SINTEF

SINTEF A27272 - Åpen

Rapport

Digitale sårbarheter i helsesektoren – En oppsummering av funn fra workshop holdt i mai 2015 i regi av Lysneutvalget

Forfatter(e)
Aida Omerovic
Erlend Andreas Gjære

SINTEF IKT
2015-06-05

SINTEF

SINTEF IKT

Postadresse:
Postboks 124 Blindern
0314 Oslo

Sentralbord:
Telefaks: 22067350

Foretaksregister:
NO 948 007 029 MVA

Rapport

Digitale sårbarheter i helsesektoren – En oppsummering av funn fra workshop holdt i mai 2015 i regi av Lysneutvalget

EMNEORD:
Helse, digitale sårbarheter, tiltak

VERSJON
2.0

DATO
2015-06-05

FORFATTER(E)
Aida Omerovic
Erlend Andreas Gjære

OPPDRAGSGIVER(E)
Lysneutvalget

OPPDRAGSGIVERS REF.
Lene Bogen Kaland

PROSJEKTNR
102010764

ANTALL SIDER MED VEDLEGG:
34

Sammendrag

Digitalt sårbarhetsutvalg (Lysneutvalget) ble nedsatt av regjeringen den 20. juni 2014. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Lysneutvalget har vært gjennom en fase med informasjonsinnhenting, hvor flere aktører fra helsesektoren har, eller er i ferd med, å bidra med skriftlige innspill.

På bakgrunn av dette ble en rekke aktører med tilknytning til helsesektoren invitert til en workshop for å drøfte sårbarheter innenfor denne sektoren og diskutere effektive tiltak for å møte dagens og fremtidens utfordringer. SINTEF ble av Lysneutvalget engasjert for å bistå med fasilitering av workshopen, som ble avholdt 21. mai 2015 i Oslo med 26 deltakere med tilknytning til sektoren. Programmet bestod av fem innlegg, gruppediskusjoner og plenumsdiskusjoner.

Denne rapporten oppsummerer hovedfunnene fra workshopen med tanke på sårbarheter og tiltak som har blitt påpekt av deltakerne under hele workshopen.

UTARBEIDET AV
Aida Omerovic

SIGNATUR

KONTROLLERT AV
Atle Refsdal

SIGNATUR

GODKJENT AV
Bjørn Skjellaug

SIGNATUR

RAPPORTNR	ISBN	GRADERING	GRADERING DENNE SIDE
SINTEF A27272	9788214059168	Åpen	Åpen

Historikk

VERSJON	DATO	VERSJONSBESKRIVELSE
1.0	2015-05-27	Initielt (internt) utkast sendt til workshop-deltakerne for gjennomlesing og evt. tilbakemeldinger innen 1. juni 2015.
2.0	2015-06-05	Endelig versjon etter innspill fra Lysneutvalget og Ikomm AS.

Innholdsfortegnelse

Forkortelser

BYOD: "Bring your own device"
Difi: Direktoratet for forvaltning og IKT
Epj: Elektronisk pasientjournal
HelseCSIRT: Helsesektorens hendelseshåndtering "Computer Security Incident Response Team"
Hdir: Helsedirektoratet
HF: Helseforetak
HoD: Helse- og Omsorgsdepartementet
IoT: "Internet of things"
KS: Kommunenes sentralforbund
RHF: Regionale helseforetak
ROS: risiko og sårbarhet

Sammendrag

Digitalt sårbarhetsutvalg (Lysneutvalget) ble nedsatt av regjeringen den 20. juni 2014, og er ledet av professor Olav Lysne. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget skal levere sin utredning i form av en NOU til Justis- og beredskapsdepartementet innen utgangen av september 2015. Mandatet er omfattende og spenner over områder som sårbarhet i kritisk infrastruktur og samfunnsfunksjoner, datakriminalitet, personvern og sikring av informasjon.

Lysneutvalget har vært gjennom en fase med informasjonsinnhenting, hvor flere aktører fra helsesektoren har bidratt eller er i ferd med å bidra med skriftlige innspill. På bakgrunn av dette ble en rekke aktører med tilknytning til helsesektoren invitert til en workshop for å drøfte sårbarheter innenfor denne sektoren og diskutere effektive tiltak for å møte dagens og fremtidens utfordringer.

SINTEF ble av Lysneutvalget engasjert for å bistå med fasilitering av workshopen, som ble avholdt 21. mai 2015 i Oslo med 26 deltakere med tilknytning til sektoren. Programmet bestod av fem innlegg som representerte følgende perspektiver: forskning, leverandør til sektoren, helseregion, en kommunes erfaringer fra arbeid med helsetjenester, og myndighetenes arbeid med digitale sårbarheter. I tillegg ble det gjennomført gruppediskusjoner om sårbarheter og tiltak, samt plenumsdiskusjoner.

Denne rapporten oppsummerer hovedfunnene fra workshopen med tanke på sårbarheter og tiltak som har blitt påpekt av deltakerne både under innleggene, under gruppearbeidet samt gjennom plenumsdiskusjonene. Workshopen er gjennomført under Chatham House Rule. Dette medfører blant annet at denne rapporten, med unntak av Vedlegg 1, oppsummerer synspunkter og erfaringer som er nevnt av de ulike deltakerne under workshopen på en måte som ikke relaterer de nevnte sårbarhetene/tiltakene (eller andre funn, synspunkter og erfaringer som presenteres i rapporten) til bestemte deltakere eller virksomheter som har deltatt i eller bidratt til workshopen.

Blant hovedfunnene fra workshopen er at:

- Helsetjenester i fremtiden i stadig støtte grad vil bli utført i tilknytning til hjemmet.
- Det er sannsynlig at offentlig helse- og omsorgssektor vil miste kontroll over deler av den digitale tjenesteleveransen til innbyggerne, blant annet fordi den enkelte bruker selv har råderett hjemme og samtidig tar aktivt initiativ til innføring og bruk av ny teknologi.
- Det vil kreves stor innsats før sentrale systemer med strenge krav til sikkerhet og personvern kan gi tilfredsstillende integrasjon mot infrastruktur i utstyr, applikasjoner og data fra innbyggernes private hjem.
- På veien vil nye sårbarheter introduseres, samtidig som det er fare for at noen gamle vil gjøre seg ytterlig gjeldende.
- Dagens helsesektor karakteriseres av høy grad av avhengighet av IKT tjenester, brukernes forventning til at teknologi blir tatt i bruk, økt grad av tilgjengeliggjøring av systemer, samt fortsatt tilstedeværelse av gamle fagsystemer.
- Det blir stadig mer vanskelig å eliminere risiko, slik at en rekke tiltak er rettet mot håndtering av hendelser, for eksempel redundans, øvelser og beredskap.
- Eksempler på dagens digitale sårbarheter i helsesektoren inkluderer blant annet: redusert tilgjengelighet av IKT systemer, utfordringer med skytjenester, gamle fagsystemer og utstyr utenfor support, svekket personvern, vanskeligheter med tilgangsstyring, manglende beredskap og avhengighet av infrastruktur.
- Eksempler på tiltak som er diskutert inkluderer blant annet: større grad av beredskapsøvelser, opplæring, samarbeid om felles tiltak, samt undervisning og forskning innen helseinformatikk.
- Blant de eksisterende tiltakene som fungerer bra og ønskes videreført, er blant annet følgende nevnt: HelseCSIRT, normen for informasjonssikkerhet og helsenett.

1 Innledning

Digitalt sårbarhetsutvalg (Lysneutvalget) ble nedsatt av regjeringen den 20. juni 2014, og er ledet av professor Olav Lysne. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Utvalget skal levere sin utredning i form av en NOU til Justis- og beredskapsdepartementet innen utgangen av september 2015. Mandatet[1] er omfattende og spenner over områder som sårbarhet i kritisk infrastruktur og samfunnsfunksjoner, datakriminalitet, personvern og sikring av informasjon. Følgende tre punkter representerer et utdrag av utvalgets mandat:

- beskrive de digitale sårbarheter som Norge står overfor i dag og i nærmeste fremtid
- vurdere hvilke konsekvenser denne sårbarheten kan få for enkeltmennesker, næringsliv og samfunnssikkerheten
- se på samarbeid mellom offentlige og private aktører.

Lysneutvalget har vært gjennom en fase med informasjonsinnhenting, hvor flere aktører fra helsesektoren har bidratt eller er i ferd med å bidra med skriftlige innspill. På bakgrunn av dette ble en rekke aktører med tilknytning til helsesektoren invitert til en workshop for å drøfte sårbarheter innenfor denne sektoren og diskutere effektive tiltak for å møte dagens og fremtidens utfordringer.

SINTEF ble av Lysneutvalget engasjert for å bistå med fasilitering av workshopen som ble avholdt 21. mai 2015 i Oslo med 26 deltakere med ulik tilknytning til sektoren. Programmet bestod av fem innlegg som representerte følgende perspektiver: forskning, leverandør til sektoren, helseregion, en kommunes erfaringer fra arbeid med helsetjenester, og myndighetenes arbeid med digitale sårbarheter. I tillegg ble det gjennomført gruppediskusjoner om sårbarheter og tiltak, samt plenumsdiskusjoner.

Denne rapporten sammenfatter og drøfter hovedfunnene fra workshopen med tanke på sårbarheter og tiltak som har blitt påpekt av deltakerne både under innleggene, under gruppearbeidet samt gjennom plenumsdiskusjonene. Workshopen er gjennomført under Chatham House Rule. Dette innebærer blant annet at denne rapporten, med unntak av Vedlegg 1, oppsummerer synspunkter og erfaringer som er nevnt av de ulike deltakerne under workshopen i en kategorisert rekkefølge og uten å relatere de nevnte sårbarhetene/tiltakene (eller andre funn, synspunkter og erfaringer som presenteres i rapporten) til bestemte deltakere eller virksomheter som har deltatt i eller bidratt til workshopen.

Denne rapporten er strukturert på følgende måte: Seksjon 2 presenterer programmet som ble gjennomført under workshopen, samt andre relevante organisatoriske aspekter knyttet til prosessen, deltakelsen og referatskrivingen. I denne seksjonen gir vi også en oversikt over de ulike deltakernes tilknytning, altså aktørene fra helsesektoren som var representert under workshopen. Seksjon 3 gir en strukturert presentasjon av innspillene fra workshopen, med hensyn på identifiserte hovedtema. Seksjon 4 oppsummerer innlegget om scenarier og sårbarheter knyttet til fremtidige helsetjenester. Seksjon 5 diskuterer trusler mot gyldighet og pålitelighet av resultatene, mens Seksjon 6 konkluderer denne rapporten.

Denne rapporten inkluderer også to vedlegg. Vedlegg 1 oppsummerer ett av innleggene som er gitt under workshopen, nemlig innlegget "Sårbarheter knyttet til utvalgte caser fra Helsesektoren" ved Erlend Andreas Gjære (Forsker ved SINTEF). Vedlegget er foredragsholderens egne skriftlige oppsummering av hans innlegg. Vedlegg 2 gir en utfyllende opplisting (i ikke-kronologisk rekkefølge, men kategorisert etter utvalgte tema) av erfaringer og synspunkter rundt digitale sårbarheter og relaterte tiltak i helsesektoren som er blitt nevnt under ulike deler av workshopen. Innholdet i dette vedlegget er basert på notatene som under workshopen ble tatt av to SINTEF forskere og tre medlemmer av Lysneutvalget. Seksjon 4 er basert på Vedlegg 1, mens Seksjon 3 er basert på Vedlegg 2.

[1] Hele mandatet er tilgjengelig på: regjeringen.no/lysneutvalget

2 Organisering og gjennomføring av workshopen

Denne seksjonen redegjør for den praktiske organiseringen av workshopen med tanke på deltakelse, programgjennomføring og rapportering.

Tabell 1 viser en oversikt over aktørene som var representert (der det ikke er nærmere angitt, hadde aktøren èn representant).

Lysneutvalget (4 deltakere)
SINTEF (2 deltakere)
Helse Nord
Sykehuspartner
Helse Sør-Øst
Helse Midt-Norge RHF
Helse Vest IKT
Ikomm AS
Legeforeningen/Akershus Universitetssykehus
Sykehuspartner
Helse- og omsorgsdepartementet (4 deltakere)
Norsk Helsenett
Pensjonist med tidligere tilknytning til sektoren
Helse Stavanger HF
Bærum kommune, PLO helseinformatikk
Helsedirektoratet
Helse Bergen
Teknologirådet
Norsk Helsenett

Tabell 1: Aktører med tilknytning til helsesektoren som var representert under workshopen

Programmet for workshopen bestod av en innledning, en runde rundt bordet der deltakerne ble bedt om å presentere seg selv og ha et navneskilt foran, fem innlegg, gruppearbeid, en felles oppsummering av gruppearbeid og plenumsdiskusjon. Følgende opplisting oppsummerer programmet:

1. Innledning og presentasjon av deltakere
2. Innlegg ved SINTEF: "Sårbarheter knyttet til utvalgte caser fra Helsesektoren"
3. Innlegg ved Sykehuspartner: "Digitale sårbarheter i Helse-Norge sett fra en leverandørs perspektiv"
4. Innlegg ved Helse Vest IKT: "Helse Vest sine erfaringer rundt digitale sårbarheter"
5. Innlegg ved Bærum Kommune: "Erfaringer rundt sårbarheter knyttet til velferdstjenester"
6. Innlegg ved Helsedirektoratet og Helse- og omsorgsdepartementet: "Hvordan jobbes det fra myndighetsperspektiv med digitale sårbarheter i helsesektoren?"
7. Gruppediskusjoner – to hovedtemaer:
    1. Digitale sårbarheter for helsesektoren
        - Kjenner deltakerne seg igjen i beskrivelsene som fremkommer av presentasjonene?
        - Hvilke andre nåværende og fremtidige digitale sårbarheter bør beskrives?
    2. Effektive tiltak for sektoren
        - Hvilke tiltak bør iverksettes for å redusere eksisterende og antatte fremtidige sårbarheter?
        - Hva fungerer bra med dagens ordninger og bør videreføres?
8. Plenum og oppsummering

Av hensyn til åpenhet og riktig gjengivelse av synspunkter, ble workshopen gjennomført under Chatham House Rule[2]. Deltakerne ble informert om at en endelig rapport ville bli skrevet, uten at eventuell sitering av uttrykte innspill og synspunkter relateres til de enkelte deltakernes navn, samt at alle deltakerne vill få en intern versjon til gjennomlesing og med mulighet til å kommentere, før den endelige versjonen skulle foreligge.

