurs eller systematisk skolering for de nåværende tilsynsførere. Dette er noe som svarene i min undersøkelse fra Helsetilsynet i fylket tyder på er av stor interesse. De tilsynsførerne som Helsetilsynet har i dag har store kunnskaper om helsetjenesten og om internkontrollsystemer samt vurderinger av konkrete forhold som forsvarlighet og kravet om taushetsplikt. De har derfor etter min vurdering et godt utgangspunkt for å tilegne seg nødvendig kunnskap for også å vurdere informasjonssikkerhet på en mer helhetlig måte.
En slik opplæring bør tilstrebes gjennomført på to måter:

A) Informasjonssikkerhet bør inn som et obligatorisk tema i den interne opplæringen av nye tilsynsførere. Dette krever en viss justering av timeplanen for revisjonskursene, men i seg selv er det ikke forbundet med spesielle kostnader. Det kan være nødvendig å vurdere om tidsrammen for det første opplæringskurset utvides med en dag, og da vil det være forbundet med kostnader tilsvarende lærerinnsats en ekstra dag samt et ekstra kursdøgn og en ekstra fraværsdag fra ordinært arbeid for hver kursdeltager.

B) Et oppdateringskurs for alle som i dag er tilsynsførere i Statens helsetilsyn og Helsetilsynet i fylket. Dette kan gjennomføres som et endagskurs der sjekklisten i kapittel 7 blir introdusert og forklart sammen med en orientering om vanlig brukte systemer for elektronisk informasjonshåndtering i helsetjenesten. Antallet personer som er aktuelle for et slikt kurs kan fort bli rundt 100 personer. Selv om disse deles på kursgrupper ulike steder i landet, kan kostnadene ved et slikt opplæringstiltak raskt bli i størrelsesorden kr. 500.000 - 1.000.000. Men med den viktigheten som informasjonssikkerhet allerede har og ikke minst slik utviklingen forventes å bli, er dette noe Helsetilsynet seriøst bør vurdere.

6.7 Forslag til tiltak for håndtering av identifiserte utfordringer

Følgende tiltak foreslås i forbindelse med håndtering av identifiserte utfordringer i fremtidige arbeid. Disse tiltakene kan være langsiktige eller kortsiktige.

6.7.1 IT-tilsyn

Fremtiden er jo IT og det elektroniske vil etter hvert overta det papirbaserte. Riksrevisjonens undersøkelse om IKT i sykehus og elektronisk samhandling i helsetjenesten utført 2007-2008, viser at alle helseforetakene unntatt Sykehuset Vestfold HF har et EPJ system [1].

Tall fra et tilsvarende grundig kartleggingsarbeid, årsrapport 2008 utgitt av Norsk Senter

[1] http://www.riksrevisjonen.no/SiteCollectionDocuments/Dokumentbasen/Dokument3/2007-2008/Dok_3_7_2007_2008.pdf, siste besøkt 25.05.2010.

for Elektronisk Pasientjournal, forteller at alle helseforetak har anskaffet EPJ og at innføringen nærmer seg å bli fullført. Det har gått over 20 år fra de første sykehusene hadde innført EPJ til siste sykehus fikk EPJ [2].

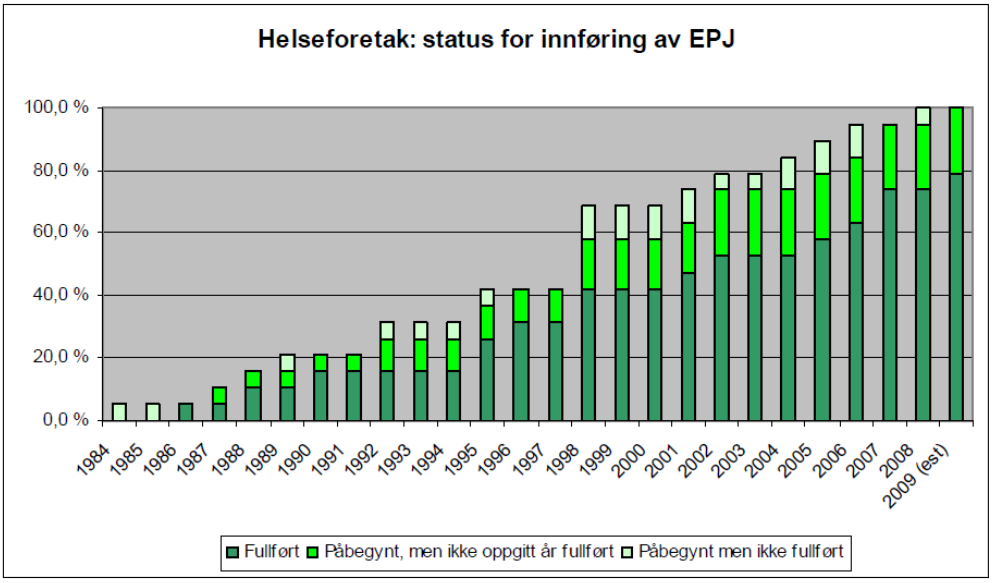

Figure 6: Andel helseforetak som har innført EPJ

Figuren hentet fra sidenummer 3 fra EPJ Monitor Årsrapport 2008.

Selv om IT-tilsyn er et svært omfattende og dekker et stort område, er resultatet og det som kommer ut av det, svært viktig med tanke på at Helsetilsynet har ansvar for menneskers liv og helse. På langt sikt bør det vurderes et eget IT-tilsyn som dekker informasjonssikkerhet i den trekanten som er mellom pasient, behandler og teknologi. Hvis dette ble integrert som en naturlig del av det tilsynet Helsetilsynet gjør med forsvarlighet og vern av taushetsplikt, ville det styrket tilsynet med sosial og helse.

Når det gjelder økonomiske, administrative og lovmessige konsekvenser av et IT-tilsyn med helseforetakene, er det ingen tvil om at dette medfører ekstra kostnader. Som jeg fortalte tidligere om Finanstilsynets opplegg, jobbet de først med en IKT-forskrift for finans. Her snakker jeg om IKT-forskrift for helse. Det er ikke sikkert at det trenges egen forskrift for det. Det kan være nok å nevne IT som et spesifikt punkt i Internkontrollforskriften for helsetjeneste. Det ville ha gitt Helsetilsynet god nok forskriftsbasis, og når det er gjort så kan de ganske fritt utvikle sine egne prosedyrer. For eksempel hvis det sto i forskriften at Internkontrollsystemet skulle omfatte kontroll med informasjonssikkerhet i henhold til anerkjente standarder, ville det være nok for å gå ut å føre tilsyn.

[2] http://www.nsep.no/publikasjoner/EPJ%20Monitor%202008.pdf, siste besøkt 29.06.2010

6.7.2 Inspeksjons- eller verifikasjonspreget tilsyn

Helsetilsynet kunne gjøre et noe enklere inspeksjons eller verifikasjonspreget tilsyn, som bare var teknisk orientert på en måte som ville gjort det raskt å gjennomføre på mange plasser. Datatilsynet gjorde noe spennende for to år siden da de hadde en spørreundersøkelse til alle regionale helseforetak om hvordan de hadde sikre IT-teknologien og informasjonsprosedyrene sine og fikk Helseforetakene selv til å gi en selvmelding tilbake på sin egen status. Helsetilsynet kunne bedt alle legekontor f. eks om å gi en kort beskrivelse etter en spørsmålsliste om hvordan de har ivaretatt sin informasjonssikkerhet.

6.8 Diskusjon

Datatilsynet gjennomfører årlig 5 - 15 tilsyn i forhold til helsetjenesten. Helsetilsynet gjennomfører ca 300 tilsyn hvert år. Fram til nå har ikke informasjonssikkerhet blitt vektlagt av Helsetilsynet. Dersom man sikrer at informasjonssikkerhet blir inkludert i Helsetilsynets øvrige arbeid, vil det derfor bety en vesentlig styrking av tilsynet på dette området i Norge. Jeg vurderer det slik at på grunn av det store volumet av tilsyn som gjennomføres av Helsetilsynet, vil selv en liten styrking av tilsyn med informasjonssikkerheten, f.eks. gjennom bruk av en sjekkliste som beskrevet her i oppgaven, bety en reell forbedring.

Det er dessuten ytterligere muligheter ved å øke samarbeidet om planlegging og gjennomføring av tilsyn mellom Helsetilsynet og Datatilsynet. Selv om man ikke kan gjennomføre slike fellestilsyn i et større omfang, tyder erfaringene fra fellestilsyn med to større helseforetak i 2006 på at slike felles satsninger gir virkninger langt ut over de virksomhetene som det blir ført tilsyn med. Helsetilsynet og Datatilsynet bør derfor i samarbeid på et strategisk grunnlag vurdere regelmessig å gjennomføre noen få større tilsyn med et innhold rettet mot forhold der risiko og sårbarhet vurderes som stor.

Når det gjelder hensiktsmessig metode for Helsetilsynet, kan jeg se på de alternativene jeg har på bakgrunn av de kravene jeg har identifisert. Jeg kan ikke se at ISO 27005 er en metode som egner seg. En troverdig kompetanse på ISO 27005 kan ikke oppnås med en dags opplæring og slikt tilsyn kan ikke gjennomføres i løpet av endags arbeid. Ser jeg på resultatet fra forskningsspørsmål 1 som viser at Helsetilsynets kompetanse innen informasjonssikkerhet er svært lav, kan jeg si at den mest hensiktsmessige metoden er en sjekklistebasert metode. Jeg ser at behovet for kompetanseøking er stort dvs. det er vanskelig egentlig i praksis å bruke dagens metoder for å få et ordentlig tilsyn. Det vil være et omfattende prosjekt å opparbeide tilstrekkelig kompetanse i informasjonssikkerhet, så hvordan skal man da gå frem sånn at det allikevel bli et brukbart tilsyn?
Ut i fra den antagelsen, hva er hensiktsmessige risikoanalysemetode for Helsetilsynet? Det som er mest hensiktsmessig metode er en billig og enkel sjekklistebasert metode med en liten veiledning.

Hvis jeg tar utgangspunktet i SANDIA-rapporten og bruker den som et verktøy for å klassifisere metoden, finner jeg og ut fra dataene som jeg har innsamlet at kategori 3 kan være aktuelt for Helsetilsynet (se tabellen i figure 2 under seksjon 2.3). Jeg begrunner dette med at denne typen er basert på en eksplisitt standard og at den ber brukeren

om å vurdere effektiviteten av kontrollene når det gjelder å oppfylle hvert element i standarden, og den trenger lavt kunnskapsnivå for de som utførere dette.

