HELSE VEST

16 MAR 2016

Det kongelige Justis- og beredskapsdepartementet
Postboks 8005 Dep
0030 OSLO

Deres ref:	Vår ref:	Saksbehandler:	Dato:
	2015/2439 - 15493/2016	Elisabeth Meland 51963819	15.03.2016

Høring - Digital sårbarhet - sikkert samfunn NOU 2015:13

Helse Vest RHF viser til ovennevnte.

Vi har sendt NOUen «Digital sårbarhet – sikkert samfunn» ut til Helse Vest IKT AS, Helse Vest Innkjøp HF, Sjukehusapoteka Vest HF og de fire sykehus helseforetakene og bedt om innspill.

Tre av sykehusforetakene og Helse Vest IKT AS har kommet med innspill. Disse ligger vedlagt. Helse Vest IKT AS har, som det følger av vedlegget, hatt høringssaken til behandling i sitt styret.

Helse Vest RHF har ikke noen innspill ut over det som fremkommer i det vi har mottatt fra våre foretak.

Vennlig hilsen

Ivar Eriksen
eierdirektør

Elisabeth Meland
seniorrådgiver

All elektronisk post til Helse Vest skal sendes til postmottak: post@helse-vest.no

Vedlegg

Postadresse:
Helse Vest RHF
Postboks 303 Forus
4066 Stavanger

Elektronisk adresse:
post@helse-vest.no
www.helse-vest.no

Besøksadresse:
Nådlandskroken 11
4066 Forus

Generell informasjon:
Sentralbord: 51 96 38 00
Org.nr: 983 658 725

HELSE VEST IKT AS

SAK 010-16

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest IKT AS
DATO:	01.03.2016
SAKSHANDSAMAR:	Erik M. Hansen
SAKA GJELD:	**«Digital sårbarhet – sikkert samfunn» – innspel til høyring**
ARKIVSAK:	
STYRESAK:	**010/16 D**
STYREMØTE:	**09.03.02016**

FORSLAG TIL VEDTAK

1. *Styret drøftar innspel til høyring av NOU 2015:13 «Digital sårbarhet – sikkert samfunn» og ber administrasjonen ta innspel vidare til Helse Vest RHF innan frist for svar på høyring.*

Oppsummering

NOU 2015:13, «Digital sårbarhet – sikkert samfunn» er til høring. Utredningen har drøftet hvordan «Beskytte enkeltmennesker og samfunn i en digitalisert verden». Administrasjonen mener denne utredningen er relevant for Helse Vest IKT, og for helseforetakene i Helse Vest RHF.

Fakta

Hele utredningen kan leses ved å følge lenken nedenfor;
https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/?ch=1&q=

Utvalget har gjort følgende vurderinger om helse- og omsorgssektoren og foreslått 4 tiltak, jfr. følgende utdrag fra side 199-200;

> **«17.7 Vurderinger og tiltak**
>
> Helsesektoren er en svært kompleks sektor, som består av mange organisatoriske enheter, komplekse styringsmodeller og verdikjeder som på overordnet nivå ikke lar seg beskrive på en enkel måte. Utvalget har ut fra en begrenset tidsramme bare sett på et lite antall problemstillinger og tjenester innenfor dette komplekse bildet.
>
> Utvalget mener at etableringen av Norsk Helsenett har vært et nyttig grep for å samle nasjonale løsninger og sikre enhetlige krav og styring. Gitt den kompleksiteten helsesektoren består av, hadde det vært utfordrende å opprettholde tilstrekkelig kompetanse til å ivareta sikkerheten i de tjenestene som etableres, dersom alle skulle opprettholdt regionale løsninger. HelseCSIRT er et annet initiativ som fungerer godt i sektoren, og som er en viktig ressurs for de regionale helseforetakene. Norge er det eneste landet som har etablert et statlig kompetansemiljø for sikkerhet i helsesektoren i form av HelseCSIRT. Utvalget mener det er viktig at disse ordningene forvaltes på en god måte også fremover.
>
> Utvalget foreslår følgende tiltak:
>
> ***17.7.1 Sterkere styring av IKT-sikkerhet fra Helse- og omsorgsdepartementet***
>
> Flere aktører etterlyser en sterkere styring fra HOD. Utvalget stiller spørsmål ved hvorfor styringsmuligheten som departementet har til å samkjøre mellom de regionale helseforetakene, ikke benyttes i større utstrekning.
>
> *Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og styrke felles behov og for å unngå divergerende løsninger i regionene.* I helsesektoren er det et sterkt behov for beslutningsevne hos HOD og for at det gis klare føringer for hvilke standarder som skal gjelde, hvilke IKT-områder RHF-ene må samkjøre, og så videre. Dette kan gjøres gjennom Direktoratet for e-helse, men det må legges til rette for at de får tilstrekkelige virkemidler og myndighet til å bistå HOD i utøvelsen av rollen. Dette inkluderer også tilgang på nødvendig IKT-faglig kompetanse der det er nødvendig. Videre må HOD sikre god samhandling med de ulike fagmiljøene.