Etter hvert innlegg var det satt av noen minutter til spørsmål til foredragsholderen samt diskusjon i plenum. Som en del av sin innledning til gruppearbeid, presenterte Lysneutvalget foreløpig inntrykk av aktuelle sårbarheter i helsesektoren – en oversikt basert på input mottatt fra ulike aktører i forkant av workshopen. Forslag til oppdeling av deltakerne i 3 grupper (i forbindelse med gruppediskusjoner) ble utarbeidet av Lysneutvalget. En referent for hver gruppe ble også foreslått. Hver gruppe ble oppfordret til også å finne en ordstyrer, i tillegg til referenten, slik at de to ovennevnte hovedtemaene for gruppediskusjonene ble dekket.

Som en del av siste punkt på programmet oppsummerte hver av de tre gruppene (ordstyrer for gruppa supplert av øvrige gruppemedlemmer) resultatene av gruppediskusjonen. Samtidig var aktuelle tema og synspunkt diskutert i plenum. Det ble avslutningsvis orientert om prosessen videre i forhold til skriving av rapporten fra workshopen og Lysneutvalgets videre arbeid.

3 En strukturert presentasjon av innspill fra workshopen

Denne seksjonen sammenfatter innspill fra hele workshopen, basert på funn som er rapportert i Vedlegg 2 (oppsummering av digitale sårbarheter og tiltak som er uttrykt under ulike deler av workshopen). Seksjonen er strukturert etter sentrale tema som også tilsvarer den tematiske kategoriseringen av innspillene fra det ovennevnte vedlegget. Dermed er både tema og de enkelte sårbarhetene/tiltakene direkte sporbare til vedlegget. Seksjon 3.1 karakteriserer dagens digitale helsetjenester, mens Seksjon 3.2 presenterer en tematisk oversikt over innspillene fra workshopen.

3.1 Dagens digitale helsetjenester – overordnet status, erfaringer og eksempler på konkrete hendelser

I denne seksjonen sammenfattes overordnede erfaringer og kjennetegn ved IKT i dagens helsesektor, basert på innspillene som er rapportert i Vedlegg 2.

Liv og helse er det aller mest sårbare vi har, vi påvirkes av systemer rundt oss, er avhengig at de er tilgjengelig 100 % av tiden, og at informasjon kun er tilgengelig for de som berettiget. Folk forventer at teknologi blir brukt og at utviklingen går fremover, selv om de kanskje til en viss grad mister oversikten over egne data. Digitale helsetjenester er også i endring. De blir stadig mer kritiske, og får en annen trusselhverdag. Som følge av nye teknologier er sektoren nå i ferd med å gjøre endringer og tilgjengeliggjøre systemer i mye større grad enn tidligere. Det er stadig flere tjenester som «alltid» må være tilgjengelige. Helsesektoren er stor og kompleks, med mange tusen ansatte. Samtidig har også brukerne av digitale tjenester forventninger om at de nye teknologiske mulighetene brukes. Man snakker gjerne om «digitalt innfødte» og ser at tilnærmingen til personvern og sikkerhet endres blant kommende generasjoner.

Det benyttes imidlertid fremdeles gamle systemer, dvs. ulike egenutviklete fagapplikasjoner med begrenset sikkerhet. Samtidig overføres ansvaret for å ivareta sikkerheten fra fagfolk til systemene.

I realiteten er det vanskelig å eliminere risiko og forhindre at det skjer sikkerhetsbrudd. For å kompensere for dette etableres det mekanismer for å detektere og korrigere hendelser.

[2] http://www.chathamhouse.org/about/chatham-house-rule

Blant sentrale utfordringer som ble påpekt under workshopen er tilgjengelighet av IKT systemer, og beredskap i forhold til nedetid. Hvis systemer blir borte noen timer kan liv gå tapt. Helsevesenet har så små marginer at dersom man måtte stenge sykehusene noen dager kan det eksempelvis gå utover kreftpasienter som ikke får den kontrollen de skulle ha. Det finnes blant annet manuelle rutiner og mulighet for utskrifter på papir. Disse gjør at man kan holde det gående i noen timer, men ikke dager. En annen sentral utfordring som er påpekt er at de teknologiske mulighetene ikke utnyttes – det er mange selvstendige aktører; mange systemer og lite integrasjon.

Under workshopen ble det nevnt flere eksempler på konkrete sikkerhetshendelser: løsepengevirus, utgått rotsertifikat, uautoriserte endringer og usikre klienter, for å nevne noen. Øvrige erfaringer viser at en del utstyr er utenfor support og ikke lar seg oppdatere. Privat bruk av jobbsystemer nevnes også som en trussel. Utfasing og sanering av systemer kan også være krevende. I tillegg påpekes det som en sårbarhet at patching tar tid, siden oppdateringer må testes på infrastrukturen først.

3.2 Digitale sårbarheter og tiltak – en tematisk presentasjon

Under presenteres en tematisk oversikt over de sårbarhetene og tiltakene som er spilt inn under workshopen, basert på notatene i Vedlegg 2.

3.2.1 Nye teknologitrender og nye driftsmodeller

Det er påpekt en rekke sårbarheter som er spesielt knyttet til nye teknologitrender og nye driftsmodeller. Big data, dvs. sammenslåing og analyse av store datamengder, er en utfordring. Det menes for eksempel at noen aktører kan gjennomføre mer analyse og sammensying enn ønsket.

Nettsky-baserte tjenester, som for eksempel brukes som hjelp til stor regnekraft, kan medføre at sensitiv info blandes. Nettsky-teknologien åpner også for nye driftsmodeller med mange aktører. Globale kommersielle aktører vil til en viss grad kunne overta kontroll over informasjon, eller få tilgang til den. Da vil denne bli spredt – noe på ulike typer nettsky, mobile enheter med videre. Dermed vil man kunne få blanding av private og offentlige helsedata. I tillegg kan det bli utfordrende å avklare ansvar på tvers av landegrenser.

Mange aktører ønsker å lage tjenester – de vil ikke lenger bare levere programvare, men ta over driften. Disse er tradisjonelt opptatt av at programvare skal være tilgjengelig, men informasjonssikkerhet er mer enn bare tilgjengelighet. Det er derfor viktig å lage programvare-løsninger som er sikre i seg selv fremover, og ikke stole på at infrastrukturen rundt tar vare på alt. Det menes også at det er en utfordring at aktører uten tilstrekkelig erfaring ønsker å ta over drift. I tillegg er det vanskelig å finne den ansvarlige/skyldige ved hendelser i en nettsky-scenario.

3.2.2 Utstyr og tilknyttet programvare

Medisinskteknisk utstyr er i en rivende utvikling. Utstyr er også på vei inn i private hjem og pålideligheten til utstyret kan være variabel. Hjemmet vil i større grad være behandlingstedet fremover, men er også sårbart. Infrastrukturen her er privat – kanskje delt, kanskje er andre private og offentlige aktører i bildet: helsetjenester, vaktselskap, strømleverandør m.fl. Det vil kunne bli et virvar av ulike tjenesteleverandører, i tillegg til at data skal integreres og lagres. Økt bruk av "Bring your own device" er også en problemstilling. Man snakker om det utvidede legekontoret som blir trukket hjem til folk. Dette vil kunne introdusere nye risikoer. Det antas også at privat bruk i fremtiden vil vokse inn i tjenestene. Da blir det utfordrende med hvem som skal drifte disse tjenestene og hvem som bør ansvarliggjøres for eventuelle hendelser.

Markedet for "Internet of things" blir stadig større. Det er uttrykt at det er teknologileverandører som på mange måter setter premissene for det som kommer, og at sikkerheten ikke alltid er i høysetet. Det er i tillegg et utall apper som kan lese av helsedata og koble seg opp mot diagnoseutstyr med videre. Selve mobilen vil

også være en sårbar enhet – den er ikke driftet av noen helseenheter, men kan være et veldig nyttig verktøy i fremtiden.

3.2.3 Kommunene i samspill med leverandørene og sektoren

Som en sentral sårbarhet ble manglende virksomhetsstyring i forhold til digitalisering og ikt-utvikling påpekt. Det ble nevnt at virksomheter blant kommunene og i helse- og omsorgssektoren mangler en digitaliseringsstrategi. Samtidig nevnes det at manglende digitalisering også i mange tilfeller kan være en digital sårbarhet. Man innfører nemlig elektroniske verktøy uten å endre arbeidsprosesser, og lykkes dermed ikke i å hente ut gevinstene ved investeringen. Det menes at et sannsynlig resultat er at man ender opp med systemer som er mindre sikre for innbyggere og pasienter.

Videre påpekes uavklarte ansvarsforhold mellom leverandører og databehandlingsansvarlige. Samtidig observeres det at private selskaper ofte har avtale med helseforetakene i forhold til å levere for eksempel rehabiliteringstjenester eller andre helsetjenester. Disse private aktørene vil mest sannsynlig bli viktigere i tiden som kommer for å bidra til at befolkningens behov for helsetjenester dekkes. Men kommunene får i stor grad støtte av KS, Helsedirektoratet og helse- og omsorgsdepartementet, og blir pålagt å følge nasjonale føringer og programmer, mens de private helsevirksomhetene ikke har samme fokus fra sentrale myndigheter.

I forhold til sikkerhetshendelser nevnes målrettede angrep samt sikkerhetshull gjennom velferdsteknologi og "internet of things". Dette er på full fart inn hos både kommuner og private virksomheter og stiller store krav til både databehandlingsansvarlig og databehandler i forhold til sikkerhetskultur, risikobevissthet og strategi for digitalisering.

3.2.4 Kommunale velferdstjenester

Utfordringer og sårbarheter

Det er blitt påpekt at ved utvikling og innføring med kommunale velferdstjenester er det i starten mye fokus på funksjonalitet, andre problemstillinger kommer ved skalering. I forhold til drift beveger man seg fra det tradisjonelle "alt i eget hus", og vil fremover få distribuerte løsninger. I utprøving har man hatt fokus på om produktet i seg selv er godt, men når man skal skalere kommer det nye utfordringer, eksempelvis: Personvern, varsler eller posisjoner som ikke kommer frem til mottaker, eller forvaltning (hvor og hvor lenge lagres dataene med videre). To utfordringer som spesielt nevnes er uklarhet rundt situasjoner når tjenestene på sikt går på tvers av kommunegrensene, for eks. mobil trygghetsalarm, samt at pleie– og omsorg i kommunene har svake systemer.

Tiltak

Det er uttrykt at kommunene trenger bestillerkompetanse i forhold til krav til leverandører. Videre trengs det mekanismer for å spre erfaringer en kommune gjør. En kanal er Nasjonalt program for Velferdsteknologi, der 31 utviklingskommuner deltar. Det nevnes også at det finnes et samarbeid mellom KS og Hdir på velferdsteknologi og at det er opprettet arenaer for erfaringsutveksling.

3.2.5 Utfordringer knyttet til underleverandører

Erfaringer fra hendelser viser at mange av hendelsene skyldes underleverandørene. I tillegg kan underleverandør kan være mål for målrettede angrep. Det nevnes at 50% av omfattende episoder med beredskap de siste år skyldes svikt hos underleverandør. Eksempler på slike hendelser inkluderer feil på strømleveranse og arbeid på sterkstrømsanlegg, tilfeller av at ekstern leverandør har gjort oppgradering av f.eks. telefonisentral som har gitt ustabilitet, brudd på datalinjer, cluster som feiler osv.

3.2.6 Sikkerhet og kvalitet av helsedata

Utfordringer og sårbarheter

En rekke innspill med spesiell relevans for dette temaet har kommet under workshopen. Her nevnes noen av de som ikke er kategorisert under øvrige tema.

Som pasient må man forholde seg til mange aktører. Man er avhengig av at informasjonen følger med pasienten. Deling på tvers av helseforetak er noe pasienten i stor grad vil, for at legene skal kunne vite nok om dem der de søker hjelp. Integritet og tilgjengelighet er følgelig viktig for liv og helse. Det påpekes spesielt at man er avhengig av tilgjengelighet av systemer og at informasjon er utelukkende tilgjengelig for den som er berettiget. Langvarig nedetid er i ROS-analyser er definert som 4 timer. I tillegg er samhandling utfordrende. Kan man, for eksempel, i kontekst av fritt sykehusvalg ta med dataene sine?

Stortingsmeldingen "Èn innbygger – èn journal" påpeker at de teknologiske mulighetene ikke utnyttes. Det er nemlig mange selvstendige aktører og mange systemer. Ved distribuert journal er det en utfordring at man ikke vet hva man ikke har tilgang til. Det er en underkommunisert utfordring knyttet til elektronisk pasientjournal. En problemstilling som uttrykkes i forhold til visjonen, er usikkerheten om det er farligere å vite an man mangler informasjon, eller å feilaktig tro at man har fått den informasjon man trenger.

Pårørende får en del tilgang; og det er vanskelig å få til tilgangsstyring i praksis. Det kan også være vanskelig å få til hensiktsmessig tilgangsstyring og sporing i forhold til brudd på taushetsplikt. Brukeradministrasjon i forhold til distribuerte systemer er utfordrende. I tillegg er blanding av helsedata med private data en utfordring.

Tiltak

Tilgjengelighet veier tungt, og adresseres gjennom redundans og backup. Konsekvensene av bortfall av informasjon fra elektronisk pasientjournal bør komme tydeligere frem. I tillegg er NHN i gang med etablere georedundante løsninger, dvs. å få mange av de nye tjenestene som blir levert til å være geografisk spredt, heller enn å kjøre på et datasenter.

3.2.7 Utfordringer knyttet til personvern

Det påpekes blant annet at man ofte ser at «alle pasienter ønsker sikkerhet og personvern». Det menes at personvern er en utfordring og at sporing gjøres i større grad enn helt nødvendig. Noen kan avstå fra medisinsk hjelp hvis de føler seg overvåket.