7 Utvikling av sjekkliste tilpasset behovene til Helsetilsynet

Da behov for en billig og enkel metode for risikoanalyse er avdekket, utvikler jeg i dette kapitlet en slik metode basert på sjekkliste-tilnærming. Formålet med denne sjekklisten at den dekker de mest alvorlige tingene som jeg har identifisert gjennom erfaringer og tilbakemeldinger fra spørreundersøkelser.
Kapitlet gir en tekstlig beskrivelse av sjekklistemetoden og selve sjekklisten finnes i appendiks H.
Områdene beskrevet nedenfor er bygget på egne erfaringer fra arbeidet med it-sikkerhet i Helsetilsynet og skriftlig materiale [27] [11] [2] [5] [41] [10].

7.1 Krav til sjekklisten

MMinimumskompetansekrav for å bruke denne sjekklisten er at personen må ha forståelse av hvordan IT-system fungerer, hva personvern er, kjennskap til taushetsbestemmelser og å ha gjennomført informasjonssikkerhetsmodulen som må etableres i Helsetilsynets systemrevisjonskurs.
Sjekklisten kan gjennomføres i løpet av en dags arbeid. Virksomheten eller institusjonen som er utsatt for tilsyn/analysen, må avsette personressurser i området IT og informasjon, arkiv og ledelse slik at de kan svare på kontrollspørsmålene.

7.2 Område som dekkes av sjekklisten

De tingene som er mest viktige for Helsetilsynets arbeid er konfidensialitet og tilgjengelighet. Virksomhetene som utsette for tilsyn må ha gode sikkerhetsrutiner slik at tilgjengelighet til både data og personale alltid er på plass når det trenges, og tilgangsstyring gis på en forsvarlig måte slik at uvedkommende ikke har tilgang til data.
Jeg ser det fornuftig å minne om at begrepet informasjonssikkerhet omfatter:

- Sikring av *konfidensialitet*, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene.
- Sikring av *integritet*, dvs. beskyttelse mot utilsiktet endring av opplysningene.
- Sikring av *tilgjengelighet*, dvs. sørge for at tilstrekkelige og relevante opplysninger er til stede.

Når det gjelder struktur i dette kapitlet, har jeg laget tre spørsmål for hvert av områdene som sjekklisten dekker. Spørsmålene er følgende:

Hva er det?
En kort beskrivelse av dette området og oppdeling i flere underområder.

Hvorfor er dette området viktig?
Her beskrives viktigheten av området og deretter knyttes det til lovverket og/eller en standard.

Hva skal sjekkes og hvordan?
Her skal jeg beskrive hvert underområde, og deretter gi en kort beskrivelse av de hovedpunktene som skal sjekkes/kontrolleres.
Følgende områder er nærmere beskrevet:

- Styringsstem for informasjonssikkerhet, som deles i flere underområder:
  Risikovurdering, sikkerhetsrevisjon, informasjonssikkerhetsbrudd og ledelsens gjennomgang.
- Teknisk sikkerhet, som deles i flere underområder:
  Sikkerhetskopiering (backup), passord, programvare/Antivirus, bruk av e-mail, logging og oppfølging.
- Tilgangsstyring
- Håndtering av lagringsmedia og kassasjon
- Hjemmekontor
- Opplæring av ledere og medarbeidere
- Kontinuitetsplan

7.2.1 Styringssystem for informasjonssikkerhet

- *Hva er det?*
  Styringssystem for informasjonssikkerhet har en forkortelse på engelsk ISMS (Information Security Managemet System) Styringssystem for informasjonssikkerhet har en forkortelse på engelsk ISMS (Information Security Managemet System) og siden dette er et begrep som er kjent i litteraturen, vil jeg bruke denne forkortelsen videre. Alle virksomheter i helsesektoren skal etablere ISMS. Omfang av styringssystemet skal være tilpasset virksomhetens størrelse og omfanget av behandling av helse- og personopplysninger. Virksomhetens ledelse er ansvarlig for at virksomheten har de nødvendige prosedyrer (etablere og innføre) i ISMS.

  Den styrende delen av ISMS omfatter:

  a) Beskrivelse av ledelse og organisering av informasjonssikkerhet.

  b) Beskrivelse av og oversikt over formålet med behandlingene.

  c) Fastsettelse av sikkerhetsmål og -strategi.

  d) Fastsettelse av nivå for akseptabel risiko.

  Underområder som skal sjekkes/kontrolleres er følgende:
  a) Risikovurdering b) Sikkerhetsrevisjon c) Informasjonssikkerhetsbrudd
  d) Ledelsens gjennomgang

- *Hvorfor er dette området viktig?*
  ISMS skal sikre at personvernet og sikkerhetsarbeidet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte.
  Manglende risikostyring kan medføre at risiko ikke blir påvist, og at nødvendige sikringstiltak ikke blir iverksatt. Manglende rutiner for rapportering og håndtering av sikkerhetsbrudd kan medføre at det ikke er mulig å treffe korrigerende tiltak i rett tid.

  Når det gjelder lovparagrafene vil jeg nevne de mer rettede her:
  Dette er fastsatt i Personopplysningsforskriften Del I.
  Sikkerhetsledelses gjennomgang jf. Personopplysningsforskriften §2-3
  Risikovurdering jf. Personopplysningsforskriften §2-4
  Sikkerhetsrevisjon jf. Personopplysningsforskriften §2-5 og Helseregisterloven
  Avvikshåndtering jf. Personopplysningsforskriften §2-6 og Internkontrollforskriften av 20. des. 2002 nr. 1731, jf. helsepersonelloven §16, 2. ledd.

  Alle disse underområdene er i samsvar med I ISO/IEC 27002:2005 kapitlene 4, 5, 6 og 13.

- *Hva skal sjekkes og hvordan?*
  Risikovurdering
  Risiko er produktet av konsekvensen av og sannsynligheten for at noe går galt. Sannsynlighet og konsekvens kan fastsettes med skalaen liten - middels - stor, eller med en tallskala.
  Leder må avgjøre hvilke systemer og virksomhetsområder det skal gjennomføres vurderinger av. Mange virksomheter er underlagt krav i lov eller forskrift om å gjennomføre risikovurdering. En risikovurdering eller risikoanalyse skal avdekke trusler og hendelser som kan berøre driften. Truslene innen informasjonssikkerhet er noe som kan føre til brudd på konfidensialitet, integritet og/eller tilgjengelighet. Eksempel på slike hendelser er brann, svikt i utstyr og feil i data. Resultatet av risikovurderingen skal kommunisere hva det er viktig for virksomheten å gjøre noe med. Der risikoen er større enn akseptert nivå må det vurderes om det skal settes inn tiltak for å redusere sannsynligheten og/eller konsekvensen. Tiltak må vurderes etter hva slags type risiko det er snakk om.

  Sikkerhetsrevisjon
  Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. §2-6. Resultat fra sikkerhetsrevisjon skal dokumenteres og gjennomgås ifm. ledelsens gjennomgang.
  I den årlige sikkerhetsrevisjon skal det kontrolleres at alle avvik er håndtert. Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten.

  Informasjonssikkerhetsbrudd

En sikkerhetshendelse skader eller truer personell, informasjon eller verdier. Den som oppdager en hendelse skal umiddelbart varsle nærmeste leder.

Informasjonssikkerhetshendelser kan være:

a) Tap av tjenester, utstyr eller funksjoner.

b) Teknisk svikt eller overbelastning i systemene.

c) Menneskelig feil.

d) Manglende samsvar med policy og retningslinjer.

e) Brudd på fysiske sikkerhetsordninger.

f) Ukontrollerte systemendringer.

g) Teknisk svikt i programvare eller maskinvare.

h) Brudd på aksessrettigheter.

Ledelsens gjennomgang
Virksomhetens ledelse skal jevnlig, eksempelvis årlig, gjennomgå sikkerhetsmål og strategi. Slik ledelsesgjennomgang vil ha som formål å vurdere hvorvidt de beslutninger som er tatt, er i samsvar med virksomhetens behov for informasjonsteknologi og informasjonssikkerhet. Gjennomgangen vil danne grunnlag for eventuelle endringer av sikkerhetsmål eller strategi. Praktisk kan ledelsesgjennomgang gjennomføres innenfor rammen av årlig økonomi- eller virksomhetsplanlegging.

Kontroll og oppfølging

- Ledelsen skal utarbeide og vedta en plan for risikovurderinger.
- Ledelsen skal foreta kontroll av risikovurderingene og påse at resultatet av risikovurderingene er i henhold til fastlagte akseptkriterier.
- Sikkerhetsrevisjoner skal gjennomføres jevnlig og minimum årlig. Ledelsen skal utarbeide og vedta en plan for sikkerhetsrevisjoner i virksomheten.
- Avvikshåndtering iverksettes ved sikkerhetsbrudd og/eller når oppgaver utføres i strid med gjeldende prosedyrer eller "vanlig praksis". Virksomheten skal ha en egen prosedyre for håndtering av avvik.

Formålet med ledelsens gjennomgang er å avdekke om sikkerheten ivaretas iht. mål, strategier og prosedyrer og beslutte handlingsplaner for det videre sikkerhetsarbeidet. Ledelsen gjennomgang skal gjennomføres minimum årlig og i sammenheng med årlig økonomi eller virksomhetsplanlegging.

7.2.2 Teknisk sikkerhet

- *Hva er det?*
  Dette området kan deles i tre underområder:
  - Sikkerhetskopi (backup).
  - Passordshåndtering.
  - Programvare/Antivirus.

- Bruk av e-mail.
- Logging og oppfølging.

Sikkerhetskopi (backup)
Alle virksomheter i helsesektoren skal ta sikkerhetskopi av helse- og personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk. Målet er å sikre konfidensialitet, integritet og tilgjengelighet til alle driftsmessige og systemmessige IKT leveranser for virksomheten. Virksomheten skal etablere prosedyre for sikkerhetskopiering og sørge for at den blir gjennomført. Videre må sikkerhetskopiene verifiseres ved å teste den regelmessig (tilbakeføre data). Sikkerhetskopi tapene må oppbevares både på sikre steder og må være lett tilgjengelig ved behov.