Opprettelsen av Direktoratet for e-helse gir en mulighet for å utarbeide en samlet styringsstruktur som dekker både primær- og spesialisthelsetjenesten, med ansvar for å implementere og følge opp løsningene knyttet til e-helsesamarbeid. En slik løsning vil, spesielt i kommunesektoren, være til støtte for mange mindre aktører som kan ha vansker med å rekruttere og vedlikeholde tilstrekkelig egenkompetanse. Sikkerhetskrav i innkjøpsprosessene kan for eksempel i større grad samkjøres med større vekt på leverandøransvar.

Utvalget har gjennom sitt arbeid registrert at det er utgitt en stor mengde utredninger som omhandler IKT i helsesektoren, de siste årene. Flere av disse ser ut til å beskrive dagens utfordringer på en god måte, og det synes å være stor bevissthet i sektoren om hvilke forbedringstiltak som er nødvendige. Utvalget stiller spørsmål ved hvorfor ikke flere av tiltakene er fulgt opp, og om mengden utredninger i seg selv er til hinder for en effektiv iverksetting av tiltakene. Flere har uttrykt at evnen til å lære av tidligere utredninger ikke alltid er til stede, og at man i stor grad «finner opp hjulet på nytt». Utvalget har ikke vurdert hvorvidt dette skyldes manglende gjennomføringsevne, økonomi, eller styringsevne og -vilje. *Utvalget mener imidlertid at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det sikres gjennomføringskraft for disse. Som en del av dette foreslår utvalget at det nye Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT-sikkerhet i helsesektoren.*

Helsefaglig personell, som best kjenner sine egne arbeidsprosesser, må være med på å sette premissene for sikkerhetstiltak, slik at disse blir tilstrekkelig forankret i virksomheten. Sterk involvering av helsepersonell vil ikke stå i motsetning til sterkere nasjonal styring. Utvalget anerkjenner at kompleksiteten i sektoren, samt lang historikk med systemer som arves og lappes på, gjør at dette er en utfordring.

Utvalget observerer at Normen er ønsket velkommen av sektoren, og at den i all hovedsak fungerer bra. Normen gjør at helseforetakene tør å stille krav, og leverandørene blir mer oppmerksomme på temaet ved anskaffelser. Prosessen med å utvikle Normen har hatt en god effekt i seg selv og økt kompetansen i bransjen. Utvalget er orientert om at det er laget minimumskrav beregnet for små enheter. *På bakgrunn av innspill mener utvalget likevel det bør vurderes forenklinger i Normen for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.*

17.7.2 Mer forskning på IKT-sikkerhet innenfor ny helse- og velferdsteknologi

Den raske utviklingen av helse- og velferdsteknologi gir en rekke nye muligheter, men kan også føre til økt sårbarhet dersom det ikke tas nødvendige forholdsregler. Dette kan være både sårbarheter innad i helseforetakene og sårbarheter knyttet til bruk av helsetjenester utenfor helseforetakenes kontroll i privathjem. Behovet for kontroll av utviklingen understrekes av de tidligere beskrevne sårbarhetene knyttet til velferdsteknologi, som et økt antall angrepsflater, uklarheter omkring databehandleransvar og manglende digitaliseringsstrategi.

Etter utvalgets vurdering bør helse- og velferdsteknologi som i stor grad endrer samfunnet, utredes og følges opp av en offentlig debatt før implementering. Utvalget mener det er behov for en mer spisset forskningsinnsats for å se på sikkerhetsaspektene ved teknologien, samtidig som man ivaretar de mulighetene og utfordringene som ny helse- og velferdsteknologi vil gi. Forsøk som pågår med ny helse- og velferdsteknologi, bør videre samordnes nasjonalt for å sikre kompetanseoverføring. Det nye Direktoratet for e-helse bør sikre at disse initiativene samordnes.