Innsyn i loggene er vanskelig når loggene er spredt i ulike systemer. Det er også observert eksempler på at pårørende installerer webkamera for å følge med. Følgelig stilles spørsmålet: hva hvis helsepersonell tar avstand fra å gi helsehjelp fordi de føler seg overvåket? I tillegg er det med stort omfang av leverandører utfordrende å finne ut hvor personvernet eventuelt ble brutt.

3.2.8 Brukervennlighet av systemer og opplæring

Utfordringer og sårbarheter

Opplæring anses som viktig da det er mye turnover i sektoren. Behovet for opplæring er synliggjort på flere nivåer og i forhold til flere aspekter. Norm-sekretariatet, for eksempel, reiser rundt og holder kurs for hele sektoren.

Det har blitt nevnt at helsepersonell sliter med å forstå systemer grunner bl.a. økende kompleksitet. Det er også en utfordring at brukerne ikke forstår konsekvenser av handling i forhold til bruk av verktøy. Ulik bruk av verktøy medfører varierende datakvalitet.

Tiltak

Det er uttrykt at når man skal engasjere brukere er det viktig at man lager enkle prosedyrer som kan integreres i daglig drift, på linje med HMS-runder. Informasjon om IT-sikkerhet til brukere bør også være mest mulig konkret, og gjerne ta utgangspunkt i aktuelle hendelser og scenarier. I tillegg er det påpekt at ledelsen må utdannes, slik at man oppnår en viss konsistens i forhold til relevant kompetanse.

3.2.9 Ansvar for IKT-sikkerhet

Utfordringer og sårbarheter

Det oppleves som et problem at både ledelse og brukere ikke er nok bevisst sitt ansvar innenfor IT-sikkerhet. Det kan for eksempel være vanskelig for ledelsen å forholde seg til IT-sikkerhet, enten på grunn av manglende kunnskap, eller fordi IT-sikkerhet skiller seg fra andre områder hvor man også har styringsansvar. I tillegg nevnes det at en direktør som er behandlingsansvarlig har begrenset reell innflytelse på (valg av) IKT-løsninger.

Det oppleves som en utfordring at man som systemeier lokalt har ansvar men ikke innflytelse. Det nevnes også at HF'ene har for liten påvirkning på innkjøpssituasjonen i forhold til det ansvaret de har for systemenes funksjon. For eksempel: databehandlingsansvarlig er den enkelte direktør for helseforetaket, men beslutning om hvilke systemer som kjøpes inn ligger i sykehuspartner, helseVest IKT og lignende.

Tiltak

Flere aktuelle tiltak ble spilt inn i kontekst av dette temaet. Her oppsummeres de som ikke er kategorisert under øvrige tema i denne seksjonen.

Det er viktig at man definerer og bevisstgjør alle parter. Alle bør være klar over hvilken rolle de har og hva deres ansvar er. Det kan i tillegg være vanskelig for ledelsen å forholde seg til IT-sikkerhet enten på grunn av manglende kunnskap, men også fordi IT-sikkerhet skiller seg fra andre områder hvor man også har styringsansvar. En mulig løsning på dette er å fokusere på det som er felles med andre styringssystem, som f.eks. HMS. Det er også viktig at linjene for rapportering av IT-sikkerhet går mest mulig direkte til ledelsen. Dette gjør at man unngår siling av informasjon, samtidig som det bevisstgjør ledelsen på ansvaret den har.

Fra et kommuneperspektiv bør øverste nivået ta et større ansvar. Leverandørene bør også ta et ansvar, samtidig som deres kunder utfordrer dem. I forhold til «ansvarliggjøring av de ansatte» er det uttrykt at det jobbes målrettet etter ISO 27001, men at ledelsen må legge til rette for at det blir gjort på en sikker måte. Videre er det gitt uttrykk for at det ofte blir pålagt enkeltpersoner å ivareta mye IKT-sikkerhet. Et tiltak er at man fra ledelsen legger til rette for at dette ikke skjer, eksempelvis med tekniske mottiltak.

3.2.10 Kommunikasjon mellom aktører

Utfordringer og sårbarheter

Det uttrykkes som et problem at informasjon fra HoD/Hdir ikke når frem til brukermiljøene i helseforetakene (f.eks. databehandlingsansvarlig, relevante IT-miljø). Informasjon og forespørsler fra HoD og Hdir blir rettet direkte til RHFene. Disse siler informasjon og styrer hva de vil sende videre og til hvem. RHFene har heller ikke direkte kompetanse på IT-sikkerhet. Man kan dermed risikere at informasjon/forespørsler ikke når frem til de relevante miljøene i helseforetakene, eller at informasjon kommer frem for seint til at man rekker å gjøre noe med den, som f.eks. høringsuttalelser.

Det uttrykkes også at det er utfordringer knyttet til kommunikasjon med andre helseaktører – eksempelvis rundt utvikling og bruk av fellesløsninger, elektronisk meldingsutveksling, tilgangsstyring osv. Man har også utfordringer med sikker kommunikasjon, nøkkelutveksling osv. I tillegg ser man at tekniske systemer ikke

klarer å ivareta de kravene lovene stiller til behandling av helseopplysninger. Det kan også være vanskelig med kravstilling til internasjonale leverandører.

Samtidig spør man hva som er mest kritisk for pasientsikkerheten og for pasienten som sluttbruker: å ivareta taushetsplikten eller at informasjon er tilgjengelig for de som skal ha den? Det kan nemlig bli store konsekvenser ved langvarig bortfall av eksempelvis elektronisk kommunikasjon. Medisinskteknisk utstyr er kritisk, samtidig som man klarer å leve uten DIPS noen dager. Akuttfunksjonene vil nok fortsette å behandle selv om digital samhandling opphører. Men i en slik situasjon vil kommunikasjon mellom sykehusene stoppe opp. I tillegg vil kommunikasjon til sykehus og fastleger stoppe opp. Dermed vil samhandlingen bli mer og mer viktig fremover.

Tiltak

Generelt etterspørres det strammere styring fra HoD for å sikre standardisering i IT-prosesser. Et konkret eksempel er at det oppleves som et problem at det ikke finnes mere standardiserte rutiner for å vurdere IT-sikkerhet ved innkjøp. Dette gjelder både generelle IT-system og spesifikt helseutstyr med en sterk IT-komponent. Man har opplevd å bli møtt med "men Helse-X har allerede godkjent denne".

Det er også argumentert at hvis RHF-er tar beslutninger uten å involvere de lokale foretakene, hvordan skal man da gi eierskap? Det handler om å være med fra starten av og passe på at også direktørene i foretakene, ikke bare RHF-ene er involvert. RHF er ikke databehandlingsansvarlig, og da må departementet kommunisere med foretakene. Et mulig tiltak kan være at HoD/Hdir identifiserer relevante mottakere som må få informasjon direkte, parallelt med det som sendes til RHFene.

I tillegg er det nevnt at det er ønskelig at HoD/Hdir tar initiativ til å opprette mere standardiserte rutiner på tvers av sektoren og sørge for at disse brukes.

3.2.11 Behov for standarder og felles rammeverk

Det er stilt spørsmål ved behov for større grad av bruk av standarder, styringssystemer og felles rammeverk. Blant annet spør man om det er for svakt at Difi bare "sterkt anbefaler" ISO27001. Det finnes krav til beredskap og tilgjengelighet, men ikke i forhold til for eksempel ISO standarder. Standardisering på har imidlertid en kostnad. Det påpekes også at bruk av standarder ikke nødvendigvis løser problemer – her vil varierende grad av kunnskap, kultur og språklig fortolkning likevel skape store ulikheter.

Standarder som brukes for meldingsutveksling baserer seg på internasjonale standarder. De som driver medisinskteknisk utstyr kan dermed vanskelig tilpasse sikkerhetskravene, da det er internasjonale standarder som setter kravene. Samtidig nevnes det at så langt har nasjonale leverandører dominert i markedet, men på infrastruktursiden har man leverandører fra hele verden. Det er i tillegg nevnt at man antar at velferdsteknologi i stor grad vil bli levert fra utlandet.

3.2.12 Avhengighet av infrastruktur

Det er uttrykt at den aller største sårbarheten er avhengighet til telekom, på grunn av viktigheten av kommunikasjon. Man er kritisk avhengig av det for alle tjenester – varslinger, personsøk mv. Videre kan bortfall av sentral infrastruktur være livsfarlig, og representerer dermed en trussel. Samtidig er avhengighet til vann og kloakk en sårbarhet – sykehus må stenge etter få timer om dette bortfaller.

3.2.13 Beredskap, sikkerhetskultur og øvelser

Utfordringer og sårbarheter

Beredskap og øvelser anses som svært viktig. Kjennetegn for helsesektoren viser at man er gode på beredskap og manuelle rutiner. Blant innspillene er at det er bra om man klarer å identifisere risiko – men sårbar-

heten er avhengig av hvordan man møter den risikoen. Det påpekes derfor at øvelser er veldig viktig og at man må gjøre mer innen øvelser på digitale sårbarheter. Mange hendelser inntreffer som følge av manglende opplæring, holdninger og årvåkenhet. Man har en regional sikkerhetsinstruks og undersøker årlig hvor mange som kjenner til denne. Man ser at trenden er nedadgående og vurderer derfor å styrke bruk av e-læringsprogrammer.

Tiltak

Det øves på nedetid av IKT systemer, men man får ikke mulighet til å øve på redusert bemanning. Videre er det viktig å fortsette å øve og bli gode på håndtering av hendelser. Det er uttrykt at det trengs beredskapsplaner og øvelser i forhold til situasjoner når journalsystemer er ute av funksjon. I tillegg bør det gjennomføres flere rene IKT-øvelser i helsesektoren.

3.2.14 Felles tiltak – samarbeid, standardisering og styring

Utfordringer og sårbarheter

Det er, som nevnt ovenfor, mange avhengigheter mellom aktørene innen helsesektoren. I tillegg er det avhengigheter mellom sektorer. Uten felles tiltak kan mulighetene for samspillet bli begrenset, samtidig som resultatene av ulike tiltak kan bli variable i forhold til typer tjenester og deres sikkerhet. Dette vil representere en sårbarhet.

Tiltak

Det ble etterlyst en overordnet strategi og styring, slik at man unngår å sette i gang med mange enkelttiltak som ikke henger sammen. Sterkere nasjonal styring etterlyses også for å styrke felles behov og for å unngå konkurranse mellom regionene. I tillegg etterlyses det at man stiller krav til andre sektorer, siden det er mye som utveksles. Det er også uttrykt at det er viktig med felles tiltak i kommunesektoren samt at det er behov for at systemeier/virksomhetsledelse i mye større grad tar grep om digitalisering i egen virksomhet og ikke lar dette være overlatt til IKT-ansvarlig.

Mer konkret er det uttrykt et behov for eller ønske om:

- Nasjonal samordningsgruppe mellom departementene, hvor problematikken rundt informasjonsbehandling blir adressert. Mangel på dette vil avskjære muligheten for erfaringslæring mellom sektorer.
- Informasjonsutveksling i akutte situasjoner. Man må ta i bruk risikostyring her; at ledelsen ser på noen overordnede tiltak som skal implementeres.
- Sikkerhetskrav i innkjøpsprosessene.

3.2.15 Kompetansebygging, undervisning og forskning

Utfordringer og sårbarheter

Det er for lite evaluering av temaene som blir diskutert under denne workshopen. Det påpekes også at det er veldig få akademiske miljøer på helseinformatikk. I tillegg nevnes det at det gjøres veldig liten forskning på konsekvensene av det som innføres og at det er liten evaluering av store IT-prosjekter.

Tiltak

Man kunne trengt en mer akademisk tilnærming til helseinformatikk. Helseinformatikk som fag (utdanning og forskning) bør dermed fokuseres mer på. I tillegg et det uttrykt at det trengs mer forskning på dataflyt og dataeierskap, samt tilgangsstyring.

Digitalisering, informasjonssikkerhet og personvern bør inngå som tema i utdanningsprogram som for eksempel ny nasjonal satsning på lederutdanning i primærhelsetjenesten.

Videre etterlyses det involvering av helsepersonell i hverdagen i større grad enn det som gjøres, slik at man inkluderer de som har forståelse for arbeidsprosesser, strukturering av informasjon mv.

3.2.16 IKT som tiltak for økt pasientsikkerhet

Det ble nevnt at det finnes dokumentasjon på at ca. 10% av pasientene som behandles på sykehus blir skadet som følge av behandlingen. Når pasienter påføres skader gjennom behandling uten at det har noe med IKT å gjøre, er spørsmålet om IKT kunne blitt brukt som tiltak mot dette? Det er imidlertid mer nærliggende å tro at verktøy skal støtte og stille understøttende spørsmål, ikke at man skal lene seg til verktøyene. Det ble derfor etterlyst at datasystemene kanskje «spør mer» om ulike tiltak er gjort, som støtte for forsvarlig pasientbehandling.

Det er også blitt påpekt at dersom pasientsikkerhetsperspektivet er avgjørende må man se på summen av systemer langt utover det som omtales som et enkeltstående epj-system, da det er summen av samtlige systemer og aktiviteter som er avgjørende.

3.2.17 Hva fungerer bra i dag (og ønskes videreført)

En del velfungerende eksisterende tiltak er allerede nevnt ovenfor i kontekst av ovennevnte tema. I tillegg har følgende blitt påpekt under workshopen:

- Man har oppnådd bedre sikkerhet med Dips enn tidligere og må ikke glemme gevinstene dette har medført.
- HelseCSIRT gjør en viktig jobb for sektoren og er en massiv bidragsyter til å heve informasjonssikkerheten i sektoren. Men det er likevel viktig at det ikke blir en hvilepute for de regionale – de er fortsatt ansvarlige for håndtering lokalt, og må være i stand til dette.
- Normen for informasjonssikkerhet betraktes som en god veileder for folk flest, selv om det er mange som har andre meninger om den. Eksempelvis uttrykkes det at den ikke passer for de aller minste helseforetakene. Begrunnelsen er at mange av de som skal bruke den ikke vil ha ressurser til å følge opp normen, fordi den er for omfattende. I forhold til normen menes det også at det er behov for oppdateringer. Enkelte forslag til tiltak oppleves som utdaterte. Det etterlyses også mer konkrete forslag til hvordan man skal forholde seg til IT-sikkerhet.
- Helsenett trekkes frem som et velfungerende samarbeid.