Passord
Formålet med passord er å sikre konfidensialitet og integritet ved behandling av helse- og personopplysninger. Brukernavn og passord er personlig og skal være hemmelig. Dårlige passord opphever andre sikkerhetstilstak så det må ikke brukes passord som andre enkelt kan tenke seg frem til. Ved mistanke om at andre har fått kjennskap til passordet, må det byttes straks.
Virksomheten må ha rutiner for passord og passordhåndtering. For eks felles brukernavn og passord må ikke benyttes i applikasjoner med helse- og personopplysninger. Rutinen må også inneholde når en ansatte endrer avdelingen (med tanke på ansvarsområde), fratrer eller tar permisjon fra stilingen og det må finnes en passordpolicy. Policyen skal inneholde passordlengde, type karakter, obligatorisk periodisk bytting av passord og sperring av konto etter antall mislykkede forsøk. Det kan bli varierende passordskrav etter hvem som logge seg på (brukertype) og hvilken type applikasjon eller database brukeren logger seg på.

Programvare/Antivirus
Det er viktig at uprofesjonelle verktøyer ikke brukes, særlig i den mindre styrte del av helsesektoren. Oppgradering av programvarer er en viktig del bl.a. sikkerhetsoppdateringer, antivirus og signaturfilene til den.
Kun IT-folkene må ha tilgang til installering og testing av programvarene. Testing av programmer må foregå i et testemiljø hvor det ikke finnes helse opplysninger. Vanlige brukere må ha begrenset tilgang til nedlasting av programvare og ikke ha administrator- rettigheter for installering av programmer.

Bruk av e-mail
Virksomheten må ha klare regler for at sensitive data ikke sendes pr vanlig e-mail. Ved behov for bruk av slik kommunikasjon, må innholdet krypteres eller utveksles i sikre kanaler (SSL). Videre og innen policyen må det ikke tillates mottak av kjørbare filer som vedlegg til e-mail, da dette kan føre til spredning av virus, trojaner og annen ondsinnet kode m.m.

Logging og oppfølging
Alle virksomheter i sektoren som behandler helse- og personopplysninger elektronisk, skal føre og kontrollere hendelsesregistre. Virksomheten skal etablere prosedyrer som

sikrer at hendelsesregistrering (loggføring) etableres. Den skal sikres mot innsyn, endring og sletting av uautorisert personell. Dersom oppføringer i hendelsesregistre kan knyttes til enkeltpersoner, skal loggføringene slettes når de sikkerhetsmessige formål er oppfylt, men først etter 2 år.
Et loggregister for en autorisert bruker må minimum inneholde:

- Entydig identifikator for den autoriserte brukeren.
- Rollen den autoriserte brukeren har ved tilgangen.
- Virksomhetstilhørighet for den autoriserte brukeren (vanligvis virksomhet eller databehandler).
- Organisatorisk tilhørighet til den som er autorisert (avdelingsnavn eller avdelingskode er normalt tilstrekkelig). Kan være lik virksomhetstilhørighet om virksomheten ikke har avdelingsstruktur.
- Hvilken type opplysninger det er gitt tilgang til.
- Grunnlaget for tilgangen (for eksempel helsehjelp, nødrettstilgang, administrativ bruk).
- Tidspunkt og varighet for tilgangen (dato og klokkeslett).
- Begrunnelse ved bruk av nødrettstilgang.

- *Hvorfor er dette området viktig?*
  Sikkerhetskopi kjøres for a sikre at helse- og personopplysninger kan gjenopprettes om de skulle gå tapt som følge av bl.a.:
  - Feil i utstyr eller programvare.
  - Utilsiktet sletting av bruker.
  - Tilsiktet ødeleggelse/hærverk.
  - Tap/tyver av utstyr.

  Passord er viktig for at data ikke kommer på avvei eller blir endret.
  Programvare og bruk av e-mail:
  De er viktige fordi det kan medføre at uvedkommende får tak i data, de kan slettes eller endres. I tillegg til kan det hende at hele foretaket og flere andre rammes av for eks. et virus.
  Logging og oppfølging
  Den er viktig for den kan:
  - Gi oversikt over autorisert bruk av helse- og personopplysninger i virksomheten.
  - Sette virksomheten i stand til å avdekke uautorisert bruk, eller forsøk på uautorisert bruk, av helse- og personopplysninger.
  - Forebygge, avdekke og forhindre gjentagelse av sikkerhetsbrudd i informasjonssystemene.
  - Legge til rette for pasient/brukers rett til innsyn i hendelsesregistre, slik at vedkommende gis mulighet til å ivareta egne rettigheter.
  - legge til rette for ansattes rett til innsyn i opplysninger som er lagret om vedkommende i hendelsesregisteret.

Lovhjemmel:
Buckup: Personopplysningsforskriften §2-12 Sikring av tilgjengelighet og Helseregisterloven §16 Tilgjengelighet.
Passord: Personopplysningsforskriften §§2 - 11 Sikring av konfidensialitet og 2-13 Sikring av Integritet.
Programvare/Antivirus/Bruk av-email:
Personopplysningsforskriften §§2-12 Sikring av tilgjengelighet,§§2 - 11 Sikring av konfidensialitet og 2-13 sikring av integritet
Logging og oppfølging:
Personopplysningsforskriften §2-14 Sikkerhetstiltak, §2-16 Dokumentasjon og §7-11, Det kan bli lovkrav når "Forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre" blir godkjent.

Alle disse underområdene er i samsvar med I ISO/IEC 27002:2005

- *Hva skal sjekkes og hvordan?*
  Sikkerhetskopi:
  Er det etablert prosedyre for sikkerhetskopiering, testes tapene jevnlig ved å tilbakeføre dataene (restore)? Er denne kompetansen tilgengelig internt eller eksternt? Har virksomheten rutiner for oppbevaring av tapene, også kopier utenfor huset? Hvordan er dette organisert?

  Passord:
  Har virksomheten rutiner for passordhåndtering? Har de passordpolicy (kan det verifiseres?). Dersom de bruker eksterne utstyr for pålogging (trådløs eller mobil), hvordan foregår pålogging (i krypterte kanaler SSL eller vanlige)? Får brukere opplæring i passordshåndtering? Pålagt skriftlig krav at alle må ha skjermbeskytter med passord for eks. i sikkerhetsinstruks for brukerne?

  Programvare/Antivirus:
  Om virksomheten har en rutine/policy for håndtering av programvare bl.a. nedlasting, installering, testing, oppgradering og oppdatering. Videre om det legges vekt på hvilken type verktøy som brukes ved programvareinnkjøp og kriteriene som bestemmer dette. Videre om virksomhetene har tilstrekkelig virusbeskyttelse.

  Bruk av e-mail:
  Om Virksomheten følger noen regler for bruk av e-post, brukes krypterte e-post for utveksling av data evt. I hvilket tilfelle, finnes det policy for innkommende e-mailer, og har ansatt fått opplæring og bevisstgjøring om reglene/eller konsekvensene av å ikke følge reglene.

  Logging og oppfølging:
  Har virksomheten har etablert prosedyrer for loggføringe? Rutiner for oppfølging, oppbevaring og sletting av loggføringer. Tilgang til loggene og hvor godt beskyttet mot manipulering.

7.2.3 Tilgangsstyring

- *Hva er det?*
  De ansatte skal gis tilgang (autoriseres) til virksomhets lokaler, systemer, infrastruktur og informasjon ut fra tjenstlig behov. Tilganger til systemet endres løpende når en bruker endrer sine tilgangsbehov eller slutter. Alle systemer, informasjon og infrastruktur skal sikres med tilgangskontroll. Leder er ansvarlig for at det minst årlig foretas en gjennomgang av alle tilganger eller ved endring og innføring av nytt system. Organiseringen av tilgangsrettigheter i et EPJ-system baseres på roller (hvilken profesjon man tilhører, hvilke arbeidsoppgaver man har), og hvor man arbeider (geografisk tilhørighet). De ulike grupper av helsepersonell får tilgang til hele eller deler av pasientjournalen ut fra hva man i kraft av sin rolle og sine arbeidsoppgaver vil ha behov for. Klart definerte roller og rollemaler kan være et hjelpemiddel for å definere tilgangsrettigheter i et EPJ-system.
  Hvilken informasjon har man tilgang til (informasjonsdypde), avhenger av hvilke deler (journalgrupper/kapitler) av journalen det er gitt tilgang til. Her gjelder det også tilgangs varighet dvs. tilgang til informasjonen med hensyn på tid. Formålet med tilgangsstyring er å sikre at helse- og personopplysninger kun er tilgjengelig etter tjenstlig behov. Dette innebærer at brukere autentiseres på en betryggende måte og at tilganger tildeles, administreres, kontrolleres og fjernes.

- *Hvorfor er dette området viktig?*
  Dette er viktig fordi uautoriserte ikke skal få tilgang til uberettige data.

  Lovhjemmel
  Tilgang til helseopplysninger regulert i flere lovverk bl.a. i:

  - Forvaltningsloven §13 om taushetsplikt
  - Helsepersonelloven §21 om taushetsplikt, §25 om opplysninger til samarbeidende personell og §45 om utlevering av og tilgang til journal og journalopplysninger.
  - Helseregisterloven§11 om krav til formålsbestemthet, saklighet, relevans m.v.,§13 om tilgang til helseopplysninger i den databehandlingsansvarliges og databehandlers institusjon og om den registrertes rett til innsyn i logg fra behandlingsrettet helseregister.
  - Helseforskningsloven §7. Taushetsplikt.
  - Andre aktuelle bestemmelser finnes i bl.a. personopplysningsloven, pasientrettighetsloven og pasientjournalforskriften.

  Tilgangsstyring er i samsvar med I ISO/IEC 27002:2005 kap. 11.

- *Hva skal sjekkes og hvordan?*
  Virksomheten må ha utarbeidet rutiner for tildeling/endring/avslutning av autorisasjoner for eks. benytting av autorisasjonsskjema. Tilgang til EPJ skal dokumenteres i journalen med opplysninger om hvem som er gitt tilgang og periode. For å sikre at tilgangen er autorisert og i henhold til regelverket, er logg-gjennomganger et viktig kontrolltiltak å avdekke uautorisert tilgang. Deaktivering av brukerkontoer som ikke

er i bruk kan være et kontrolltiltak.