17.7.3 Etablere løsninger for å imøtekomme utviklingen innenfor helse- og velferdsteknologien

Ved innføring av helse- og velferdsteknologi bør hovedregelen være at tjenesteeieren av slike løsninger tar et overordnet ansvar for sikkerheten i hele verdikjeden og ikke utelukkende baserer seg på at sikkerheten er ivaretatt av underliggende tjenester som for eksempel ekom-tilbydere. Også på dette området er leverandørkjeder og verdikjeder viktig. Se for øvrig omtale av verdikjeder i punkt 23.1 «Etablere nasjonalt rammeverk for å ivareta en helhetsvurdering av verdikjeder».

Utvalget støtter Norsk Helsenetts forslag om at helsenettet, i samarbeid med sektoren, bør vurdere om det er sentrale felleskomponenter (innen kommunikasjon mot Internett) som sektoren behøver for å fremme en trygg innføring av velferdsteknologiske løsninger.

17.7.4 Gjennomføre flere IKT-øvelser der kritiske systemer er ute av funksjon

Det er behov for å ha en beredskap for bortfall av IKT i helsesektoren, enten dette skyldes tilsiktede eller utilsiktede IKT-hendelser. Mindre grad av manuelle rutiner å falle tilbake på kan i fremtiden gi nye og økte sårbarheter. *Utvalget mener det bør gjennomføres flere IKT-øvelser der kritiske systemer er ute av funksjon.* Se også kapittel 20 «Styring og kriseledelse». I tillegg kreves det at sentrale helsetjenester kan opprettholdes uavhengig av IKT-støtte. Utvalget stiller spørsmål ved om man ved fremtidens heldigitaliserte helsesystemer (eksempelvis strukturerte pasientjournaler) vil ha mulighet og evne til å gå tilbake til manuelle systemer, og om vi med dette påfører oss en ny sårbarhet.»

Kommentarer

Administrasjonen mener utvalget peker på utfordringer der ansvaret ***både*** ligger til virksomhetene og utfordringer der ansvaret ligger på et nivå over virksomhetene. Deres vurderinger av utfordringer på nivå over virksomhetene kan også deles i det som gjelder ***samfunnet i stort***, og det som gjelder *helse- og omsorgssektoren* spesielt. I oppsummeringen for helse- og omsorgssektoren er det pekt på tiltak for på nivå ***over*** virksomhetene.

Administrasjonen gir i hovedsak tilslutning til de vurderingene og anbefalingene utvalget gjør når det gjelder digital sårbarhet i samfunnet i stort.

Administrasjonen har følgende innspill til de 4 tiltakene foreslått av Lysneutvalget;

1. Sterkere styring av IKT- sikkerhet fra HOD
   Anbefalingen må sees i sammenheng med det virksomhetene har ansvaret for. Med økende digitalisering av helse- og omsorgssektoren vil det, på et tidspunkt, også bli nødvendig å vurdere organiseringen av sektoren, evnt. organiseringen av leveransene av IKT-tjenestene til sektoren. Utredningen av «Én innbygger – én journal» har mye bakgrunnsdokumentasjon for denne problemstillingen.

2. Mer forskning på IKT-sikkerhet innenfor ny helse- og velferdsteknologi
   Forskning på IKT-sikkerhet bør fortrinnsvis gjøres på tvers av sektorer og ikke sektorvis.

3. Etablere løsninger for å imøtekomme utviklingen innenfor helse- og velferdsteknologien

Utviklingen av teknologibruken i helse- og omsorgssektoren har dessverre vært hindret av «ideologiske» synspunkter på IKT-sikkerhet og ubalanserte vurderinger av personvern versus pasientvern. Et eksempel er tidlig «skepsis» til bruk av GPS for demente pasienter, som nå er endret til en klar anbefaling om bruk av slik teknologi.

4. Gjennomføre flere IKT-øvelser der kritiske systemer er ute av funksjon
   Enig, jfr. også innspill nedenfor.

Administrasjonen mener i tillegg at følgende tiltak er viktige å fokusere på *internt* i virksomhetene i Helse Vest;

- Tilstrekkelig *redundans* i relevant infrastruktur
  - Strøm, kjøling, nettverk, servere, lagring, etc., etc.
- *Dobbel kontroll* med oppsett/endring av oppsett
- *Ansvar* i den enkelte virksomhet – *og* – *nasjonal* styring
- Beredskapsøvelser
  - Håndtere *svikt* i IKT *(hvordan unngå nedetid for IKT)*
  - Håndtere *konsekvenser av svikt* i IKT *(hvordan drive sykehus uten IKT)*
- Sikkerhetskultur – her er det mer å gjøre!