4 Et blikk mot fremtiden – scenarier og sårbarheter

Workshopen ble innledet med et blikk mot fremtiden – den digitale utviklingen i helsesektoren de kommende 15 årene, og de sårbarhetene som oppstår eller forsterkes på bakgrunn av nye trender. Under sammenfattes hovedmomentene, basert på en mer detaljert redegjørelse som er gitt i Vedlegg 1.

Et sentralt moment i framtidsutsiktene for digitale helsetjenester er at de i større og større grad vil utføres i tilknytning til hjemmet. For eksempel vil mange undersøkelser og konsultasjoner kunne gjøres uten at man fysisk oppsøker en lege. Målet er en helsesektor som skalerer til å møte framtidens økte behov, men utviklingen kan til en viss grad karakteriseres som teknologidrevet. Det er sannsynlig at offentlig helse- og omsorgssektor vil miste kontroll over deler av den digitale tjenesteleveransen til innbyggerne, blant annet fordi den enkelte bruker selv har råderett hjemme og samtidig tar aktivt initiativ til innføring og bruk av ny teknologi. Det vil kreves stor innsats før sentrale systemer med strenge krav til sikkerhet og personvern kan gi tilfredsstillende integrasjon mot infrastruktur i utstyr, applikasjoner og data fra innbyggernes private hjem. På veien vil nye sårbarheter introduseres, samtidig som det er fare for at noen gamle vil gjøre seg ytterlig gjeldende. Sårbarhetene som spesielt har blitt fremhevet, inkluderer blant annet:

- Lav integritet på medisinsk utstyr og ukjent tillit til dataene som samles inn, er en sårbarhet i en tid når selv-diagnostisering blir mer utbredt.
- Ved bruk av privat-eid utstyr og infrastruktur sammenblandes private og helsemedisinske data. Sikring av sistnevnte data er ikke nødvendigvis ivaretatt i tilstrekkelig grad, slik at sensitive opplysninger kan komme på avveie.

- Infrastrukturen i hjemmet brukes av flere aktører, blant annet leverandører av helse- og velferdstjenester. Internett-tilkoblingen fra en bolig kan være en sårbarhet når den deles mellom forskjellige aktører/tjenesteleverandører.
- Fjernstyring av hjemmet til ulike formål blir mer vanlig. Dette kan medføre at det oppstår et sikkerhetsmessig klasseskille mellom de som har råd til godt utstyr, og de som kjøper det billigste – uten at pris kan garantere for sikkerheten.
- Sikkerhet har ikke nødvendigvis fokus når utviklingen er teknologidrevet. Fordelen av å være først på markedet veier tyngre enn hensynet til sikkerhet.
- Plassering av infrastrukturen og utstyret hjemmet kan medføre at tyver får fysisk tilgang, eller at angrep over nett inntreffer.
- Sending av falske alarmer fra hjemmet er en sårbarhet; spesielt når mange slike alarmer utløses samtidig, noe som kan ta ressurser fra helsetjenesten.
- Løsningene blir i større grad sosio-tekniske systemer med mange aktører. Brukeradministrasjon blir mer sårbar når den deles på tvers av flere instanser.
- Godt personvern er en forutsetning for at datainnsamling og tjenester skal bli akseptert blant folk. Følelse av kontinuerlig overvåking kan gi folk redusert tillit til helsevesenet, og dermed kan de vegre seg mot å oppsøke eller ta imot helsehjelp. Samtidig er det en trygghet for mange.
- Overvåking av helsepersonell som besøker hjemmet er også er sårbarhet.
- Tilgangsstyring er en utfordring. Blant annet skal pårørende gis tilgang til deler av data og systemer.
- Grenser mellom private data og helsedata vannes ut, slik at også private data kan vurderes brukt til helseformål. Det kan være uklart hvem har eierskap til dataene og hvem som er databehandlingsansvarlig til enhver tid.
- Big data og analyse kan representere en trussel mot personvernet. Dilemmaet er at vi får mange muligheter, men gjør oss samtidig avhengige av de eksterne og blir desto mer sårbare.
- Underleverandører blir flere og de kan bli mål for målrettede angrep. Da bør de ha god sikkerhetskultur og tilsvarende rutiner og opplæring omkring taushetsplikt som man forventer av helse- og omsorgssektoren for øvrig.
- Ettersom kjeden av tjenesteleverandører blir større, blir også hendelseshåndtering på sikt mer krevende. Da stilles spørsmålet hvem som har ansvaret hvis noe går galt, og hvordan utenlandske leverandører kan bli fulgt opp.

5 I hvilken grad er resultatene representative?

I kontekst av empiriske studier snakker man gjerne om gyldighet og pålitelighet. Pålitelighet handler i hovedsak om hvorvidt man ville oppnådd de samme resultatene dersom studien ble utført på nytt, uavhengig av den opprinnelige. Gyldighet handler om hvorvidt

- vi adresserer det som er relevant og ment å bli adressert
- sammensetning av deltakere i en studie (hvorvidt de er representative) og statistisk analyse av resultatene
- skjulte sammenhenger av de ulike faktorene/variablene som blir studert
- begrensninger i forhold til muligheten til å generalisere resultatene til andre domener og kontekster.

Resultater basert på empiri er ofte utsatt for trusler mot pålitelighet og gyldighet. Naturligvis er det mange trusler som kan påpekes i forhold til oppsummering av funn basert på en workshop. Selv om mange aktører med omfattende kompetanse og erfaring fra sektoren var representert under workshopen, kan det alltid stilles spørsmålstegn til om denne forsamlingen var representativ. Det er for eksempel blitt påpekt at større grad av det kliniske perspektivet var savnet under workshopen.

De rapporterte funnene representerer enten individuelle eller (til en viss grad) delte meninger og erfaringer. I den grad de er individuelle, er det ikke spesifisert i oppsummeringen (Vedlegg 2), slik at enkelte utsagn og

meninger kun er subjektive og lite representative for gruppa (deltakerne i workshopen). Det er i tillegg blitt påpekt at det finnes for lite forskning på helseinformatikk, og at det spesielt savnes grundig evaluering av de påstandene og utfordringene som er blitt diskutert. Faktaopplysninger eller generelle erfaringer som er spilt inn og nevnt, er i de fleste tilfeller ikke underbygget med dokumentasjon eller annen evidens. Likevel er det bestrebet å inkludere flest mulig meninger og argumenter i både oppsummeringen i vedlegg 2 og følgelig også i drøftingen i Seksjon 3.

Hvorvidt workshopen har adressert alle relevante tema, er også en annen usikkerhet. Det er bestrebet å representere en rekke sentrale perspektiver under innleggene og å åpne mest mulig for ytringer og diskusjon blant de øvrige deltakerne. Likevel er det usikkert om alle relevante aspekter er tatt opp under selve workshopen, og om gjennomføringen/programmet i tilstrekkelig grad har lagt til rette for det.

Måten funnene er blitt presentert på kan også til en viss grad påvirke oppfatningen av innhold og relevans av funnene. Denne rapporten begrenser seg til kun de argumentene som er blitt nevnt og dermed notert under workshopen. Notatene som ble tatt av tilsammen fem referatskrivere representerer et utdrag av innspillene, med de usikkerhetene det innebærer. Vedlegg 2 er gjengivelse av de notatene, strukturert etter valgte tema. Diskusjonen i Seksjon 3 er direkte sporbar til Vedlegg 2. Vedlegg 1 er en foredragsholders egne oppsummering av sitt foredrag. En tidlig versjon av rapporten har blitt sendt til alle workshop-deltakerne for gjennomlesing og kommentarer. I tillegg er det gjort rede for prosessen bak workshopen og organiseringen i Seksjon 2. På denne måten er det blitt forsøkt å unngå subjektivitet fra rapportforfatterens side, i forhold til presentasjonen av funnene.

Mange trusler mot gyldighet er dermed involvert i denne sammenhengen, noe som generelt er vanlig i kontekst av empiri. Likevel er det et viktig faktum at vi hadde samlet en god pool av eksperter fra sektoren. En rekke sårbarheter og tiltak har blitt eksemplifisert og begrunnet med deres konkrete erfaringer. Tatt i betraktning den betydelige erfaringen og kompetansen som ble samlet under denne workshopen, bør den representerte kompetansen og mangfoldet av deltakerne til en viss grad oppveie de mange usikkerhetene og truslene mot gyldighet og pålitelighet.

6 Konklusjon

Digitalt sårbarhetsutvalg ble nedsatt av regjeringen i 2014. Utvalget skal foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. I mai 2015 arrangerte utvalget en workshop for å drøfte sårbarheter innenfor helsesektoren, og diskutere effektive tiltak for å møte dagens og fremtidens utfordringer. Programmet bestod av flere innlegg, gruppediskusjoner og plenumsdiskusjoner.

Under hele workshopen ble mange synspunkter og erfaringer spilt inn av deltakerne, med tanke på digitale sårbarheter og relevante tiltak (eksisterende og nye). En rekke tema har blitt adressert, blant annet: organisering og kommunikasjon mellom aktører i sektoren, ansvar for IKT sikkerhet, personvern, integritet av data, nye tiltak, eksisterende tiltak og løsninger som fungerer, osv. Denne rapporten gjør rede for gjennomføringen av workshopen og sammenfatter funn fra alle deler av workshopen – innleggene, gruppearbeidet samt plenumsdiskusjonene. Rapporten er basert på notater tatt under workshopen av flere deltakere, samt tilbakemeldinger etter deltakernes gjennomlesing av en foreløpig versjon.

Blant hovedfunnene fra workshopen er at:

- Helsetjenester i fremtiden i stadig støtte grad vil bli utført i tilknytning til hjemmet.
- Det er sannsynlig at offentlig helse- og omsorgssektor vil miste kontroll over deler av den digitale tjenesteleveransen til innbyggerne, blant annet fordi den enkelte bruker selv har råderett hjemme og samtidig tar aktivt initiativ til innføring og bruk av ny teknologi.

- Det vil kreves stor innsats før sentrale systemer med strenge krav til sikkerhet og personvern kan gi tilfredsstillende integrasjon mot infrastruktur i utstyr, applikasjoner og data fra innbyggernes private hjem.
- På veien vil nye sårbarheter introduseres, samtidig som det er fare for at noen gamle vil gjøre seg ytterlig gjeldende.
- Dagens helsesektor karakteriseres av høy grad av avhengighet av IKT tjenester, brukernes forventning til at teknologi blir tatt i bruk, økt grad av tilgjengeliggjøring av systemer, samt fortsatt tilstedeværelse av gamle fagsystemer.
- Det blir stadig mer vanskelig å eliminere risiko, slik at en rekke tiltak er rettet mot håndtering av hendelser, for eksempel redundans, øvelser og beredskap.
- Eksempler på dagens digitale sårbarheter i helsesektoren inkluderer blant annet: redusert tilgjengelighet av IKT systemer, utfordringer med skytjenester, gamle fagsystemer og utstyr utenfor support, svekket personvern, vanskeligheter med tilgangsstyring, manglende beredskap og avhengighet av infrastruktur.
- Eksempler på tiltak som er diskutert inkluderer blant annet: større grad av beredskapsøvelser, opplæring, samarbeid om felles tiltak, samt undervisning og forskning innen helseinformatikk.
- Blant de eksisterende tiltakene som fungerer bra og ønskes videreført, er blant annet følgende nevnt: HelseCSIRT, normen for informasjonssikkerhet og helsenett.

VEDLEGG 1: Framtidens sårbarheter i helsesektoren

En oppsummering av innlegget "Sårbarheter knyttet til utvalgte caser fra Helsesektoren" gitt under workshopen av Erlend Andreas Gjære (Forsker ved SINTEF)

Hvor går den digitale utviklingen for helsesektoren de kommende 15 årene? Et sentralt moment er at helsetjenester i større og større grad vil utføres i tilknytning til *hjemmet*. Målet er en helsesektor som skalerer til å møte framtidens økte behov, men utviklingen kan til en viss grad karakteriseres som teknologidrevet. Det er sannsynlig at offentlig helse- og omsorgssektor vil miste kontroll over deler av den digitale tjenesteleveransen til innbyggerne, blant annet fordi den enkelte bruker selv har råderett hjemme og samtidig tar aktivt initiativ til innføring og bruk av ny teknologi. Det vil kreves stor innsats før sentrale systemer med strenge krav til sikkerhet og personvern kan gi tilfredsstillende integrasjon mot infrastruktur i utstyr, applikasjoner og data fra innbyggernes private hjem. På veien vil nye sårbarheter introduseres, samtidig som det er fare for at noen gamle vil gjøre seg ytterlig gjeldende.

VIDEOKOMMUNIKASJON FOR KONSULTASJON og liknende må nødvendigvis gå over Internett via standardiserte åpne protokoller, som igjen må sikres mot avlytting ut fra innholdet som potensielt kan kommuniseres her. Teknisk oppsett på brukersiden vil samtidig kreve sitt av brukervennligheten på tilbudet, og kan være sårbar for feilkonfigurasjoner og bortfall, og det blir mange undersøkelser og konsultasjoner som vil kunne gjøres uten at man fysisk oppsøker en lege.

LAV INTEGRITET PÅ MEDISINSK UTSTYR brukt til innsamling av helsedata kan bli en sårbarhet, i en tid hvor selv-diagnostisering er utbredt og pasienter kan insistere på at deres data skal bli brukt. Stadig rimeligere medisinsk utstyr vil øke graden av privatisering, slik det allerede har startet med mobilen og f.eks. målinger av puls, blodtrykk, søvnrytme, osv. Hvordan skal man forholde seg til dataene som samles inn?

PRIVATE ENHETER/APPLIKASJONER/INFRASTRUKTUR BRUKES til innsamling av helsedata, som selvsagt kan være sårbare for data-lekkasjer via deres naturlige sammenblanding med privat-eid innhold og programvare. Systemene skal også integreres mot grensesnitt som til slutt ender opp i elektronisk journal, men også gjerne lagres flere steder på veien, inkludert hos globale – potensielt dominerende – aktører hvor brukerens kontroll over dataenes lagring og prosessering er liten, med mindre det foreligger særlig gode avtaler.