7.2.4 Håndtering av lagringsmedia og Kassasjon

- *Hva er det?*
  Personsensitive data skal ikke lagres på flyttbare medium (minnepinner, diskett, CD og lignende) uten kryptering. Bærbare maskiner som brukes for behandling av sensitive informasjon må være kryptert. Dette må være full kryptering av harddisk, sperring av alle nettverkskort og hvor kun krypterte minnepinner tillates brukt. Gammelt IKT-utstyr som kasseres (fases ut av systemet) kan inneholde spor etter sensitiv informasjon, selv om dataene er slettet på vanlig måte. Utstyr som servere, arbeidsstasjoner, palmer, mobiltelefoner, skrivere, kopimaskiner, skannere og multifunksjonsskrivere kan ha harddisk eller mellomlagringssted. Derfor må disse behandles på en sikker måte, for eks ved at harddiskene tas ut, eller at det brukes godkjente programmer for sikker sletting av data før de blir kassert.
  Utskrift av personopplysninger som er sendt til skriver og ikke ble hentet med engang, kan også medføre brutt på konfidensialitet.

- *Hvorfor er dette området viktig?*
  På et ukryptert lagringsmedium er det lett å få tilgang til data. Dette er spesielt viktig når det gjelder transportable medier som minnepinner og annet bærbart utstyr. Slikt utstyr kan lett mistes eller komme på avveie. I enda større grad gjelder dette når utstyr kasseres. Det kan medføre brudd på konfidensialitet hvis du for eks kaster en harddisk som inneholder sensitive opplysninger og uvedkommende får tak i den.

  Lovhjemmel
  Personopplysningsforskriftens §2-11 Sikring av konfidensialitet, §2-12 Sikring av tilgjengelighet, §2-13 Sikring av integritet og Helsepersonelloven §§13, 16.

- *Hva skal sjekkes og hvordan?*
  Om virksomheten har rutiner for sikker kassasjon av gammelt IKT-utstyr, bruk av flyttbare lagringsmedier, makulering av papir, sikker sletting av data for spesielt utstyr for eks. SCSI-disker, sikring av at utskrift av sensitive opplysninger behandles på en forsvarlig måte og om ansatte bevisstgjøres om slike ting og konsekvensene av dette.

  Tilgangsstyring er i samsvar med I ISO/IEC 27002:2005 kap. 10.

7.2.5 Hjemmekontor

- *Hva er det?*
  PC på hjemmekontor skal ikke ha lagret informasjon underlagt lovbestemt taushetsplikt. Slik informasjon skal kunne nås på to måter:
  Enten ved oppkobling til sentralt lagrede data (i virksomheten og/eller hos databehandler), kommunikasjonen skal da være kryptert, (f. eks gjennom VPN som er en lukket og reservert kommunikasjonskanal som kan krypteres), eller via en kryptert bærbar maskin som ikke kan kobles til internett, og hvor data kun kan hentes ut til

kryptere USB disker (USB-pinner). Dokumentene kan da forflyttes på en sikker måte mellom hjem og arbeidsplass.

- *Hvorfor er dette området viktig?*
  Dette området er viktig fordi det er avgjørende å hindre uautorisert adgang, bruk og tilgang til utstyr og data benyttet for behandling av helse- og personopplysninger på et hjemmekontor dersom dette ikke skjer på en sikker måte.

  Lovhjemmel:
  Personopplysningsforskriftens §2-10 Fysisk sikring,§2-11 Sikring av konfidensialitet, §2-12 Sikring av tilgjengelighet og §2-13 Sikring av integritet.
  Hjemmekontor er i samsvar med I ISO/IEC 27002:2005 kap. 9, 10 og 11.

- *Hva skal sjekkes og hvordan?*
  Om virksomheten bruker hjemmekontorløsning for sine ansatte, i så fall hvilken type de har og hvordan påloggingen og sikring av dataene foregår.

7.2.6 Opplæring av ledere og medarbeidere

- *Hva er det?*
  Arbeidsgiver må gi nye arbeidstaker en innføring i virksomhetens sikkerhetskrav og rutiner slik at den ansatte forstår hvilke oppgaver og plikter han/hun har. Dette må også skje ved endring eller innføring av nytt system, og være en kontinuerlig aktivitet. Aktuelle lover og forskrifter samt interne krav må være lett tilgjengelig for medarbeiderne, helst gjennom et intranett. Sikkerhetskultur må innarbeides gjennom systematiske program for bevisstgjøring. Her må alle ansatte, også ledere, involveres. Ledere må gå foran som et godt eksempel.

- *Hvorfor er dette området viktig?*
  Formålet med opplæring i informasjonssikkerhet er å gi virksomhetens medarbeidere kompetanse slik at de kan ivareta et godt og hensiktsmessig personvern etter gjeldene krav slik at de forstår ansvarsforholdet i forhold til informasjonssikkerhet. Det kan ha store konsekvenser dersom en ansatt ikke ble opplært kontinuerlig på gjeldende regler og rutiner.

  Lovhjemmel: Personopplysingsforskriften §2-8 Personell

- *Hva skal sjekkes og hvordan?*
  Det skal sjekkes om virksomheten har en plan for opplæring og bevisstgjøring innen informasjonssikkerhet for sine ansatte. Får alle ansatte opplæring om betydningen av informasjonssikkerhet ved endring eller innføring av nytt system?

7.2.7 Kontinuitetsplan

- *Hva er det?*
  Kontinuitetsplanen skal sørge for at virksomheten kan opprettholde sin virksomhet på kort og lang sikt. Viktige punkter i denne fasen at den skaper trygghet, sørger for stabilitet og tigjengelighet.

- *Hvorfor er dette området viktig?*
  Manglende kontinuitetsplanlegging kan medføre avbrudd i forretningsaktivitetene og kritiske driftsprosesser.

  Lovhjemmel: Personopplysingsforskriften §2-12 Sikring av tilgjengelighet
  Hjemmekontor er i samsvar med I ISO/IEC 27002:2005 kap. 14.

- *Hva skal sjekkes og hvordan?*

Virksomheten må ha utarbeidet en egen kontinuitetsplan på IKT-området. Om virksomheten vurdert konsekvensen av evt. driftsbrudd? Om de har etablert en prosess for oppdatering?

8 Konklusjon

Jeg har samlet inn data gjennom flere kilder bl.a. intervjuer med ledelse i Statens helsetilsyn, ledere i andre tilsynsorganer, spørreundersøkelse, rundspørring på telefon og skriftlige materialer fra det offentlige. Det er betydelige utfordringer innen Helsetilsynets ansvarsområde. Basert på dette er det blitt foreslått tiltak for å håndtere disse utfordringene. Funnene viser at behovet for kompetanseheving innen informasjonssikkerhet hos tilsynsførere er veldig stor.
Jeg kan slå fast at informasjonssikkerhet ikke har hatt en selvstendig plass som vurderingstema i Helsetilsynets systemrevisjoner. I og med at konfidensialit- , integritet-, og tilgjengelighetssikring er sentrale elementer i informasjonssikkerhet, bør Helsetilsynets tilsynsførere har gode kjennskap til teknologimuligheter for disse elementene.
På lang sikt bør tenkes på et forenklet IT- tilsyn som dekker informasjonssikkerhet i den grenseflaten til pasientbehandlerteknologi.

Prosjektet var vellykket og det har skapt stort engasjement i virksomheten, og det anbefales at det gjøres et oppfølgingsprosjekt som kan bidra til integrering av informasjonssikkerhet inne i Helsetilsynets systemrevisjon.

Bibliography

[1] Cobit 4.1 handbook,isaca.org. http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx, siste besøkt 10.05.2010.

[2] Datatilsynets hjemmeside. http://www.datatilsynet.no/, siste besøkt 25.05.2010.

[3] En veiledning om internkontroll og informasjonssikkerhet utgitt av datatilsynet, november 2009. http://www.datatilsynet.no/upload/Veileder_Datatilsynet_WEB.pdf, siste besøkt 29.05.2010.

[4] Finanstilsynets nettside. http://www.finanstilsynet.no, siste besøkt 23.05.2010.

[5] Helsedirektoratets hjemmeside. http://www.shdir.no/, siste besøkt 25.05.2010.

[6] Høring av forslag til forskrift om informasjonssikkerhet, tilgangsstyring og tilgang til helseopplysninger i behandlingsrettede helseregistre. http://www.regjeringen.no/nn/dep/hod/dok/hoeringer/hoeringsdok/2010/Horing-av-forslag-til-forskrift-om-informasjonssikkerhet-tilgangsstyring-og-tilgang-html?id=604368,siste besøkt 29.05.2010.

[7] It-revisjon fra med fokus på sikkerhetsrevisjon utgitt av kith. http://www.kith.no/upload/1067/R22-02Revisjon.pdf, siste besøkt 29.05.2010.

[8] Itil website. http://www.itil-officialsite.com/home/home.asp, siste besøkt 29.06.2010.

[9] Kompetansekrav for bruk av ikt i helse- og omsorgssektoren, utgitt av kith. http://www.kith.no/upload/5486/Kompetansekrav-for-bruk-av-IKT-i-helse-omsorg_v08.pdf,siste besøkt 29.05.2010.

[10] Lovdatas hjemmeside. http://www.lovdata.no/, siste besøkt 25.06.2010.

[11] Nasjonal sikkerhetsmyndighets hjemmeside. http://www.nsm.stat.no/, siste besøkt 25.05.2010.

[12] National institute of standards and technologi website. http://csrc.nist.gov/, siste besøkt 29.06.2010.

[13] Norm for informasjonssikkerhet i helsesektoren utgitt av shdir. http://www.helsedirektoratet.no/samspill/informasjonssikkerhet/norm_for_informasjonssikkerhet_i_helsesektoren_232354, siste besøkt 20.05.2010.

[14] Norsk helsenett sf strategi, høringsutkast utgitt av norsk helsenett sf, utgitt 29.02.2010. http://www.nhn.no/Strategi%20Norsk%20Helsenett%20SF%20-%20hoeringsutkast.doc,siste besøkt 29.05.2010.

[15] Risikoanalyse - metodegrunnlag og bakgrunnsinformasjon, utgitt av kith den 08.09.2000. http://www.kith.no/upload/995/R13-00Risikoanalyse-v1.pdf, siste besøkt 29.05.2010.

[16] Risikovurdering av informasjonssystem med utgangspunkt i forskrift til personopplysningsloven, utgitt av datatilsynet den 15.02.2002. http://www.datatilsynet.no/upload/Dokumenter/infosik/veiledere/Risikovurdering_TV-506_02.pdf, siste besøkt 29.05.2010.