Konklusjon

Helse Vest IKT vil sende innspill til den felles regionale høringsuttalelsen som sendes gjennom Helse Vest RHF innen fristen 15.03.2016.

HELSE FONNA

MOTTATT
1 J MAR 2016

Helse Vest RHF
Postboks 303, Forus
4066 Stavanger

Att. Meland, Elisabeth

Deres ref:	Vår ref:	Saksbehandler:	Dato:
	2016/404 - 10000/2016	Anne Hilde Bjøntegård tlf 52732035	04.03.2016

Innspill til høring - "Digitale sårbarhet - sikkert samfunn (NOU 2015:13)

NOU 2005:13 er gjennomgått av IKT-sikkerhetsansvarlig i Helse Fonna HF, og har følgende innspill til kapittel 17 som omhandler helsesektoren.

Pkt. 17.3

Ved eventuell motstrid mellom Normen og de til enhver tid gjeldende lover eller forskrifter vil lov og forskrift gå foran Normen.

Dette er et svært viktig prinsipp og det bør tilstrebes i arbeidet med Normen at dette unngås.

Pkt. 17.4

Det finnes ingen rapporteringsplikt om IKT hendelser i helsesektoren. De regionale helseforetakene rapporterer inn til HelseCSIRT ved behov for støtte, men det er ingen fast sentral rapportering. Etter HelseCSIRT's mening er det behov for tydeligere krav til rapportering.

Det er mangel på rapportering og oversikt over hendelser. Det er ønskelig at IKT-leverandører har meldeplikt vedrørende uønskede hendelser.

Pkt. 17.5

Helsevesenet har så små marginer at liv kan gå tapt som følge av bortfall av IKT. Det finnes visse manuelle rutiner og muligheter for utskrifter på papir som gjør at sykehusene kan opprettholde driften noen timer, men ikke dager.

Postadresse:
Helse Fonna HF
Postboks 2170
5504 Haugesund

Elektronisk adresse:
post@helse-fonna.no
www.helse-fonna.no

Besøksadresse:
Karmsundsgt. 120

Generell informasjon:
Sentralbord: 0 52 53
Org.nr: 983 974 694

Vi har manuelle rutiner i de tilfellene det er bortfall av kritiske IKT-system. Eksempelvis dreier dette seg om utskrifter av journaldokumenter, men man ser at også disse rutinene har svakheter nå sykehusene ikke lenger baserer seg på papirjournaler.

Det jobbes med å forbedre disse rutinene.

Pkt. 17.5.2

Hensiktsmessig tilgangsstyring og sporing av brudd på taushetsplikt er utfordrende. Riksrevisjonen har påpekt følgende: «Ansatte i helseforetak har tilgang til helseopplysninger utover tjenestebehov, og kontrollen av tilganger til elektronisk pasientjournal er mangelfull.» En av årsakene som oppgis er at helseforetakene ikke i tilstrekkelig grad har implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger. Samtidig må det erkjennes at dette er et vanskelig område fordi det er svært mange ulike systemer med innbyrdes ulike oppsett.

- I all hovedsak har ansatte IKKE tilgang utover tjenestebehov. Legerollen er i sin natur slik at utvidet tilgang må være tilgjengelig da det for enkelte situasjoner ikke vil være tid til å etablere/endre tilgang. Alt blir logget og det må aktualiseres når utvidet tilgang benyttes.
- Nasjonalt prosjekt «Mønstergjenkjenning» vil ytterligere styrke vår kontroll.

Erfaring viser at IKT-utstyr i sektoren ofte er utenfor support og ikke lar seg oppdatere.

Systemer tilknyttet medisinsk utstyr er det som er typisk eksempel på programvareløsninger som ikke «henger med» i utviklingen, og støtter som oftest ikke nyere operativ system. Disse systemene er også sensitive mot oppdateringer av operativ systemer og antivirus. Ny-anskaffelser bringer gjerne med seg slike systemer som dette, som er veldig utsatt med tanke på sikkerhet. Leverandører av slike systemer må utvikle sine systemer opp mot dagens standard.

Pkt. 17.5.3

Det er store forskjeller mellom de regionale helseforetakene med hensyn til løsninger og valg av teknologi, og det er ingen felles prosess for samordning av krav til leverandører.