DELT INFRASTRUKTUR I HJEMMET, gjerne både privat og samtidig helt nødvendig for ulike aktører som tilbyr tjenester til hjemmet, enten det er direkte i forbindelse med helse- og velferdstilbud – inkludert private applikasjons-, utstyrs- og tjenestetilbud – eller det er internettleverandør, sikkerhets-/vaktselskap, kraftselskap/strømleverandør, brannvarsling, og tilkobling mot familie/pårørende. Selve internett-tilkoblingen fra en bolig kan være en sårbarhet når den deles med mange andre aktører og formål. Får helsedata riktig informasjonssikkerhet i nettet når det blandes med andre typer data, og dersom total belastning av f.eks. streamet medieinnhold blir svært høy?

FJERNSTYRING AV HJEMMET, f.eks. lys, temperatur og dørlåser vil stadig få nye funksjoner og integrasjoner slik at det kan brukes av andre interessenter, for eksempel i forbindelse med velferdsteknologi, og Internett legges til i arkitekturen. Det blir kort sagt alle slags "smarte" dingser hjemme, med sensorer, nettverk og aktuatorer overalt, og generelt mange potensielle angrepsflater, særlig de som ikke enkelt kan oppdateres eller hvor produsent/leverandør forsvinner med tiden. Samtidig kan det oppstå et sikkerhetsmessig klasseskille mellom de som har råd til godt utstyr, og de som kjøper det billigste – uten at pris kan garantere for sikkerheten heller.

SIKKERHET HAR IKKE NØDVENDGVIS FOKUS når utviklingen er teknologidrevet. Analyseselskapet Gartner spår ca. $ 2 billioner i markedet for *Internet of Things* innen bare 5 år, og 15% av dette innenfor helsevesenet. Her gjelder nå i høyeste grad fordelen av å være først på markedet, som ikke uten videre har sammenheng med fokus på å lage sikre løsninger.

INNBRUDDSTYVER KAN SPESIALISERE SEG på å angripe sårbare deler av hjemmets funksjoner, inkludert slike som f.eks. hjemmetjeneste kan bruke til å låse opp ytterdøren med når de kommer. Med mye teknisk utstyr i omløp risikerer man også kriminelle som lyver om at de skal reparere utstyr som er blitt plassert i hjemmet, det kan gjerne være medisinsk utstyr eller annen velferdsteknologi, og som dermed skaffer seg fysisk tilgang til hjemmets verdier.

ANGRIPER TAR KONTROLL OVER HJEMMET uten brukerens kunnskap om hva som skjer, i ytterste konsekvens. Det er samtidig vanskelig å forklare risiko på dette området uten å skape frykt.

FALSKE ALARMER BLIR SENDT fra boligen som fører til unødige ressurser fra helsetjenesten – hva om dette utløses for mange pasienter/brukere samtidig?

BARN SOM FIKLER med teknologien på måter kan ha konsekvenser for integritet og tilgjengelighet – eller det legger uvitende til rette for scenarier som nevnt over – uten at dette fanges opp lett før skaden allerede har skjedd.

NEDETID/AVBRUDD utenfor helsetjenestens kontroll, kan i tilknytning til private hjem ta ekstra lang tid å fange opp, kartlegge omfang av, involvere ansvarlig leverandør, varsle pasient/sluttbruker, og til syvende og sist gjennomføre og kvalitetssikre utbedring.

SYSTEMER ER IKKE BARE TEKNISKE, men består av store sammensetninger av folk, organisasjoner, brukere, software, hardware og ikke minst data. Helsedata må forvaltes i datastrømmer sammen med styringsdata, konfigurasjonsdata, målerdata, sensordata og mindre sensitiv informasjon. Brukeradministrasjonen blir dessuten mer sårbar når den deles på tvers av flere instanser.

FØLELSE AV KONTINUERLIG OVERVÅKNING kan gi folk redusert tillit til helsevesenet, og dermed kan vegre seg mot å oppsøke eller ta imot helsehjelp. Samtidig er det en trygghet for mange. Godt personvern er en forutsetning for at datainnsamling og tjenester skal bli akseptert blant folk. Datatilsynet snakker om innebygd personvern, dette må kravstillere og leverandører ta høyde for.

OVERVÅKNING AV HELSEPERSONELL som besøker hjemmet er blitt en relevant problemstilling, for også disse har rett til personvern. Likevel har det hendt at pårørende velger å overvåke hjemmetjenesten med webkamera. Slike kamera kan i tillegg være sårbare for offentlig adgang via Internett hvis konfigurert feil. Hva om noen da motsetter seg fra å *gi* helsehjelp, på grunn av dette?

PÅRØRENDE SKAL GIS TILGANG til (deler av) data, varslingssystemer, osv., samtidig som noe av dette krever tydelige avklaringer opp mot taushetsplikt. Digital tilgang for pårørende gir dessuten en ekstra dimensjon til det generelle problemet med god tilgangsstyring i helsevesenet.

HVOR ER TAUSHETSPLIKTEN BRUTT med potensielt mange ulike aktører involvert i tjenestetilbudet, inkludert private aktører som kommer og går? Vanskelighetsgraden øker for å oppdage og kartlegge situasjonen, dersom dette skjer. I dag brukes bl.a. mekanisme for "blålys"-tilgang (aktualisering) for tilgang i journal når rettmessig tilgang ikke kunne forutsies, men likevel er nødvendig. Kan dette følges opp i praksis, på tvers av organisasjoner? Samtidig vil pasienter forvente at informasjon er tilgjengelig, dersom de f.eks. er ute for en ulykke et annet sted enn i regionen hvor de hører hjemme.

OPPFØLGING AV LOGGER er tradisjonelt vanskelig nok å følge opp i praksis. Igjen øker vanskelighetsgraden for å oppdage og kartlegge potensielle brudd på taushetsplikten når flere organisasjoner involveres.

HELSEDATA OG PRIVATE DATA BLANDES når data integreres fra hjemmet – hvor går grensene? Hva skal inn i en journal og hva skal holdes utenfor? Kan for eksempel søvnmønster utilsiktet si noe om seksuell aktivitet? Kan *selfies* i framtiden brukes til analyse av helsetilstanden? Det kan være uklart hvem har eierskap til dataene og hvem som er databehandlingsansvarlig til enhver tid.

BIG DATA OG ANALYSE kan være en trussel mot personvernet, der det for eksempel kreves innleie av svært kraftig regnekraft til analyse av DNA, og man implisitt oppgir identiteten til personen når man sender inn prøvene. Det kan være risiko tilknyttet aktører som ikke har noen tradisjon for å håndtere sensitive helsedata skal begynne å gjøre det. Dilemmaet er at vi får mange muligheter, men gjør oss samtidig avhengige av de eksterne og blir desto mer sårbare.

"ALLE" VIL LEVERE TJENESTER, ikke lenger bare programvare, men også ta over driften selv. Disse bedriftene har gjerne alltid vært opptatt av at programvare skal være tilgjengelig, men uten å ha selve ansvaret for drift eksponert mot Internett. Du kan samtidig ikke lage brannmur-åpninger for hver enkelt komponent fra et hjem som må kommunisere inn til en datatjeneste som er i kontakt med journalsystemet. Programvaren kan altså ikke lenger stole på at infrastruktur omkring (brannmurer, sonemodeller, etc.) tar vare på konfidensialiteten, men må være sikker i seg selv – innebygd sikkerhet.

HENDELSESHÅNDTERING ER KREVENDE øvelse, og slett ikke mindre krevende dersom det involverer en hel kjede av tjenesteleverandører. Hvem har ansvaret dersom noe går galt? Hvordan følger man opp med utenlandske leverandør(er) involvert, og hvilket lovverk gjelder egentlig?

UNDERLEVERANDØRER BLIR MÅL for målrettede data-angrep, like gjerne som helseforetak i dag. Da kreves av disse god sikkerhetskultur og tilsvarende rutiner og opplæring omkring taushetsplikt som man forventer av den helse- og omsorgssektoren for øvrig.

LIV OG HELSE er det aller mest sårbare vi har. Vi er avhengig av at informasjon og utstyr er tilgjengelig 100% av tiden til alle som har tjenstlig behov, slik at informasjonssikkerhet aldri går på bekostning av pasientsikkerhet. Samtidig skal ingen få urettmessig innsyn, verken i eller utenfor helsetjenestens virksomhet. Folk forventer at tilgjengelig teknologi blir brukt, men samtidig vil de miste oversikten over hvordan data om deres egne liv blir behandlet.

Teksten i dette vedlegget gjengir innlegg av Erlend Andreas Gjære på Lysneutvalgets workshop for helsesektoren, 21. mai 2015. Innholdet er blant annet basert på funn fra et utvalg risiko- og sårbarhetsanalyser SINTEF har utført i samarbeid med relevante aktører, uten at ytterligere kontekst, referanser, mulige tiltak og indikasjoner på sannsynlighet/konsekvens for sårbarhetene er inkludert i presentasjonsformatet.

Dette vedlegget er grunnlaget for Seksjon 4.

VEDLEGG 2: Digitale sårbarheter og tiltak i helsesektoren – en kategorisert gjengivelse av notater fra workshopen

Dette vedlegget gir en strukturert opplisting av workshop-deltakernes innspill rundt digitale sårbarheter og relaterte tiltak i helsesektoren. Innspillene er notert under alle deler av workshopen: innleggene, gruppediskusjonene og plenumsdiskusjoner. Seksjonen er delt i to hoveddeler:

1. en sammenstilling av nevnte erfaringer og synspunkter (basert på innleggene, plenumsdiskusjonene og gruppediskusjonene) i forhold til eksisterende og antatte fremtidige digitale sårbarheter i helsesektoren
2. en sammenstilling av nevnte erfaringer og synspunkter (basert på innleggene, plenumsdiskusjonene og gruppediskusjonene) i forhold til tiltak for sektoren. Med tiltak mener vi både det som bør settes i verk for å redusere eksisterende og antatte fremtidige sårbarheter, samt det som fungerer bra med dagens ordning og bør videreføres.

De opplistede innspillene kan representere deltakernes individuelle standpunkter eller felles (for forsamlingen, gruppa eller flere deltakere) meninger og erfaringer. Notatene skiller ikke mellom individuelle og felles meninger. Innspillene listet opp i denne seksjonen er sammenfattet med hensyn på en rekke tema som syns å ha vært sentrale under workshopen, etter et uttrykt ønske om en tematisk sammenfatning av funn. Temaene i overskriftene er dermed av rapportforfatteren identifisert i etterkant av workshopen, slik at de noterte innspillene lettere kunne kategoriseres og struktureres. Innspillene er derfor kategorisert med hensyn på tema og deres opplisting er dermed ikke kronologisk. Selve de opplistede innspillene er en gjengivelse av notater som ble tatt av under workshopen av tre medlemmer av Lysneutvalget og to SINTEF forskere, samt tilbakemeldinger etter deltakernes gjennomlesing av en foreløpig (intern) versjon. Dette vedlegget er grunnlaget for Seksjon 3.

Digitale sårbarheter

Tema: Dagens digitale helsetjenester – overordnet status, erfaringer og eksempler på konkrete hendelser

- Liv og helse er det aller mest sårbare vi har, vi påvirkes av systemer rundt oss, er avhengig at de er tilgjengelig 100 % av tiden, og at informasjon kun er tilgengelig for de som berettiget. Folk forventer at teknologi blir brukt og utviklingen går fremover, selv om de kanskje mister oversikten over egne data.
- Tjenester er i endring, og får en annen trusselhverdag. Er nå i ferd med å gjøre endringer og tilgjengeliggjøre systemer, ala det finanssektoren gjorde for 15-20 år siden
- Tjenester som «alltid» må være tilgjengelige - 24/7, 365
- Har ca. 400 000 ansatte, er avhengig av deres beslutninger. Manglede adferd er en utfordring - snakker om «digitalt innfødte» - ser at tilnærmingen til personvern og sikkerhet endres til kommende generasjoner
- Det benyttes fremdeles gamle systemer, ulike egenutviklete fagapplikasjoner uten noen form for sikkerhet som sikkerhetspersonell ikke får «bukt med» sårbarhet ved overføring av personlig ansvar til system (dvs. fra helsepersonellets ansvar)
- Mener det fostres «zero-risk» - men får ikke den balansen mellom risikoaversjon og risikoappetitt som trengs.
- En leverandør kan ikke forhindre at det vil ha skjedd sikkerhetsbrudd? For å kompensere for dette etableres det mekanismer for å detektere og korrigere.
- De fem største sårbarhetene sett fra en leverandørs perspektiv: endringer, tilgangsstyring, systemdokumentasjon, patching/antivirus og deteksjon.
- Topp fem digitale sårbarheter sett fra en helseregions ståsted:
    - Skytjenester