[17] Sviktende tilgangsstyring i elektroniske pasientjournaler, utgitt av datatilsynet i april 2009. http://www.datatilsynet.no/upload/Ttilgang%20på%20tvers_270409.pdf, siste besøkt 25.05.2010.

[18] Tilsynsmelding 2006, utgitt av statens helsetilsyn i mars 2007. http://www.helsetilsynet.no/upload/Publikasjoner/tilsynsmelding/tilsynsmelding2006.pdf, siste besøkt 22.06.2010.

[19] Veileder i personvern og informasjonssikkerhet for helse- og sosialtjenester i kommuner, versjon 1.0, ugitt av shdir. http://www.helsedirektoratet.no/vp/multimedia/archive/00171/Veileder_i_personve_171309a.pdf, siste besøkt 29.05.2010.

[20] Veiledning i risiko- og sårbarhetsanalyse ros, utgitt av nasjonal sikkerhetsmyndighet i 2006. https://www.nsm.stat.no/Documents/Veiledninger/ROS_2004_veiledning.pdf, siste besøkt 29.05.2010.

[21] Veiledning i sikkerhetsadministrasjon, utgitt av nasjonal sikkerhetsmyndighet i 2006. https://www.nsm.stat.no/Documents/Veiledninger/Grunnlagsdokument-%20sikkerhet.pdf, siste besøkt 29.05.2010.

[22] Veiledning lover og regler med betydning for informasjonssikkerhet, versjon 1.2, utgitt av it-sikkerhetsforum, desember 2008. https://www.nsm.stat.no/Documents/KIS/Publikasjoner/ISF%20-%20Veiledning%20lover%20og%20regler%20v1.2.pdf, siste besøkt 29.06.2010.

[23] Veiledning til ğ 5-1 gjennomføring av konfigurasjonskontroll, utgitt av nasjonal sikkerhetsmyndighet i 2002. https://www.nsm.stat.no/Documents/Veiledninger/Veiledning_i_Konfigurasjonskontroll_v2_0.pdf, siste besøkt 29.05.2010.

[24] NIST Special Publication 800-30. Risk management guide for information technology systems, july 2002.

[25] ENISA ad hoc working group on risk assessment and risk management. Risk assessment and risk management methods,version 1.0, deliverable 2,30.03.2006. http://www.enisa.europa.eu, siste besøkt 22.06.2010.

[26] W.G. Bornman and L. Labuschagne. A comparative framework for evaluating information security risk management methods, april 2004.

[27] Torgeir m.fl Daler. Håndbok i datasikkerhet - informasjonsteknologi og risikostyring. tapir akademisk forlag, trondheim, 2002.

[28] K. Dunn. Chapter 6: Interviewing. qualitative research methods in human geography, second edition, edited by ian hay. south melbourne, vic.: Oxford university press, 2005.

[29] ENISA. Management: Implementation principles and inventories for risk management/risk assessment methods and tools. Technical report, European Network and Information Security Agency (ENISA), June 2006.

[30] M. Evans. Chapter 11: Participant observation: The researcher as research tool.qualitative methods in human geography, edited by: John eyles and david m. smith.cambridge: Polity press. 1998.

[31] Fra ISOs hjemmeside. http://www.iso.org, siste besøkt 10.06.2010.

[32] Paul D. Hockel. Implementing itil across contrasting organizational structures,university of maryland university college,december 2009. http://faculty.ed.umuc.edu/~sdean/ProfPaps/Bowie/F09/Hockel.pdf, siste besøkt 22.06.2010.

[33] I. M. Holme and B. K Solvang. "metodevalg og metode bruk", tano, otta, 1996.

[34] ISACA. The risk it framework excerpt, utgitt 2009. https://www.isaca.org/Knowledge-Center/Research/Documents/RiskIT-FW-Excerpt-8Jan09.pdf, siste besøkt 22.06.2010.

[35] Mehari overview april 2010. http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Overview.pdf, siste besøkt 22.06.2010.

[36] Jason E. Stamp Philip L. Campbell. Sandia report, sand2004-4233, a classification scheme for risk assessment methods,august 2004. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5888&rep=rep1&type=pdf, siste besøkt 22.06.2010.

[37] Artur Rot. Enterprise information technology security: Risk management perspective, 2009. http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1171-1176.pdf, siste besøkt 22.06.2010.

[38] M.N.K. m.fl Saunder. Research methods for business students, pentice hall, london, 2000.

[39] Bruno Celso C. de Freitas Sofia C. Marçal. Mapping cmmi project management process areas to scrum practices, 2007. http://www.cesar.org.br/files/file/SCRUMxCMMMI_IEEE-final03.pdf, siste besøkt 23.06.2010.

[40] Basie Von Solms. Information security governance: Cobit or iso 17799 or both? computers and security,2005 24, 99-100.

[41] Norsk standard NS-ISO/IEC 27002:2005. Informasjonsteknologi sikkerhet administrasjon av informasjonssikkerhet.

[42] T. Thagaard. "systematikk og innlevelse. en innføring i kvalitativ metode" fagbokforlaget, bergen,1998.

[43] Gill. Valentine. Chapter 7: Tell me about: using interviews as a research methodology. methods in human geography, a guide for students doing a research project, second edition. edited by robin flowerdale and david martin. harlow: Pearson/prentice hall. 2005.

[44] Anita Vorster and Les Labuschagne. A framework for comparing different information security risk analysis methodologies, 2005.

[45] K Widerberg. Historien om et kvalitativt forskninsprosjekt. universitetsforlaget, oslo.

[46] Emmanuele Zambon1 and Sandro Etalle. Architecture-based qualitative risk analysis for availability of it infrastructures, university of twente, june 20, 2009.

A Utdrag av lovverket

A.1 LOV 2001-05-18 nr 24: Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)

§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. Tilgang kan bare gis i den grad dette er nødvendig for vedkommendes arbeid og i samsvar med gjeldende bestemmelser om taushetsplikt. Kongen i Statsråd kan i forskrift gi nærmere bestemmelser om tilgang til helseopplysninger. Forskriften kan for tilgang til helseopplysninger i behandlingsrettede helseregistre gjøre unntak fra første ledd første punktum. Tilgang til helseopplysninger i behandlingsrettet helseregister på tvers av virksomheter kan bare gis etter uttrykkelig samtykke fra den registrerte. Kongen i Statsråd kan i forskrift gjøre unntak fra kravet om uttrykkelig samtykke i tredje ledd, jf. §2 nr. 11. Én forespørsel om og tilgang til helseopplysninger i annen virksomhet kan bare omfatte én pasient om gangen. Den registrerte har rett til innsyn i logg fra behandlingsrettet helseregister om hvem som har hatt tilgang til helseopplysninger om ham eller henne. Endret ved lov 19 juni 2009 nr. 68.

§13a. Forbud mot urettmessig tilegnelse av helseopplysninger

Det er forbudt å lese, søke etter eller på annen måte tilegne seg, bruke eller besitte helseopplysninger som behandles etter denne loven uten at det er begrunnet i helsehjelp til pasienten, administrasjon av slik hjelp eller har særskilt hjemmel i lov eller forskrift.
Tilføyd ved lov 9 mai 2008 nr. 34 (i kraft 9 mai 2008 iflg. res. 9 mai 2008 nr. 442).

§14. Utlevering av helseopplysninger

Helseopplysninger kan utleveres eller overføres for sammenstilling som er tillatt etter ǧ 12. Sammenstilte helseopplysninger kan, etter at navn og fødselsnummer er fjernet, utleveres eller overføres til en virksomhet som bestemt av departementet, når formålet er å avidentifisere eller å anonymisere opplysningene.
Helseopplysninger kan dessuten utleveres eller overføres når utlevering eller overføring har hjemmel i eller i medhold av lov, og den som mottar opplysningene har adgang til å behandle dem etter personopplysningsloven.

§15. Taushetsplikt

Enhver som behandler helseopplysninger etter denne lov, har taushetsplikt etter forvaltningsloven §§13 til 13e og helsepersonelloven.
Taushetsplikten etter første ledd gjelder også pasientens fødested, fødselsdato, personnummer, pseudonym, statsborgerforhold, sivilstand, yrke, bopel og arbeidssted. Opplysninger til andre forvaltningsorganer etter forvaltningsloven §13 b nr. 5 og 6 kan bare gis når det er nødvendig for å bidra til løsning av oppgaver etter loven her, eller for å

forebygge vesentlig fare for liv eller alvorlig skade for noens helse.
Taushetsplikt er likevel ikke til hinder for utlevering av opplysninger om en pasient skal betale egenandel til helsepersonell eller andre som gir helsehjelp til pasienten eller yter andre tjenester til pasienten som folketrygden er stønadspliktig for. Taushetsplikt er heller ikke til hinder for utlevering av slike opplysninger til helseforetakene i forbindelse med oppgjør for syketransport.
Opplysninger om en pasients navn, transportbehov og om pasienten skal betale egenandel og eventuelt beløpet kan gis til transportør i forbindelse med transport som omfattes av spesialisthelsetjenesteloven §2-1a første ledd nr. 6.
Endret ved lov 18 des 2009 nr. 137 (i kraft 1 jan 2010 iflg. res. 18 des 2009 nr. 1583).

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

Den databehandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet, kvalitet og tilgjengelighet ved behandling av helseopplysninger.
For å oppnå tilfredsstillende informasjonssikkerhet skal den databehandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den databehandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.
En databehandlingsansvarlig som lar andre få tilgang til helseopplysninger, for eksempel en databehandler eller andre som utfører oppdrag i tilknytning til informasjonssystemet, skal påse at disse oppfyller kravene i første og annet ledd. Kongen kan gi forskrift om sikkerhet ved behandling av helseopplysninger etter denne lov. Kongen kan herunder sette nærmere krav til elektronisk signatur, kommunikasjon og langtidslagring, om godkjenning (autorisasjon) av programvare og om bruk av standarder, klassifikasjonssystemer og kodeverk, samt hvilke nasjonale eller internasjonale standardsystemer som skal følges.

§17. Internkontroll

Den databehandlingsansvarlige skal etablere og holde vedlike planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i eller i medhold av denne loven, herunder sikre helseopplysningenes kvalitet.
Den databehandlingsansvarlige skal dokumentere tiltakene. Dokumentasjonen skal være tilgjengelig for medarbeiderne hos den databehandlingsansvarlige og hos databehandleren. Dokumentasjonen skal også være tilgjengelig for tilsynsmyndighetene.
Kongen kan i forskrift gi nærmere regler om internkontroll.