Dette stemmer ikke for Helse Vest. Det er lokale forskjeller, men disse utgjør et mindretall og det er stadig fokus på regionalisering. Samordning av krav til leverandører foregår, men har forbedringspotensial.

Pkt. 17.5.4

Det blir etterlyst en tettere involvering av helsepersonell, slik at de som har forståelse for arbeidsprosesser, strukturering av informasjon, og så videre, inkluderes.

Støttes, men det er en gjentakende utfordring når helsepersonell tas ut av ordinær «drift».

Etablere en overordnet nasjonal kompetansestrategi innen IKT-sikkerhet.

Informasjonssikkerhet har vært lite aktuelt i utdanningssammenheng frem til nyere tid. Det har ikke vært noe tilbud om studiesatsing innenfor informasjonssikkerhet, slik at kompetansenivået kan være veldig ulikt for IKT-personell/sikkerhetspersonell i virksomheter.

Pkt. 17.5.5

Mangelfull styring av tilgang er en problemstilling som sist ble påpekt av Riksrevisjonen i 2013, og som tidligere er påpekt i forbindelse med Datatilsynets kontroll av flere sykehus i 2008. Det er imidlertid viktig å bemerke at etablering av en forsvarlig tilgangsstyring i sykehusene er spesielt krevende, selv om det ikke kan frita for å etablere tilgangsstyring i samsvar med lovgiverens krav.

Det er et kontinuerlig fokus på tilgangskontroll. Det blir ved anskaffelser stilt krav til funksjonalitet som skal oppfylle lovens rammer.

Dagens systemer (IKT systemer, organisering og kompetanse) har åpenbare mangler når det gjelder å understøtte innbyggernes rett til personvern. Helsepersonell gis for omfattende tilgang i forhold til hva de reelt sett har tjenstlig behov for. Det er avdekket store mangler i logging av tilganger som gis, hvilket gjør det vanskelig å gjennomføre etterkontroller for å avdekke urettmessig tilegning av opplysninger.

- I all hovedsak har ansatte IKKE tilgang utover tjenestebehov. Legerollen er i sin natur slik at utvidet tilgang må være tilgjengelig da det for enkelte situasjoner ikke vil være tid til å etablere/endre tilgang. Alt blir logget og det må aktualiseres når utvidet tilgang benyttes.
- Nasjonalt prosjekt «Mønstergjenkjenning» vil ytterligere styrke vår kontroll.

Pkt. 17.7.1

Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og styrke felles behov og for å unngå divergerende løsninger i regionene. I helsesektoren er det et sterkt behov for beslutningsevne hos HOD og for at det gis klare føringer for hvilke standarder som skal gjelde, hvilke IKT områder RHF-ene må samkjøre, og så videre.

Helse Vest som region har høy grad av samkjøring.

Flere har uttrykt at evnen til å lære av tidligere utredninger ikke alltid er tilstede, og at man i stor grad «finner opp hjulet på nytt». Utvalget har ikke vurdert hvorvidt dette skyldes manglende gjennomføringsevne, økonomi, eller styringsevne og vilje. Utvalget mener imidlertid at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det sikres gjennomføringskraft for disse.

Som en del av dette foreslår utvalget at det nye Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT sikkerhet i helsesektoren.

Forslag til årlig statusrapport støttes da dette kan gi dokumentasjon for å understøtte om denne oppfatningen er korrekt.

På bakgrunn av innspill mener utvalget likevel det bør vurderes forenklinger i Normen for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.

Støttes.

Pkt. 17.7.4

Utvalget mener det bør gjennomføres flere IKT øvelse der kritiske systemer ute av funksjon.

Støttes.

Vennlig hilsen
Klinikk for medisinsk service og beredskap

Anne Hilde Bjøntegård

Anne Hilde Bjøntegård
Klinikkdirektør

Høringssvar «Digital sårbarhet – sikkerhet samfunn»

Dette er Helse Bergen HF sitt høringssvar på NOU 2015:13.

Helse Bergen HF har vurdert rapportens kapittel 17 (*Helse og omsorg*), 20 (*Styring og kriseledelse*), 21 (*Avdekke og håndtere digitale angrep*) og 23 (*Tverrsektorielle sårbarhetsreduserende tiltak*).

Oppsummering fra workshop om digitale sårbarheter er utelatt fra høringssvar.