    - Opplæring/sikkerhetskultur
    - Fellesløsninger (regionalt/nasjonalt)
    - Utstyr utenfor support
    - Bortfall av infrastruktur
- Hvis systemer blir borte noen timer kan liv gå tapt. Helsevesenet har så små marginer at dersom man måtte stenge sykehusene noen dager kan det eksempelvis gå utover kreftpasienter som ikke får den kontrollen de skulle ha. Har noen manuelle rutiner og utskrifter på papir. Disse gjør at man kan holde det gående i noen timer, men ikke dager.
- Noen har også passive databaser, men dagevis uten DIPS er ikke en triviell sak for helseforetakene. Kommunene har også manuelle rutiner, men jo lenger nedetid jo vanskeligere blir det.
    - Fokus hittil har vært på to ytterpunkter av skalaen: objektsikkerhet, samt liv og helse
- Utfordringer: de teknologiske mulighetene utnyttes ikke; det er mange selvstendige aktører; mange systemer og lite integrasjon.
- Utstyr utenfor support: Mange gamle løsninger lar seg ikke lenger oppdatere software-messig eller hardware-messig.
- 2014: sendt mange millioner helsemeldinger over helsenettet. Er avhengig av at systemene rundt fungerer. Eks. at rotsertifikatet fra Buypass gikk ut – mange legekontorer fikk ikke rettet opp dette. Konsekvens: flere tusen henvisninger ble liggende ubehandlet. Årsak: manglende kompetanse og forståelse. Ser at RHF-en må bistå legekontorene, selv om det ikke er deres rolle, for å få pasienter til behandling
- Løsepengevirus – har hatt insidenter forårsaket av dette – et ondsinnet virus som krypterte filer, og som krever at bitcoin blir brukt til å sette inn på TOR-konto. Viruset begynner å kryptere nettverksfiler, og på sykehus er dette katastrofalt. Hvis man ikke har backup da, er dataene tapt. Infeksjonsvektoren fra en legitim nettside som ofte ble bruk av personellet. Siden dette er en helt ny sårbarhet er det ingen signaturer som plukket dette opp. A gå offline for å beholde kontroll under slike situasjoner er kun gjort en gang tidligere da et norsk sykehus ble rammet av Conficker-viruset.
- Privat bruk av jobbsystemer er også en trussel.
- Har stor grad av uautoriserte endringer – gjør at man ikke er sikker på hvordan man skal gjenopprette. Hvis strømmen skulle gå er det ikke sikkert man klarer å gjenopprette alle tjenester som de var, fordi endringer ikke er dokumentert noe sted.
- Utfasing kan også være krevende.
- Sanering av systemer – unikt for bransjen er at den er politisk styrt, får ikke vokse organisk. Et eksempel er at en ansatt fikk beholde operasjonsplanlegger, fordi vedkommende ikke ville bruke Dips. Å holde en eldgammel infrastruktur i live medfører enorme sårbarheter. Gjør at man som leverandør blir satt i en veldig vanskelig situasjon – informasjonssikkerhet er en veldig liten del av beslutningsprosessen høyere opp. I forhold til sanering av systemer må helseforetakene være klarere på å innordne seg de regionale føringene for IKT.
- Endepunktene er vanskelige å kontrollere, og driftsleverandørene har derfor som policy å behandle alle klienter som om de var kompromittert. Til enhver tid er 3-4 pc'er kompromittert, og det må de leve med. Kan ikke ha ambisjon om å patche innenfor det regimet som leverandører legger opp til. Eksempelvis må de regionale driftsleverandørene teste patchene på infrastrukturen før de rulles ut – kan ikke risikere at IKT-infrastrukturen bryter sammen. Vil alltid ha et delta fra en sårbarhet er kjent, til at de er implementert.
- Erfaringer fra Heartbleed viste at organisasjonen har utfordringer med nødpatching på serversiden.
- Patcher må testes på infrastrukturen først, noe som tar tid.
- Klienter (endepunktene) er kronisk usikre – vedvarende en sikkerhetsrisiko på alle måter – stoler på ansatte, men ikke på klientene.

Tema: Nye teknologitrender og nye driftsmodeller

- Big data er en utfordring – noen aktører kan gjennomføre mer analyse/sammensying enn ønsket.

- Nettsky –hjelp til stor regnekraft kan medføre at sensitiv info blandes.
- Outsourcing og sky kan by på nye utfordringer.
- En utfordring at aktører uten tilstrekkelig erfaring ønsker å ta over drift.
- Vanskelig å finne den ansvarlige/skyldige ved hendelser, i en nettsky scenario.
- Folk forventer at teknologi blir brukt, vanskelig å ha oversikt over hvordan data blir behandlet.
- Globale kommersielle aktører vil på mange måter kunne overta vår informasjon – da vil denne bli spredt – noe på privat nettsky, noe offentlige, noe på mobiltelefoner mv. Vil kunne få blanding av private og offentlige helsedata. Dette gjør det vanskelig å definere hva som er privat og hva som er offentlig?
- Nettsky kan brukes til prosessering og medisinsk utstyr. Hva slags informasjon blant dette er sensitiv? Kan man eie dataene selv? Vil kreve en rekke avveininger fremover.
- "Alle" vil lage tjenester – de vil ikke lenger bare levere programvare, men ta over driften. Disse er tradisjonelt opptatt av at programvare skal være tilgjengelig, men informasjonssikkerhet er mer enn bare tilgjengelighet. Må lage programvare-løsninger som er sikre i seg selv fremover, og ikke stole på at infrastrukturen rundt tar vare på alt.
- Hvordan avklare ansvar på tvers av landegrenser?
- Fellesløsninger (regionalt/nasjonalt): samler man mye informasjon i sentrale løsninger kan det bli utsatt.
- Trenden med big data – det kommer til å bli en større problemstilling fremover. Eksempelvis vil man i Norge kunne gjenkjenne enkeltpersoner. Eksempel fra England hvor altfor mye informasjon er lekket allerede, og solgt til industrien. Helseregioner sender allerede i dag data til England for å analysere disse og sammenligne med andre land.

Tema: Utstyr og tilknyttet programvare

- Utstyr er på vei inn i private hjem og pålideligheten til utstyret kan være variabel.
- Medisinskteknisk utstyr er i en rivende utvikling.
- Markedet for IOT er estimert til et par billioner dollar frem til 2020. Mener det er teknologileverandører som på mange måter setter premissene for det som kommer, og at det ikke alltid er sikkerheten som er i høysetet.
- Hjemmet vil være behandlingstedet fremover, men er også sårbart. Infrastrukturen her er privat – kanskje delt, kanskje er andre private og offentlige aktører i bildet: helsetjenester, vaktselskap, strømleverandør m.fl. Det vil kunne bli et virvar av ulike tjenesteleverandører, i tillegg til at data skal integreres og lagres. Økt bruk av BYOD er også en problemstilling.
- Videobasert konsultasjon gjøres allerede i dag i Nordsjøen. Dvs. folk blir utstyrt med medisinsk utstyr hjemme, som gjør det mulig å gjøre grunnleggende diagnose hjemmefra. En forutsetning er å kunne kommunisere med helseinstitusjoner. Da fordrer dette at det er en åpen og standardisert plattform. Teknisk oppsett på brukersiden må forbedres for at dette skal kunne gjøres
- Ser også på app-siden – et utall apper som kan lese av helse, og koble seg opp mot diagnoseutstyr mv. Selve mobilen vil også være en sårbar enhet – ikke driftet av noen helseenheter, men kan være et veldig nyttig verktøy i fremtiden.
- Helsetjenester blir trukket hjem til folk, slik at man snakker om " det utvidede legekontoret". Da har man plutselig 5 millioner mennesker og enheter. Vil man få et ansvar for at disse er på nett? Vil man trenge et varsel om at disse enhetene er på? Vil introdusere risiko, og hva er sårbarheten for det? Hvor setter man terskelen? Privat bruk vil antagelig i fremtiden vokse inn i tjenestene. Da blir det utfordrende med hvem som skal drifte disse tjenestene. Hvordan ansvarliggjøre det? Helsetjenesten blir nødt til å overføre mer til de private, men hvem er de private? Er det enkeltpersoner, eller virksomheter som et mellomledd? Viktig at dette ikke bare omhandler personvern, eksempelvis vil enkeltpersoner ønske å publisere sine data?

Tema: Kommunene i samspill med leverandører og sektoren

- Manglende virksomhetsstyring i forhold til digitalisering og ikt-utvikling.
- Virksomheter både blant kommunene og i helse- og omsorgssektoren mangler digitaliseringsstrategi. Manglende digitalisering kan også i mange tilfeller være en digital sårbarhet – man innfører elektroniske verktøy men endrer ikke arbeidsprosesser og henter ut gevinstene ved investeringen – og ender da mest sannsynlig opp med systemer som er mindre sikre for innbyggere og pasienter.
- Uavklarte ansvarsforhold mellom leverandører og databehandlingsansvarlige;
- Målrettede angrep; dette ser vi i større grad enn tidligere. Det blir stadig mer krevende for bransjen å holde tritt med trusselbildet. Vi anser dette som en utfordring for bransjen generelt – mer enn en spesifikk utfordring for egen virksomhet.
- Sikkerhetshull gjennom velferdsteknologi og internet of things; dette er på full fart inn hos både kommuner og private virksomheter. Stiller store krav til både databehandlingsansvarlig og databehandler i forhold til sikkerhetskultur, risikobevissthet og strategi for digitalisering.
- Private selskaper har ofte avtale med helseforetakene i forhold til å levere for eksempel rehabiliteringstjenester eller andre helsetjenester. Disse private aktørene vil mest sannsynlig bli viktigere i tiden som kommer for å bidra til at befolkningens behov for helsetjenester dekkes.
- Kommunene får i stor grad støtte av KS, Helsedirektoratet og helse- og omsorgsdepartementet og blir pålagt å følge nasjonale føringer og programmer. De private helsevirksomhetene har ikke samme fokus fra sentrale myndigheter.

Tema: Kommunale velferdstjenester

- Å gå fra analog til digital trygghetsalarm, er for en kommune et stort løft å gjøre alene.
- Ved utvikling og innføring med kommunale velferdstjenester er det i starten mye fokus på funksjonalitet, andre problemstillinger kommer ved skalering.
- Man beveger seg fra det tradisjonelle "alt i eget hus", og vil fremover få distribuerte løsninger. I utprøving har man hatt fokus på om produktet i seg selv er godt, men når man skal skalere i kommunisere kommer det nye utfordringer, eksempelvis:
    - Personvern
    - Varsler eller posisjoner kommer ikke frem til mottaker
    - Forvaltning (hvor og hvor lenge lagres dataene mv)
- Har valgt å gjøre risikoanalyser knyttet til kommunens velferdstjenester i pilotprosjektene.
- Hva når tjenestene på sikt går på tvers kommunegrensene, for eks. mobiltrygghetsalarm?
- Pleie- og omsorg i kommunene har svake systemer

Tema: Utfordringer knyttet til underleverandører

- Erfaringer fra hendelser viser at mange av hendelsene skyldes underleverandørene. Gjelder særlig feil på strømleverandør m.v.
- Underleverandør kan være mål for målrettede angrep.
- 50 % av omfattende episoder med beredskap de siste år skyldes svikt hos underleverandør.
    - Særlig feil på strømleveranse og arbeid på sterkstrømsanlegg
    - Tilfeller av at ekstern leverandør har gjort oppgradering av f.eks. telefonisentral som har gitt ustabilitet.
    - Lynnedslag, brudd på datalinjer, cluster som feiler.

Tema: Sikkerhet og kvalitet av helsedata

- Integritet og tilgjengelighet er viktig for liv og helse.
- Deling på tvers av helseforetak er noe pasienten i stor grad vil, for at legene skal kunne vite nok om dem der de søker hjelp.

- Som pasient må man forholde seg til mange aktører. Man er avhengig av at informasjonen følger med pasienten.
- Se stortingsmelding "Èn innbygger – èn journal" som påpeker at de teknologiske mulighetene ikke utnyttes. Det er mange selvstendige aktører, mange systemer
- Tre mål uttrykt i "Èn innbygger – èn journal". Har gjort endringer i journalloven fra 1.1.2015, som gjør det mulig for RHF å ha et felles epj og som gjør det enklere å samarbeide med pasienter. I tillegg pågår det arbeid med utredning av fremtidsutfordringer.
- Èn innbygger – èn journal – hvordan skal man forholde seg til det som strategi? Kan snakke om en hovedjournal, men vil likevel være en rekke journaler som ikke vil kunne avgi informasjon til hovedjournalen Èn innbygger – èn journal er en visjon. Hvordan det skal gjøres jobber Hdir med å utrede nå.
- Legeforeningen har vært positive til visjonen "Èn innbygger – èn journal" – at de som yter helsehjelp skal få tilgang til den informasjonen de trenger. Et tankekors at de som er mest opptatt av dette ikke bruker informasjon til å yte helsehjelp, men for å gjenbruke informasjon. Jo mer standardisert/strukturert informasjon man lager jo mindre handlefrihet for den enkelte. Bør ha mer fokus på helsepersonellets bruk av journalen, og ikke så mye fokus på gjenbruk.
- Det er en underkommunisert utfordring knyttet til elektronisk pasientjournal. Hva er farligst ved å vite at det er informasjon man ikke har, fremfor at man tror man har fått informasjon man trenger, men som man ikke har fått, fordi den ligger et annet sted? Dette er en problemstilling ved visjonen.
- Ved distribuert journal er det en utfordring at man ikke vet hva man ikke har tilgang til.
- Epj-systemenes troverdighet (dvs. kvaliteten på den tilgjengelige informasjon) er avgjørende for faktisk bruk, de må ha både positiv og negativ troverdighet, altså at det som er nedtegnet er korrekt og at det ikke er relevant informasjon som ikke er lagt inn.
- Struktur er avgjørende både for gjenfinningsmulighet og troverdighet
- Pårørende får en del tilgang; og det er vanskelig å få til tilgangsstyring i praksis.
- Det kan også være vanskelig å få til hensiktsmessig tilgangsstyring og sporing i forhold til brudd på taushetsplikt. Brukeradministrasjon i forhold til distribuerte systemer er utfordrende.
- Blanding av helsedata med private data er en utfordring.
- Avhengig av 100% tilgjengelighet og at info er 100% kun for den som er berettiget.
- Tilgangsstyring, logger osv. – det er utfordringer med å følge opp dette.
- Tilgangsstyring er et problem – det er vanskelig å holde oversikt på hvem som skal ha tilgang på hva.
- Langvarig nedetid er i ROS-analyser er definert som 4 timer.
- Samhandling er utfordrende. Kan man i kontekst av fritt sykehusvalg ta med dataene sine?
- Integritet vil bli enda viktigere fremover – det tas ofte for liten hensyn til dette. Er det en økt sårbarhet at man får flere feil, eller at man ikke oppdager det man skal?