§18. Databehandlers rådighet over helseopplysninger

En databehandler kan ikke behandle helseopplysninger på annen måte enn det som er skriftlig avtalt med den databehandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse. I avtalen med den databehandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av §16.

A.2 FOR 2000-12-15 nr 1265: Forskrift om behandling av personopplysninger (personopplysningsforskriften)

Kapittel 2. Informasjonssikkerhet

§2-1. Forholdsmessige krav om sikring av personopplysninger

Reglene i dette kapittelet 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.

§2-2. Pålegg fra Datatilsynet

Datatilsynet kan gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

§2-3. Sikkerhetsledelse

Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges.
Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål.
Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.
Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.

§2-4. Risikovurdering

Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.
Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og §2-2.
Resultatet av risikovurderingen skal dokumenteres.

§2-5. Sikkerhetsrevisjon

Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig. Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.
Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. §2-6.
Resultatet fra sikkerhetsrevisjon skal dokumenteres.

§2-6. Avvik

Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd, skal behandles som avvik.
Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.
Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.
Resultatet fra avviksbehandling skal dokumenteres.

§2-7. Organisering

Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.
Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.
Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.
Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.
Bruk av informasjonssystemet som har betydning for informasjonssikkerheten, skal utføres i henhold til fastlagte rutiner.

§2-8. 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.

§2-9. Taushetsplikt

Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.

§2-10. Fysisk sikring

Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her.
Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten.
Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.

§2-11. 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.
For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte.
Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet.

§2-12. 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.

§2-13. 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.

§2-14. 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. Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.
Sikkerhetstiltak skal dokumenteres.

§2-15. Sikkerhet hos andre virksomheter
Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.
Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register. Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet.

Den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale.
Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikas-

jonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

§2-16. Dokumentasjon

Rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.
Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.
Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten.

Kapittel 3. Internkontroll

§3-1. Systematiske tiltak for behandling av personopplysninger

Den behandlingsansvarlige skal etablere internkontroll i samsvar med personopplysningsloven §14. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang det er nødvendig for å etterleve krav gitt i eller i medhold av personopplysningsloven, med særlig vekt på bestemmelser gitt i medhold av personopplysningsloven §13.
Internkontroll innebærer at den behandlingsansvarlige blant annet skal sørge for å ha kjennskap til gjeldende regler om behandling av personopplysninger, tilstrekkelig og oppdatert dokumentasjon for gjennomføring av de ovenstående rutiner, samt ha denne dokumentasjonen tilgjengelig for de den måtte angå.
Den behandlingsansvarlige skal også ha rutiner for oppfyllelse av sine plikter og de registrertes rettigheter etter det til enhver tid gjeldende personvernregelverk, herunder ha rutiner for
a) innhenting og kontroll av de registrertes samtykke, jf. personopplysningloven §§8, 9 og 11,
b) vurdering av formål med behandling av personopplysninger i samsvar med personopplysningsloven §11 bokstav a,
c) vurdering av personopplysningenes kvalitet i forhold til det definerte formålet med behandling av opplysningene, jf. personopplysningsloven §§11 bokstav d og e, 27 og 28, samt oppfølging av eventuelle avvik,
d) oppfyllelse av begjæringer om innsyn og informasjon, jf. personopplysningsloven §§16 til 24,
e) oppfyllelse av krav fra den registrerte om reservasjon mot visse former for behandling av personopplysninger, jf. personopplysningsloven §§25 og 26,
f) oppfyllelse av personopplysningslovens regler om melde- og konsesjonsplikt, jf. personopplysningsloven §§31 til 33.

Databehandlere som behandler personopplysninger på oppdrag fra behandlingsansvarlige, skal behandle opplysningene i samsvar med rutiner behandingsansvarlige har oppstilt.

B Spørreskjema sendt alle Helsetilsynet i fylkene

Helsetilsynet i fylket v/fylkeslegen

Jf. epost fra assisterende direktør Geir Sverre Braut av 22. februar 2010. Etter helseregisterloven §31 er det Datatilsynet som har hovedoppgavene knyttet til tilsyn med helsetjenestens etterlevelse av kravene i helseregisterloven. Men Statens helsetilsyn og Helsetilsynet i fylket kan i forbindelse med planlagt tilsyn, behandling av tilsynssaker og behandling av klagesaker etter pasientrettighetsloven komme over opplysninger om forhold som må vurderes opp mot kravene i helseregisterloven, enten av Helsetilsynet selv, eller ved oversendelse til Datatilsynet.

Statens helsetilsyn er kjent med at mange har ytret ønske om en økt kompetanse når det gjelder vurdering av sikkerhet, risiko og funksjonalitet i systemer for elektronisk pasientjournal og pasientadministrative systemer.
For å få et mer systematisk grunnlag for å vurdere behovet for kompetanseoppbygging og eventuelt også utarbeide praktiske hjelpemidler til bruk ved vurderingen av slike systemer, ønsker vi svar på spørsmålene nedenfor.
Spørsmålene er konsentrert om emneområder som er sentrale for å forstå og vurdere sikkerhet i informasjonssystemer. De har sitt utgangspunkt dels i kravstrukturen i personopplysningsloven med forskrifter og helseregisterloven, dels i de tematiske tilnærmingene som for eksempel Riksrevisjonen og Datatilsynet bruker i sitt arbeid.
Vi ber om å få tilbake ett skjema fra hvert kontor. Dersom det er ønskelig kan fritekstkommentarer gis etter hvert spørsmål, eller til slutt i skjemaet.
Vi trenger ikke opplyst på skjemaet hvem som har svart på kontorets vegne eller hvilket kontor skjemaet kommer fra. Det vil ikke bli gjort noen sammenligninger mellom kontorene med utgangspunkt i dette datamaterialet. (Vi satser på god oppslutning i første runde, og kommer ikke til å sende noen purring.)

Svarene sendes til Ali Barzinje på e-post (abz@helsetilsynet.no) så snart som mulig og helst innen 8. mars 2010.

Det første settet med spørsmål er relatert til opplevde utfordringer i tilsynsarbeidet. Det andre settet er relatert til kompetanse og opplevd behov for kompetanseøkning.

Vi regner ikke med at noen har eksakte, dokumenterbare data å vise til, så vi er godt fornøyd med svar som bygger på kvalifisert synsing!

Med hilsen

Geir Sverre Braut Ali Barzinje

Opplevde utfordringer i tilsynsarbeidet

Hvor ofte opplever Helsetilsynet i fylket at det forekommer saker/forhold i tilsyns- og forvaltningsarbeider der man må vurdere:

		Aldri vært aktuelt	Sjelden (~årlig)	Hyppig (>månedlig)
1	Skade/tapspotensialet ved feil/uhell knyttet til informasjonssikkerhet i helsetjenesten			
2	Virksomhetens policy informasjonssikkerhet			
3	Virksomhetens organisering av informasjons-sikkerhetsarbeidet			
4	Opplæring av ansatte i informasjonssikkerhet			
5	Personellsikkerhet, autorisasjon av tilgang			
6	Oppfølgende kontroll av tilgang til innhold i IT-systemer			
7	Fysisk sikring av infrastruktur og datautstyr			
8	Sikkerhet i grenseflaten mellom ulike soner i IT-systemet (f.eks. pasientjournal og administrative systemer)			
9	Avbruddstrygghet			
10	Virksomhetens oppfølging av brudd på lovkrav eller interne krav til informasjonssikkerhet			

Figure 7: Kartlegging av utfordringer i tilsynsarbeid

Kommentarer:

Kompetanse og opplevd behov for kompetanseøkning

Hvordan opplever Helsetilsynet i fylket sin egen kompetanse når det gjelder tilsynsmessig vurdering av:

		Ingen kompetanse	Bør bli bedre	Tilfredsstillende kompetanse
1	Skade/tapspotensialet ved feil/uhell knyttet til informasjonssikkerhet i helsetjenesten			
2	Virksomhetens policy informasjonssikkerhet			
3	Virksomhetens organisering av informasjons-sikkerhetsarbeidet			
4	Opplæring av ansatte i informasjonssikkerhet			
5	Personellsikkerhet, autorisasjon av tilgang			
6	Oppfølgende kontroll av tilgang til innhold i IT-systemer			
7	Fysisk sikring av infrastruktur og datautstyr			
8	Sikkerhet i grenseflaten mellom ulike soner i IT-systemet (f.eks. pasientjournal og administrative systemer)			
9	Avbruddstrygghet			
10	Virksomhetens oppfølging av brudd på lovkrav eller interne krav til informasjonssikkerhet			

Figure 8: Kartlegging av opplevd behov for kompetanseøkning

Kommentarer:

C Oversikt over intervjuobjekter

1. Intervju med erfaren tilsynsfører som har ledet en rekke av kontrollene innen helse- og sosialsektoren i Datatilsynet den 25.03.2010.

2. Intervju med tilsynsrådgiver i Finanstilsynet den 22.04.2010.

3. Telefonintervju med ledere i de fem største Helsetilsynet i fylket, og et mindre kontor, i perioden 15.04 til 20.04.2010.

4. Intervju med assisterende helsedirektør i Statens helsetilsyn den 04.05.2010.

D Intervjuguide for intervju med erfaren tilsynsfører i Datatilsynet

Tilsynsføreren har ledet en rekke av kontroller innen helse- og sosialsektoren

1. Først presentasjon av meg, min oppgave og formålet.
2. Kan du si litt om din organisasjon, dens oppgaver, din stilling og dine oppgaver her, hvor lenge har du jobbet her? Din erfaring med helse- og sosialsektor? Hvor mange ganger du var på tilsynsbesøk ?
3. Kan du forklare ansvarsdeling/arbeidsdeling mellom Statens helsetilsyn og Datatilsynet?
4. Dere har vært sammen med hverandre i er par tilsyn i sykehusene som ble utført for 3-4 år siden? Hvorfor sluttet dere å jobbe sammen?
5. Hva er forventningene Datatilsynet har til Helsetilsynet, ikke bare oss sentralt, men også Helsetilsynet i fylkene?
6. Kan du si litt om tilsynsprosessen og i hvor stor grad informasjonssikkerhet er integrert i den?
7. Opplever Datatilsynet at det er nok kompetanse/bevisstgjøring hos ansatte i Helsetilsynet i fylkene ift. tilgang, Personopplysninger, Helseregisterloven osv.? Hva bør Helsetilsynet gjøre for å forbedre dette?
8. Datatilsynets krav til tjenestene?
9. Datatilsynets fortolkning av loven?
10. Hva er de sentrale IT-truslene som alle må ha beredskap for, i følge Datatilsynets erfaring?
11. Kan du si litt om Datatilsynets systemrevisjon, om den inneholder IT-tilsyn?
12. På hvilken måte vurderer Datatilsynet spørsmålet om virksomhetenes risikoanalyser er gode nok?