Tema: Utfordringer knyttet til personvern

- Personvern er en utfordring, sporing er tilstede i større grad enn helt nødvendig.
- Noen kan avstå fra medisinsk hjelp hvis de føler seg overvåket.
- Innsyn i loggene er vanskelig når loggene er spredt i ulike systemer.
- Hvor er personvernet i den nye tjenesten? Det man strengt tatt trenger å vite er at GPS er online og at batteri er ladet, ikke å kunne spore en pasient til enhver tid. Datatilsynet snakker om innebygd personvern, dette må leverandørene ta høyde for.
- Ser eksempler på at pårørende installerer webkamera for å følge med – hva hvis helsepersonell tar avstand fra å gi helsehjelp fordi de føler seg overvåket? Med stort omfang av leverandører – hvordan finne ut hvor personvernet ble brutt?
- I diskusjoner ser man ofte «alle pasienter ønsker sikkerhet og personvern». Flertallet lever godt med de reguleringer man har, men det er mindretallet vi må beskytte. Personvern er en menneskerett vi

har hatt. Stadig oftere at man ser at flertallet ønsker en løsning, selv om den kommer på kant med personvernet. Eksempel på at enkeltpersoner må kunne komme til behandling hos lege, uten at pårørende kjenner til det, kan være svært viktige grunner til å skjerme enkeltindivider.

Tema: Brukervennlighet av systemer og opplæring

- Helsepersonell sliter med å forstå systemer grunner bl.a. økende kompleksitet.
- Også en utfordring at brukerne ikke forstår konsekvenser at handling i forhold til bruk av verktøy. Ulik bruk av verktøy medfører varierende datakvalitet. Det er lite fokus på konsekvenser som skapes når ting går galt.

Tema: Ansvar for IKT-sikkerhet

- Det oppleves som et problem at både ledelse og brukere ikke er nok bevisst sitt ansvar innenfor IT-sikkerhet.
- Det kan være vanskelig for ledelsen å forholde seg til IT-sikkerhet enten på grunn av manglende kunnskap, men også fordi IT-sikkerhet skiller seg fra andre områder hvor man også har styringsansvar.
- Leverandøren har blitt premissgiveren til RHF-et, øvrige (systemeiere) som har faglig kompetanse både på helse og IKT, blir ikke tatt med. Systemeiere har liten innflytelse på systemer. Ansvaret i forhold til dette er uklart.
- En direktør som er behandlingsansvarlig har begrenset reell innflytelse på (valg av) IKT-løsningene.
- I kommunal sektor hat ledelse og eierskap har vært savnet.
- Hva skal man gjøre hvis helsesektoren er delvis ansvarlig for det som står i hjemmene til folk?
- Det at noen får fortsette å kjøre systemer fordi de ikke vil bytte – hva skyldes dette? I stor grad manglende bevissthet? Men helseforetakene står fritt i forhold til å bestemme hvilke anskaffelser de skal gjøre. Ser nå en endring at de regionale helseforetakene flytter mer makt fra et helseforetak/sykehus til det regionale leddet. Tjenesteleverandøren tar ikke beslutningen, det er foretakene som bestiller. Mye skyldes at man er politisk styrt. Helsepersonell opplever at det er veldig langt igjen – de må få hverdagen til å gå. Det er lite dialog mellom helsepersonell (som står overfor enkeltpasient) og de som sitter langt unna.
- Utfordring at man som systemeier lokalt har ansvar men ikke innflytelse. De som har ansvar må også ha innflytelse. Alternativt må de som har innflytelse på systemer også ha ansvar. Men i USA har leverandørene fått inn klausul på at dersom en pasient dør er det ikke leverandøren som har ansvar, men legen som har behandlet
- HF ene har for liten påvirkning på innkjøpssituasjonen i forhold til det ansvaret de har for systemenes funksjon, for eksempel databehandlingsansvarlig er den enkelte direktør for helseforetaket, men beslutning om hvilke systemer som kjøpes inn ligger i sykehuspartner, helseVest IKT osv.

Tema: Kommunikasjon mellom aktører

- Det er et problem at informasjon fra HoD/Hdir ikke når frem til brukermiljøene i helseforetakene (f.eks. databehandlingsansvarlig, relevante IT-miljø). Informasjon og forespørsler fra HoD og Hdir blir rettet direkte til RHFene. Disse siler informasjon og styrer hva de vil sende videre og til hvem. RHFene har heller ikke direkte kompetanse på IT-sikkerhet. Man kan dermed risikere at informasjon/forespørsler ikke når frem til de relevante miljøene i helseforetakene, eller at informasjon kommer frem for seint til at man rekker å gjøre noe med den, som f.eks. høringsuttalelser.
- Det er utfordringer knyttet til kommunikasjon med andre helseaktører – eksempelvis rundt fellesløsninger, elektronisk meldingsutveksling, tilgangsstyring mv. Har også utfordringer med sikker kommunikasjon, nøkkelutveksling mv. Ser også at tekniske systemer ikke klarer å ivareta de kravene lovene stiller til behandling av helseopplysninger. Kan også være vanskelig med kravstilling til internasjonale leverandører.

- De største utfordringene knyttet til sikring av sensitiv informasjon er manglende klassifisering av informasjon, manglende mulighet for sikker tilgjengeliggjøring av informasjon på tvers av virksomheter, manglende databehandleravtaler og manglende kapasiteter på logganalyse. I tillegg kommer alle utfordringene knyttet til kommunikasjon med andre helseaktører.
- Hva er mest kritisk for pasientsikkerheten og for pasienten som sluttbruker? Ivareta taushetsplikten og at informasjon er tilgjengelig for de som skal ha informasjonen? Kan bli store konsekvenser ved langvarig bortfall av eksempelvis elektronisk kommunikasjon. Det å få riktig tilgang til relevant informasjon? Medisinskteknisk utstyr er kritisk, man klarer å leve uten DIPS noen dager. Akuttfunksjonene vil nok fortsette å behandle selv om digital samhandling opphører. Men kommunikasjon mellom sykehusene, vil stoppe opp, kommunikasjon til sykehus og fastleger vil stoppe opp. Den samhandlingen vil bli mer og mer viktig fremover.

Tema: Behov for standarder og felles rammeverk

- Er det for svakt at Difi bare "sterkt anbefaler" ISO27001?
- Har krav til beredskap, tilgjengelighet, men ikke på standard-nivå (ISO). Få inn risiko inn i ledelseshjul?
- Man forstår ikke hvor viktig IKT er for systemet. Standardisering på en gitt standard har en kostnad.
- Det er ikke standardisert forvalting av systemtekniske beskrivelser og infrastrukturinformasjon, siden det ikke er sensitive personopplysninger.
- Styringssystemer som gjøres litt annerledes enn hva en leder er kjent med (f.eks. sikringsanalyse fremfor RoS-analyse), slik at man slipper å koble inn fagpersoner hele tiden i våre egne litt ulike fagfelt. Er det behov for en nasjonal standard for styringssystem? Heller se på hva som er felles, enn hva som er forskjellig.
- Bruk av standarder løser ikke nødvendigvis problemer, her vil varierende grad av kunnskap, kultur og språklig fortolkning likevel skape store ulikheter.
- Standarder som brukes for meldingsutveksling baserer seg på internasjonale standarder. De som driver medisinskteknisk utstyr får ikke tilpasset sikkerhetskravene, fordi det er internasjonale standarder som setter kravene
- Tror Norge ligger foran i bruk på IKT i helsesektoren - langt foran USA, NL m.fl
- Norge er verdens beste land til å følge EU-direktiver?
- Innen velferdsteknologi har man samarbeid gjennom Continua
- Så langt har nasjonale leverandører dominert i markedet
- På infrastruktursiden har man leverandører fra hele verden.
- Velferdsteknologi vil i stor grad bli levert fra utlandet?

Tema: Avhengighet av infrastruktur

- Den aller største sårbarheten er avhengighet til telekom, på grunn av viktigheten av kommunikasjon. Kritisk avhengig av det for alle tjenester - varslinger, personsøk mv.
- Bortfall av sentral infrastruktur er en trussel.
- Avhengighet til vann og kloakk er en sårbarhet – sykehus må stenge etter få timer om dette bortfaller.
- Bortfall av teknisk infrastruktur er livsfarlig. Kanskje ikke så farlig hvis man allerede er på sykehus. Men dersom man er utenfor vil man ikke få inn pasienter, ambulanser mv. Se DSB rapport som anslår antallet dødsfall pr. uke Noen av de store helseforetakene har redundante løsninger for strøm/datarom.

Tema: Beredskap, sikkerhetskultur og øvelser

- Øvelser er veldig viktig. Vi er veldig gode på øvelser f.eks. Ebola. Men gjør ingenting innen øvelser på digitale sårbarheter.

- Bra om man klarer å identifisere risiko – men sårbarheten er avhengig av hvordan man møter den risikoen.
- Opplæring/sikkerhetskultur: Mange hendelser inntreffer som følge av manglende opplæring, holdninger og årvåkenhet. Har en regional sikkerhetsinstruks, undersøker årlig hvor mange som kjenner til denne. Ser at trenden er nedadgående, vurderer derfor å styrke bruk av e-læringsprogrammer.
- Øver for lite på kritisk infrastruktur – og bygger ikke dette godt nok inn i eksisterende øvelser. Eks. ble det kjørt øvelse i Hdir for 2 år siden i forhold til e-Resept, som ikke var planlagt. Fordel: får vite svakheter med en gang, men må kjenne sine begrensinger og ikke kjøre over for lang tid.

Tema: Andre sårbarheter som bør omtales og øvrige innspill

- Må stresse det poenget at hvis man skal modernisere helsevesenet så må øvrige sektorer følge etter. Kan ikke operere med gammelt lovverk. Hvis innbyggerne ønsker høy grad av tilgjengelighet, så flyttes ansvaret over til den enkelte. Blir et mer sårbart folk, men kanskje ikke en så sårbar helsetjeneste?
- Kjenner igjen alle problemstillingene. Men det føles som om de som snakker ikke har satt sitt ben i helsesektoren. Eks. «hadde bare legene og sykepleierne gjort som jeg sa», fremfor at man analyserer *årsakene* til at de ikke gjør det. Mangler dialog mellom teknologer og helsepersonell. Mener pasientperspektivet ofte er fraværende.
- Mye av det som har skjedd er IKT-styrt, og ikke styrt etter arbeidsprosesser. Dette representerer en sårbarhet. «For mange ingeniører». Andre i gruppen mente at man forsøker å få til høy grad av faglig forankring, både når det gjøres ROS-analyser, men også når nye systemer introduseres. Etterlyses at flere klinikere/helsepersonell blir inkludert inn i arbeidet.
- Tidligere var man bedre på å involvere helsepersonell. Det er stilt spørsmål om dagens gigantprosjekter er brudd på tjenestemannsloven, ettersom helsepersonell ikke blir trukket inn i tilstrekkelig grad. «På 80-tallet var man opptatt av å *spørre* brukerne, på 90-tallet *forstå* brukerne, men nå *ignorere* brukerne – de blir ofte bare tatt med som gissel.
- Man er mest sårbare i overganger mellom organisatoriske enheter, mellom sykehus, kommuner mv., fordi man er svært ulikt organisert mv. Er nå i en utvikling med å få nasjonale løsninger, store datasentre. Gjør dette at Norge som samfunn blir mer sårbart, ettersom det rammer hele virksomheten? Desentraliserte løsninger fikk mer lokale virkinger, men samfunnet gikk videre. Gjør utviklingen oss mer eller mindre sårbare?
- Logganalyse – forsøk på uautoriserte oppslag i journal. Se mønstergjenkjenningsprosjektet – dette er svært viktig. Eks. i Danmark kan man få SMS om noen har snoket i journalen din.
- Bransjen synes å starte forfra med alle problemer. Eks. strukturering av journal – jobbet med dette i 50 år. Hadde man startet med å lese eksisterende litteratur, ville mye vært enklere
- Hva kunne man ha gjort dersom man *ikke* måtte følge disse store prosjektene? Eks. sitter enkeltsykehus med gamle systemer som er en risiko for sykehusene, fordi de må i påvente av en ny felles løsning for regionen. Alle de store prosjektene har en tendens til å bli så store at de ikke kommer i mål.
- Etter 22.juli - to ting fra helsesektoren har fått spesielt fokus:
    - De regionale AMK-tiltakene har ikke systemer som kommuniserer. Her er det satt i gang initiativer.
    - Innføring av nødnettet vil også redusere sårbarhetene
- Helsesektoren blir i større grad konkurranseutsatt enn før – styrke pasientens valg, som gjør at både innad i privat sektor og mellom offentlig og privat sektor får man økt konkurranse. Det gjør at man kanskje ikke vil vise alle kortene, ettersom man er i en konkurransesituasjon.
- Når brukeren og befolkningen tar i bruk teknologi vil det kunne bli større grad av tilfeldighet, og som kan gjøre sektoren mer sårbar.
- Helsepersonell sier at man øver ukentlig, fordi systemene går ned. Trenger ikke øve, fordi det skjer jevnlig.

- Har vært lite utsatt for outsourcing, på grunn av lovgivning. Tror man vil bli utfordret der på mellomlang sikt. Land som aksepterer den type virkemidler (eks trussel om å legge journal på nett hvis de ikke får lønnsøkning) bør man kanskje ikke outsource til.
- Hva finnes av dokumentasjon – senter for klinisk dokumentasjon og forskning i Troms: Hvor mange har sett på digitale skadekonsekvenser?
- Digitale kjølesystem/styringssystem er en tjeneste som er viktig for drift av sykehus. Disse er ofte underlagt annen administrasjon enn IT-drift. Slike system styres over nettet og er dermed sårbare for angrep og hendelser. Dersom man mister evnen til å kontrollere temperatur i et sykehus vil det gå ut over evnen til å behandle pasienter.
- Redning er en viktig del av helsetjenesten, men ikke underlagt HOD. Bør se til redningssentralene, samt viktig prosjekt som pågår - SAR i Nord, samt Akuttutvalget.
- Det ble savnet et klinisk perspektiv inn i diskusjonene, det ble mye teknologidrevet. Den kliniske siden sier det er for mange ingeniører.

Tiltak for sektoren

Tema: Kommunale velferdstjenester

- Det som trengs av kommunene er bestillerkompetanse i forhold til krav til leverandøren. Men også kommunikasjon – hvem har ansvar for hva?
- Håper velferdsteknologi-prosjektet fra Hdir kan komme ut med noen anbefalinger?
- Hvordan spres erfaringer en kommune gjør? Nasjonalt program for Velferdsteknologi – 31 utviklingskommuner deltar her - gjennom dette spres kommunes kunnskap. I tillegg finnes det annet kommunesamarbeid.
- Det er et samarbeid mellom KS og Hdir på velferdsteknologi og opprettet arenaer for erfaringsutveksling.

Tema: Sikkerhet og kvalitet av helsedata

- Tilgjengelighet veier tungt, og adresseres gjennom redundans og backup.
- NHN holder på å etablere georedundante løsninger. Å få mange av de nye tjenestene som blir levert til å være georedundante, og ikke kjøre på et datasenter.
- Konsekvensene av bortfall av epj-informasjon må komme tydeligere frem, hvis dette området skal anses som en vesentlig sårbarhet, her er det ulike oppfatninger

Tema: Brukervennlighet av systemer og opplæring

- Det er viktig med opplæring, da det er mye turnover i sektoren.
- Norm-sekretariatet reiser rundt og holder kurs for hele sektoren, inkludert kommuner (også mindre tannlegekontorer).
- Når man skal engasjere brukere er det viktig at man lager enkle prosedyrer som kan integreres i daglig drift, på linje med HMS-runder. Informasjon om IT-sikkerhet til brukere bør også være mest mulig konkret, og gjerne ta utgangspunkt i aktuelle hendelser og scenarier. De ganger dette har vært gjort har det ført til større forståelse om hva som kreves av den enkelte samt økt forståelse for gjennomførte tiltak.
- Ledelsen må utdannes, ellers blir det mye tilfeldigheter i forhold til hvor mye kompetanse og kunnskap som blir med.

Tema: Ansvar for IKT-sikkerhet

- Det oppleves som et problem at både ledelse og brukere ikke er nok bevisst sitt ansvar innenfor IT-sikkerhet. Det er viktig at man definerer og bevisstgjør alle parter: Bruker, Eier og Drifter. Alle må være klar over hvilken rolle de har og hva deres ansvar er.

- Det kan være vanskelig for ledelsen å forholde seg til IT-sikkerhet enten på grunn av manglende kunnskap, men også fordi IT-sikkerhet skiller seg fra andre områder hvor man også har styringsansvar. En mulig løsning på dette er å fokusere på det som er felles med andre styringssystem, som f.eks. HMS. Det er også viktig at linjene for rapportering av IT-sikkerhet går mest mulig direkte til ledelsen. Dette gjør at man unngår siling av informasjon, samtidig som det bevisstgjør ledelsen på ansvaret den har.
- Også fra et kommuneperspektiv bør øverste nivået ta et større ansvar. Leverandørene må også ta et ansvar, men de som virkelig kan utfordre dem er de som skal kjøpe tjenestene fra dem. Veldig mange stoler nok for mye på det leverandøren sier.
- Paradoks at det blir uttrykt at PKI/NSI på nasjonalt nivå er for tidlig. Gjør at helsesektoren må skaffe det selv, fordi man ikke har en nasjonal infrastruktur. Her er det rom for å handle inn smartere. Bruker mye tid og ressurser på semi-proprietære løsninger fra private aktører. Føler at man som tjenesteleverandør blir overlatt til seg selv, ønsker at deres eiere burde lage standarder.
- I forhold til «ansvarliggjøring av de ansatte» – man jobber målrettet etter ISO 27001, men ansvaret ligger hos ledelsen. De må legge til rette for at det blir gjort på en sikker måte. Syns det ofte blir pålagt enkeltpersoner å ivareta for mye IKT-sikkerhet, det må man fra ledelsen legge til rette for at ikke skjer, eksempelvis med tekniske mottiltak

Tema: Kommunikasjon mellom aktører

- Hvis RHF-er tar beslutninger uten å involvere de lokale foretakene, hvordan skal man da gi eierskap? Det handler om å være med fra starten av og passe på at også direktørene i foretakene, ikke bare RHF-ene er involvert. RHF er ikke databehandlingsansvarlig, og da må departementet kommunisere med foretakene. Et mulig tiltak kan være at HoD/Hdir identifiserer relevante mottakere som må få informasjon direkte, parallelt med det som sendes til RHFene.
- Generelt etterspørres det strammere styring fra HoD for å sikre standardisering i IT-prosesser. Et konkret eksempel er at det oppleves som et problem at det ikke finnes mere standardiserte rutiner for å vurdere IT-sikkerhet ved innkjøp. Dette gjelder både generelle IT-system og spesifikt helseutstyr med sterk IT-komponent. Man har opplevd å bli møtt med "men Helse-X har allerede godkjent denne".
- Det er ønskelig at HoD/Hdir tar initiativ til å opprette mere standardiserte rutiner på tvers av sektoren og sørge for at disse brukes.

Tema: Beredskap, sikkerhetskultur og øvelser

- Øvelser er viktig. Vi øver på det meste, men det man ikke får mulighet til å øve på, er redusert bemanning.
- Trenger beredskapsplaner og øvelser i forhold til situasjoner når journalsystemer er ute av funksjon
- Kjennetegn for helsesektoren viser at man er gode på beredskap og manuelle rutiner.
- Må fortsette å øve og bli gode på håndtering av hendelser.
- En region har gjort test med å kjøre på nødrutiner over en hel helg – og det virket. Bortsett fra dette trengs flere øvelser.
- Det bør gjennomføres flere rene IKT-øvelser i helsesektoren. Helse SørØst har ikke gjennomført noen slike øvelser så langt.

Tema: Felles tiltak – samarbeid, standardisering og styring

- Det ble etterlyst en overordnet strategi og styring. Det ser ut som man «lar 1000 blomster blomstrer». Viktig at man ikke bare setter i gang med masse enkelttiltak som ikke henger sammen. Eksempelvis kom 22.juli-kommisjonen opp med mange tiltak, men viktig at man tar en grundig debatt på dette, og hva som bør prioriteres). I stor grad finner mange opp hjulet på nytt.

Hvem er riktig adressat? Det må være HOD. Hdir er ikke alltid koordinert allerede i dag, med delingen vet man ikke hva man får. Det er risikabelt.

- Sterkere nasjonal styring, også for å styrke felles behov og for å unngå konkurranse mellom regionene
- Det bør også stilles krav til andre sektorer, siden det er mye som utveksles.
- Behov for nasjonal samordningsgruppe mellom departementene, hvor dette med informasjonsbehandling blir inkludert. Mangel på dette vil avskjære muligheten for erfaringslæring mellom sektorer. Mange finner opp hjulet på nytt
- Informasjonsutveksling i akutte situasjoner – der vil det nok trengs tiltak. Må ta i bruk risikostyring her – at ledelsen ser på noen overordnede tiltak som skal implementeres.
- Helsemessig «Kube» - kunne man bygget noe tilsvarende for informasjonssikkerhet? For å rute henvendelser fra alle utvalg, Riksrevisjonen mv. Dette stjeler ressurser fra foretakene.
- Man bruker IKT til å standardisere sykehusene, mens det burde vært omvendt.
- Spesielt for kommunesektoren, med mange små aktører og mangelfull kompetanse hos de mange mindre kommunene bør det vurderes større grad av leverandøransvar
- Trenger sikkerhetskrav i innkjøpsprosessene.
- Det ble etterlyst en strategi for overordnet styring – hjulet blir i stor grad oppfunnet på nytt.
- Viktig med felles tiltak i kommunesektoren.
- Det er behov for at systemeier/virksomhetsledelse i mye større grad tar grep om digitalisering i egen virksomhet og ikke lar dette være overlatt til IKT-ansvarlig.

Tema: Kompetansebygging, undervisning og forskning

- Helseinformatikk – både inn i utdanningen og i forskning. For lite evaluering av det man jobber med.
- Hvem skal bruke informasjon i hvilke løsninger? Se prosjekt i USA – hvordan informasjon skal flyte mellom offentlige myndigteter. Jobbes med arkitekturer på hvem som skal ha tilgang til informasjon i hvilke situasjoner. Eierskap til data – hvem skal eie disse? Dette er ting man må jobbe opp å se på tvers i hele helsevesenet. Kan sikre og kryptere dataene, slik at man sikrer dataene mens de flytter seg over ulike domener, ikke bare når de er lagret.
- Må ikke skille teknologi og det faglige, fagfolk må kunne sette premisser, slik at det blir forankret i virksomheten i dag. Her er det mange parallelle – to spor – som ikke er koblet.
- Viktig å involvere helsepersonell i hverdagen i større grad enn det som gjøres i dag. Teknologiverdenen må akseptere at bransjen kan ha et annet synspunkt. Det må jobbes langsiktig for å bygge opp den kompetansen og forståelsen som trengs for å forstå systemene i sektorene. Ha med noen som har forståelse for arbeidsprosesser, strukturering av informasjon mv.
- Forskning? Kan forske på anonyme data, avidentifiserte data, det gjør ting mye enklere
- Helseinformatikkforskning – det gjøres veldig liten forskning på konsekvensene av det som innføres. Det er veldig liten evaluering av alle disse store IT-prosjektene, og får ingen konsekvens. Kunne trengt en mer akademisk tilnærming til helseinformatikk.
  Bør også opplæring inn i utdanningen - lærer ingenting om dette i utdanningen i dag.
- Det er veldig få akademiske miljøer på helseinformatikk – kun noe ved HiB, Tromsø, Agder, Gjøvik (++?)
- Helseinformatikk som fag (utdanning og forskning) bør fokuseres mer på – det er for lite evaluering av temaene som blir diskutert under denne workshopen.
- Digitalisering, informasjonssikkerhet og personvern bør inngå som tema i utdanningsprogram som for eksempel ny nasjonal satsning på lederutdanning i primærhelsetjenesten

Tema: IKT som tiltak for økt pasientsikkerhet

- Når pasienter påføres skader gjennom behandling uten at det har noe med IKT å gjøre, er spørsmålet om IKT kunne blitt brukt som tiltak mot dette?
- Det er mer nærliggende å tro at verktøy skal støtte og stille understøttende spørsmål, ikke at man skal lene seg til verktøyene.
- Datasystemene bør kanskje «spørre mer», etterlyse om ulike tiltak er gjort, som støtte for forsvarlig pasientbehandling
- Dersom pasientsikkerhetsperspektivet er avgjørende må man se på summen av systemer langt utover det som omtales som et enkeltstående epj-system, det er summen av samtlige systemer og aktiviteter som er avgjørende, for eksempel transport operasjonsstuas funksjoner osv.
- Det er dokumentert at ca 10% av pasientene som behandles på sykehus blir skadet som følge av behandlingen, IKT/epj, har ikke ført til noen nedgang i disse skadene – et tankekors?

Tema: Hva fungerer bra i dag (og ønskes videreført)?

- Man har oppnådd bedre sikkerhet med Dips enn tidligere – må ikke glemme gevinstene dette har medført
- Leger og sykepleiere tenker fortsatt selv – dette er en styrke. Kan havne i en situasjon langt frem, hvor man ikke venner seg til å tenke selv, fordi man er vant til at systemet tenker for deg
- Helse CSIRT ble trukket frem av flere. Det har medført en betraktelig kvalitetsheving av IT-sikkerheten. HelseCSIRT er et tiltak som fungerer bra, men må samtidig opprettholde kompetanse i regionene.
- HelseCSIRT gjør en viktig jobb for sektoren – en massiv bidragsyter til å heve informasjonssikkerheten i sektoren. Men likevel viktig at det ikke blir en hvilepute for de regionale – de er fortatt ansvarlige for håndtering lokalt, og må være i stand til dette.
- Normen er også bra, men det er behov for oppdateringer. Enkelte forslag til tiltak oppleves som utdaterte. Det etterlyses også mer konkrete forslag til hvordan man skal forholde seg til IT-sikkerhet.
- Normen er en god veileder for folk flest, selv om det er mange som har andre meninger om den. Eksempelvis passer den ikke for de aller minste helseforetakene. Mange av de som skal bruke den vil ikke ha ressurser til å følge opp normen, fordi den er for omfattende.
- Normen kan gjerne bli enda mer tydelig på enkelte områder, selv om mange av fakta-arkene er bra. Den har bidratt mye. Normen bør også styrkes og aktualiseres. Normen gjør at vi tør å stille krav, og leverandørene blir mer obs på temaet. Det blir et tema i anskaffelsene, til og med kapselendoskopi.
- Helsenett trekkes frem som et velfungerende samarbeid
- Har erfaringer med å håndtere hendelser – er i beredskap hver dag. Til tross for en del misnøye med dagens løsninger er alle enige om at man ikke vil tilbake til der man var

Tema: Øvrige tiltak og innspill

- Det ble etterspurt en klassifiseringsmulighet for informasjon som man ikke ønsker skal falle under offentlighetsloven, men som heller ikke faller under sikkerhetsloven. Eksempel som nevnes er beskrivelse av kritisk infrastruktur. Tilgang på slik informasjon kan gjøre det enklere å gjennomføre uønskede hendinger.
- Det er nødvendig med risikovurdering på lokalt nivå.
- Gjenstår arbeid med å strukturere helsedata – må se til internasjonale standarder.
- Viktig tilnærming: må i større grad ha en gruppe profesjonelle helsepersonell som blir med fast- er for store kulturforskjeller. Mange mener at systemet ikke er laget for å ta hensyn til klinkere, og føler heller ikke at de har innflytelse
- Sterkere involvering av private aktører i nasjonale programmer, mer helhetlig fokus på helsesektoren
- Tilgjengeliggjøring av Normen, mer moderne, e-læring

- Noen av sårbarhetene har man tiltak for å håndtere – men på enkelte områder vil man se at sårbarheten er spesielt høy, at man ikke allerede har hatt det på agendaen og må begynne å jobbe med.
- Sjekk ut «Bad Health information can kill» - eksempler på caser hvor systemer er innført med god intensjon, men får store konsekvenser
- Det kliniske skjønnet kan forsvinne, og flere blir redde for å gjøre feil. Det er i dag rom for å gjøre en del skjønn, fordi man er individuelle personer. Dette vil kunne forsvinne. Må vurdere hvilke sårbarheter dette kan medføre. Det vil gjøre enkeltindividet mer sårbart, fordi det er en risiko for at man ikke blir utredet godt nok fordi man ikke passer inn i en standard sjekkliste

Teknologi for et bedre samfunn

www.sintef.no