E Kartlegging av kompetanse innenfor informasjonssikkerhet ved et utvalg av fylker

Telefonintervju:

0. Innledningsvis ble formålet kort forklart, jf. ovenstående.

1. Spørsmål 1: Hvor mange personer (ikke årsverk) er involvert i planlagt tilsyn (systemrevisjoner) med helsetjenestene?

2. Spørsmål 2: Hvor mange av disse har gjennomgått opplæring innenfor informasjonssikkerhet (kurs, seminarer, studier eller lignende)?

3. Spørsmål 3: Får ansatte ved kontoret annen opplæring eller bevisstgjøring innenfor informasjonssikkerhet (ut over det som er nødvendig for ivaretakelsen av interne rutiner og systemer (ePhorte, taushetsplik etter forvaltningsloven)?

Table 1: Resultat fra telefonrundspørring

Fylke	1.	2.	3.	4.	5.	6.
Intervjuet	Fl. 15.4	Fl. 16.4	Fl. 15.4	Fl. 15.4	Fl. 15.4	Fl. 16.4
Spørsmål 1	6	11	10	13	12	18
Spørsmål 2	0	0	0	0	0	2 *
Spørsmål 3	Nei **	Nei ***	Nei	Nei ****	Nei	Nei

* To ansatte deltar i mastergradsutdanning i samfunnssikkerhet og er skolert i risikoanalyse.

** Har deltatt på fellestilsyn med Datatilsynet og lært mye av det.

*** Har hatt tilsyn fra Datatilsynet på egne systemer og lærte mye av det.

**** Har juridisk saksbehandler med høy kompetanse på regulering av informasjonssikkerhet.

F Intervjuguide for intervju med en tilsynsrådgiver i Finanstilsynet

1. Presentere meg, min oppgave og formålet.
2. Kan du si litt om din organisasjon, dens oppgaver, din stilling og dine oppgaver her, hvor lenge har du jobbet her? Hvor mange ganger du har vært på tilsynsbesøk?
3. Kan du si litt om tilsynsprosessen? Helt fra begynnelsen til slutten?
4. Bl. Oppgavene som du nevnte, var IT-tilsyn, kan du si litt om bakgrunnen, når dere begynte med den og hva slags rammeverk dere bruker?
5. Hvordan bruker dere COBIT i deres arbeid? Dens oppbygging?
6. Er informasjonssikkerhet veldig integrert i deres arbeid? På hvilken måte?
7. Hva har dere funnet ut i deres tilsyn ift. informasjonssikkerhet? og hvordan?
8. Hva er de mest kjente sårbarheter i dette systemet som dere kjører nå? Og hva er de største truslene mot driftssikkerheten?
9. Outsorcing:fører dere IT-tilsyn bare hos tjenestemottakeren eller hos hovedleverandøren også?
10. Når brukeren endrer sitt IT-system eller gjør endringer, hvordan foregår tilsynet?
11. Hva er deres erfaring med COBIT, hva er ulempene med den?
12. Har dere noe dokumentasjon som jeg kan låne og benytte i min oppgave?

G Intervjuguide for intervju med assisterende helsedirektør i Statens helsetilsyn

1. Hvorfor må/bør en tilsynsfører i Helsetilsynets ha kjennskap til informasjonssikkerhet?
2. På hvilken måte betraktes informasjonssikkerhet som en del av Helsetilsynets tilsyn? både praktisk og i regleverket?
3. Jeg etterlyser en gapanalyse med hensyn på kunnskapsnivå om informasjonssikkerhet til tilsynsførere:
   - **3.1** Hvor langt må du bevege deg fra der du er nå, til dit du ønsker å være?
   - **3.2** Hva er minimumskravet med hensyn på kunnskapsnivå innen informasjonssikkerhet?
4. Klargjøre rammene for tilsynsmetode:
   - **4.1** Hva er deres metodekrav for å føre tilsyn?
   - **4.2** Nødvendig kunnskapsnivå for tilsynsførere (10-årig, vg. skole.osv.) Nødvendig tid for å føre et tilsyn. Hvor raskt må et tilsyn være? For eks. budsjettert 20 timers arbeid.
   - **4.3** Nøyaktighet (gyldighet/pålitlighet). Hvor mye unøyaktighet kan komme inn i en tilsynsrapport, for eks. når det gjelder avvik, alvorlige feil?
   - **4.4** Inneholder den metoden som dere gjør nå en bit om informasjonssikkerhet?
5. IT-tilsyn:
   - **5.1** Selv om det er en omfattende og krevende jobb, men på langt sikt og hvis lovverket tillater det, er det aktuelt for Helsetilsynet å gjøre IT-tilsyn for helseforetakene på lik linje som Finanstilsynet gjør?
   - **5.2** Hva må gjøres da? egen IKT-forskrift for Helsetilsynet, egen prosedyre? Nødvendig tid for å føre et tilsyn. Hvor raskt et tilsyn må være? For eks. budsjettert 20 timers arbeid.
   - **5.3** Hvordan kan Helsetilsynet gjøre IT-tilsyn uten at dette påvirker (går ut over) tilsyn med sosial og helse som er kjerneoppgaven til Helsetilsynet?
   - **5.4** På hvilken måte kan et IT-tilsyn gå i retning av å styrke tilsynet med sosial og helse?
6. Alternativer:
   - **6.1** Hvis IT-tilsyn ikke blir aktuelt, hva kan alternativet være særlig med tanke på utviklingen og at risikoene innen IT og informasjonssikkerhet er store? Hvordan kan tilsynsførere gjøre tilsyn med nåværende kunnskap om informasjonssikkerhet? Betyr dette at retningslinjer for Systemrevisjonen må skrives på nytt slik at de kan inneholde en egen del om informasjonssikkerhet?

6.2 jf. spørsmålet i 4.1, Kan en sjekkliste for tilsynsførere om IS og en veiledning i bruk av den, være aktuelt?

6.3 Er det aktuelt å dele tilsynet i to deler, en helsefaglig , som utføres av helsefaglige personer, og en basert på IS, som utføres av de som har kunnskap innen informasjonssikkerhet?

7. Er det andre måter enn det som er nevnt i spørsmålene 6.1, 6.2 og 6.3 aktuelt for Helsetilsynet å gjøre tilsyn med tanke på mer dekkende innen informasjonssikkerhet?
8. Helsetilsynet og Datatilsynet:

   8.1 Dere og Datatilsynet gjorde felles tilsyn med A-hus og Helse Bergen i 2005 og 2006. Hva sier deres erfaring om disse tilsynene?

   8.2 I en undersøkelse som er gjort pr. telefon, viste det seg at en del ansatte som var sammen med Datatilsynet på tilsyn i fylkene, har fått mye nytte av den kompetansen DT har. Syns du at Helsetilsynets tilsynsfører lærer noe fra Datatilsynet ang. informasjonssikkerhet når dere går sammen?

   8.3 For å kunne bruke tverrfaglig kompetanse mellom Helsetilsynet og Datatilsynet, og for ikke å bli stilt opp mot hverandre: Har dere størst behov for å være synkronisert overfor hverandre når det gjelder tilgangsstyring, spesielt §13, hvor taushetspliktbestemmelsen møter sikkerhetsbestemmelsene?

   8.4 Datatilsynet uttrykte seg positivt når det gjelder å jobbe med Helsetilsynet. Er det ikke bedre at dere gjøre tilsyn sammen? Hvorfor sluttet dere å gjøre felles tilsyn? Er det regleverket som setter grense for dette?

9. Avslutning:

   9.1 Hvordan kan kompetansen innen informasjonssikkerhet heves hos Helsetilsynets tilsynsførere?

   9.2 Hvor mange tilsyn fører dere pr. år til sammen på landsbasis?

   9.3 Hvor mange personer er involvert i tilsyn (tilsynsførere) har Helsetilsynet og fylkene?

H Utviklet sjekkliste

(1) Styringssystem for informasjonssikkehet

1. Har virksomheten et ledelsessystem for informasjonssikkerhet?
   JA [ ] Nei [ ]
   Kommentar

2. Har virksomheten en sikkerhetspolicy/håndbok (typisk innhold bør være: en definisjon av informasjonssikkerhet, dens mål og omfang, og betydningen av sikkerhet for å muliggjøre deling av informasjon og en kort redegjørelse for sikkerhetsreglene, prinsippene, standardene og forpliktelsene som er av særlig betydning for organisasjonen)?
   JA [ ] Nei [ ]
   Kommentar

3. Er sikkerhestspolicy/Håndbok godkjent av ledelsen og forankret i organisasjonen?
   JA [ ] Nei [ ]
   Kommentar

4. Blir feil og avvik avdekket ved gjennomgang av internkontrollen, som kan medføre risiko, rapportert til ledelsen?
   JA [ ] Nei [ ]
   Kommentar

5. Er det foretatt internkontroll med utgangspunktet i et Styringssystem?
   JA [ ] Nei [ ]
   Kommentar

6. Er ansvarlig oppnevnt for de enkelte systemer og applikasjoner?
   JA [ ] Nei [ ]
   Kommentar

7. Finnes det risikovurdering ift. Sikring av konfidensialitet?
   JA [ ] Nei [ ]
   Kommentar

8. Finnes det risikovurdering ift. Sikring av tilgjengelighet?
   JA [ ] Nei [ ]
   Kommentar

9. Er det klart definert hvilke konsekvenser brudd på retningslinjer og rutiner kan gi?
   JA [ ] Nei [ ]
   Kommentar

(2) Risikovurdering

10. Finnes det risikovurdering i tilknytning til IT-systemene?
    JA [ ] Nei [ ]
    Kommentar

11. Blir risikoanalysen utført jevnlig?
    JA [ ] Nei [ ]
    Kommentar

12. Er det etablert ved særlige behov (for eks. innføring av ny teknologi, endringer)?
    JA [ ] Nei [ ]
    Kommentar

13. Er det avklart hvilke risikoer som er uakseptable, og som må reduseres med administrative, tekniske eller andre risikoreduserende tiltak?
    JA [ ] Nei [ ]
    Kommentar

14. Har foretaket etablert ansvarsfordeling for gjennomføring og oppfølging av risikoanalysen?
    JA [ ] Nei [ ]
    Kommentar

(3) Sikkerhetsrevisjon

15. Foreligger det driftsdokumentasjon for foretakets IT-løsninger og er det etablert prosedyrer for oppdatering av denne?
    JA [ ] Nei [ ]
    Kommentar

16. Er det etablert prosedyrer som sikrer at installasjon, konfigurasjon og vedlikehold av teknologisk infrastruktur imøtekommer driftssmessige og sikkerhetsmessige krav?
    JA [ ] Nei [ ]
    Kommentar

17. Er ansvarsforholdene knyttet til sikkerhet for driftskontrollsystem entydig plassert i organisasjonen?
    JA [ ] Nei [ ]
    Kommentar

18. Er det utarbeidet prosedyrer som ivaretar konfigurasjonskontroll og oppfølging?
    JA [ ] Nei [ ]
    Kommentar

19. Har virksomheten utarbeidet og implementert en sikkerhetsinstruks for å ivareta informasjonssikerhet?
    JA [ ] Nei [ ]
    Kommentar

(4) Informasjonssikkerhetsbrudd

20. Fungerer avviksbehandling ift. informasjonssikkerhet?
    JA [ ] Nei [ ]
    Kommentar

21. Er det utarbeidet prosedyrer for håndtering av sikkerhetsbrudd/avvikk og som beskriver hva som skal gjøres, for eksempel rapportering, og oppfølging?
    JA [ ] Nei [ ]
    Kommentar

22. Foreligger en prosedyre som sikrer at problemer registreres, analyseres og at nødvendige aksjoner blir avtalt og foretatt?
    JA [ ] Nei [ ]
    Kommentar

23. Gjennomføres det vurderinger av alle registrerte problemer som ledd i forbedringsarbeidet?
    JA [ ] Nei [ ]
    Kommentar

24. Er det etablert rutiner og utpekt ansvar for å håndtere sikkerhetshendelser?
    JA [ ] Nei [ ]
    Kommentar

(5) Sikkerhetskopi (Backup)

25. Er det etablert prosedyre for sikkerhetskopiering?
    JA [ ] Nei [ ]
    Kommentar

26. Tas det daglig backup?
    JA [ ] Nei [ ]
    Kommentar

27. Fungerer avviksbehandling ift. informasjonssikkerhet?
    JA [ ] Nei [ ]
    Kommentar

28. Oppbevares sikkerhetskopier utenfor huset eller i brannnksikret skap?
    JA [ ] Nei [ ]
    Kommentar

29. Har virksomhetene regelmessige testing av restor av dataene?
    JA [ ] Nei [ ]
    Kommentar

30. Er backup-kompetansen lett tilgengelig (internt eller eksternt)?
    JA [ ] Nei [ ]
    Kommentar

31. Inneholder kontinuitetsplanen prosedyrer for back-up og recovery?
    JA [ ] Nei [ ]
    Kommentar

(6) Passordhåndtering

32. Har virksomheten rutiner for passordhåndtering?
    JA [ ] Nei [ ]
    Kommentar

33. Får ansatte opplæring og bevisstgjøring om bruk av passord?
    JA [ ] Nei [ ]
    Kommentar

34. Brukes det skjermbeskytterpassord på alle arbeidsstasjonene?
    JA [ ] Nei [ ]
    Kommentar

(7) Programvare/Antivirus(AV)

35. Gjennomføres testing av nye/endrede IT-løsninger i et relevant testmiljø?
    JA [ ] Nei [ ]
    Kommentar

36. Er patch management for fortløpende håndtering av sårbarheter i operativsystem, tjenester eller applikasjoner som avdekkes, tatt inn som en del av virksomhetens sikkerhetspolicy/-strategi?
    JA [ ] Nei [ ]

Kommentar

37. Er det etablert retningslinjer for etablering, drift og vedlikehold av AV-løsninger?
JA [ ] Nei [ ]
Kommentar

38. Er det etablert retningslinjer som beskriver hvordan den enkelte bruker skal forholde seg til potensielle farer forbundet med ondsinnet kode?
JA [ ] Nei [ ]
Kommentar

39. Benyttes det kun anerkjente løsninger for anti-virus og anti-spam?
JA [ ] Nei [ ]
Kommentar

40. Er det definert hvilke maskiner som skal ha AV-løsning installert og begrunnelse for det?
JA [ ] Nei [ ]
Kommentar

41. Kan AV-løsningene på alle maskiner tvinges til umiddelbar oppdatering fra sentralt punkt i nettverket?
JA [ ] Nei [ ]
Kommentar

42. Har AV-løsningen ulike tilgangsnivåer for endring av konfigurasjon?
JA [ ] Nei [ ]
Kommentar

43. Dersom foretaket benytter IT-tjenester via mobile enheter som mobiltelefon eller PDA, er det etablert AV-løsninger på disse?
JA [ ] Nei [ ]
Kommentar

(8) Bruk av e-mail

44. Er det etablert regler for bruk av e-mail?
JA [ ] Nei [ ]
Kommentar

45. Inneholder reglene rettningslinjer for bruk av e-mail i forbindelse med taushetsbelagte informasjon (for eks. kryptering)?
JA [ ] Nei [ ]

Kommentar

46. Er det lagt inn på serveren sperre for mottak av vedlegg som er av visse fil-typer (extention)?
JA [ ] Nei [ ]
Kommentar

(9) Loggføring og oppfølging

47. Har virksomheten etablert prosedyrer for loggføringer?
JA [ ] Nei [ ]
Kommentar

48. Gjennomføres det jevnlig kontroll/gjennomgang av logger?
JA [ ] Nei [ ]
Kommentar

49. Har virksoheten rutiner for oppbevaring og sletting av loggføringer?
JA [ ] Nei [ ]
Kommentar

50. Er loggene godt beskyttet mot manipulering?
JA [ ] Nei [ ]
Kommentar

(10) Tilgangsstyring

51. Har foretaket retningslinjer for styring av tilgangskontroll (tildeling, endring, avslutning) for de ulike systemer og brukergrupper?
JA [ ] Nei [ ]
Kommentar

52. Er det etablert prosedyrer som ivaretar sikkerhet ved opphør av ansettelsesforhold eller endring av arbeidsoppgaver?
JA [ ] Nei [ ]
Kommentar

53. Bruker virksomheten autorisasjonsskjema ved tildeleing av tilgang?
JA [ ] Nei [ ]
Kommentar

54. Finnes det risikovurdering knyttet til ansattes tilgang til programmet?
JA [ ] Nei [ ]
Kommentar

55. Er det kontroll med all ekstern tilgang til datasystemer?
JA [ ] Nei [ ]
Kommentar

(10) Håndtering av lagringsmedia og Kassasjon

56. Har virksomheten en rutine for kassasjon av gammelt datautstyr?
JA [ ] Nei [ ]
Kommentar

57. Inneholder rutinen hvordan gammelt utstyr som ble brukt for helse- og personopplysninge kasseres?
JA [ ] Nei [ ]
Kommentar

58. Sikkerhetsslettes data på disker (lagringsmedia) før makulering?
JA [ ] Nei [ ]
Kommentar

(11) Hjemmekontor

59. Har dere hjemmekontor løsning for noen ansatte som behandler sensitive data?
JA [ ] Nei [ ]
Kommentar

60. Er det inngått avtale om bruk av hjemmekontor med den enkelte medarbeider som beskriver partenes ansvar?
JA [ ] Nei [ ]
Kommentar

61. Er det etablert retningslinjer som beskriver hvordan hjemmekontormaskiner konfigureres, alternativt at disse maskinene skal konfigureres av IT-drift avdelingen i virksomheten?
JA [ ] Nei [ ]
Kommentar

62. Benyttes VPN for oppkopling til virksomhetens nettverk?
JA [ ] Nei [ ]
Kommentar

63. Er det etablert rutiner for å sikre at PC'er som blir benyttet på utsiden av virksomheten, blir oppdatert med siste versjoner av AV-løsninger og patcher?
JA [ ] Nei [ ]
Kommentar

64. Kan medarbeiderne benytte privat PC i hjemmekontorløsningen?

JA [ ] Nei [ ]
Kommentar

65. Bruker ansatte med hjemmekontor krypterte medier for overføring av data for eks. kryptert minnepinn, krypterte bærbar pc'er?
JA [ ] Nei [ ]
Kommentar

66. Krypteres helse- og personopplysninger som overføres i åpne nett?
JA [ ] Nei [ ]
Kommentar

(12) Opplæring av ledere og medarbeidere

67. Har foretaket etablert et opplæringsprogram for ansatte som inneholder sikkerhetsforståelse?
JA [ ] Nei [ ]
Kommentar

68. Har organisasjonen etablert en opplæringsplan som sikrer at medarbeidere, brukere og IT-personell får tilstrekkelig opplæring ved innføring av nye løsninger?
JA [ ] Nei [ ]
Kommentar

69. Er gjennomgang av retningslinjene for sikkerhet en del av opplæringen til nyansatte?
JA [ ] Nei [ ]
Kommentar

70. Er konsekvenser ved brudd på retningslinjer og rutiner formidlet til alle medarbeidere?
JA [ ] Nei [ ]
Kommentar

71. Gis det spesialopplæring i krisehåndtering for grupper som håndterer krisesituasjoner?
JA [ ] Nei [ ]
Kommentar

72. Har de ansatte fått opplæring i hvordan de skal rapportere mulige sikkerhetsbrudd?
JA [ ] Nei [ ]
Kommentar

(13) Kontinuitetsplan

73. Foreligger det en kontinuitetsplan?
    JA [ ] Nei [ ]
    Kommentar

74. Er det etablert en prosess for oppdatering av kontinuitetsplan?
    JA [ ] Nei [ ]
    Kommentar

75. Er det vurdert eventuelle konsekvenser ved driftsavbrudd?
    JA [ ] Nei [ ]
    Kommentar

76. Foreligger noe plan for tilgang til EPJ-data dersom systemet er ute av drift?
    JA [ ] Nei [ ]
    Kommentar