Helse Bergen HF ønsker å takke for det arbeid som er utført og for vår anledning til direkte bidrag gjennom deltakelse i workshop for helsesektoren. Rapporten fremstår helhetlig og gir et svært godt bilde av situasjon og utfordringer som foreligger innen helsesektoren. Forslag til tiltak er konkrete og gir oss et godt utgangspunkt for videre arbeid.

Kommentar til kapittel 17:

17.1 Infrastruktur
Norsk Helsenett ble etablert i 2004 og fasiliterer blant annet et kommunikasjonsnett – helsenettet – som skal legge til rette for sikker utveksling av personopplysninger og kommunikasjon for øvrig.

- ➔ *Det er et krav at virksomheter som knyttet seg til Norsk Helsenett ikke har separat Internett forbindelse fra sitt nettverk.*

17.2 Roller og ansvar
Innen IKT er foretakene i stadig større utstrekning avhengige av RHF-enes IKT enheter, som beslutter innkjøp, infrastruktur og drift av IT systemene.

- ➔ *Dette krever aktiv dialog og rapportering mellom foretaket og IKT selskapet.*

17.3 Hjemmelsgrunnlag og tilsynsvirksomhet
Ved eventuell motstrid mellom Normen og de til enhver tid gjeldende lover eller forskrifter vil lov og forskrift gå foran Normen.

- ➔ *Dette er et svært viktig prinsipp og det bør tilstrebes i arbeidet med Normen at dette unngås.*

17.4 Beredskap og hendelseshåndtering
Ifølge Norsk Helsenett anses nedetid på IKT systemer ofte som mindre kritisk enn evnen til å yte helsehjelp i sektoren, noe som ofte gjenspeiles i beredskapsplanene. Ifølge Norsk Helsenett er dette et område som antas å få større oppmerksomhet i årene som kommer.

- ➔ *Det er mangel på rapportering og oversikt over hendelser. Det er ønskelig at IKT leverandører har meldeplikt vedrørende uønskete hendelser.*
- ➔ *Dette oppfattes i stor grad som omforent, men etter hvert som mer teknologi innføres øker avhengighet og dette kan endre på den etablerte oppfatningen?*
- ➔ *Det er viktig å skille mellom ulike deler av et sykehus og ulike deler av systemporteføljen.*

Det finnes ingen rapporteringsplikt om IKT hendelser i helsesektoren. De regionale helseforetakene rapporterer inn til HelseCSIRT ved behov for støtte, men det er ingen fast sentral rapportering. Etter HelseCSIRT's mening er det behov for tydeligere krav til rapportering.

- ➔ *Det er en opplevd underrapportering på dette området. Dokumentasjon og åpenhet er sentralt for å øke prioritering av sikkerhet og fokus/kjennskap til utfordringene.*
- ➔ *Unntak ved alvorlig skade på pasient: hendelser rapporteres til Kunnskapssenteret ved vårt avvikssystem.*

17.5 Digitale sårbarheter i helsesektoren
Helsevesenet har så små marginer at liv kan gå tapt som følge av bortfall av IKT. Det finnes visse manuelle rutiner og muligheter for utskrifter på papir som gjør at sykehusene kan opprettholde driften noen timer, men ikke dager.

- ➔ *Oppfatningen deles, men her kan det være sentralt med differensiering i forhold til tjenester.*
- ➔ *Manuelle rutiner er en sentral del av vår beredskap.*
- ➔ *Vi har daglig backup av hovedjournal som rutes til flere enheter som kan gi tilgang og utskrift*
    - *Er under revisjon for ytterligere forbedring og styrking*

17.5.2 Infrastruktur og tjenester
Erfaring viser at IKT utstyr i sektoren ofte er utenfor support og ikke lar seg oppdatere.

- ➔ *Systemer tilknyttet medisinsk utstyr er det som er typisk eksempel på programvareløsninger som ikke «henger med» i utviklingen, og støtter som oftest ikke nyere operativsystem. Disse systemene er også sensitive mot oppdatering av operativsystem og antivirus.*

Hensiktsmessig tilgangsstyring og sporing av brudd på taushetsplikt er utfordrende. Riksrevisjonen har påpekt følgende: «Ansatte i helseforetak har tilgang til helseopplysninger utover tjenestebehov, og kontrollen av tilganger til elektronisk pasientjournal er mangelfull.» En av årsakene som oppgis er at helseforetakene ikke i tilstrekkelig grad har implementert gjeldende regelverk om informasjonssikkerhet og behandling av helseopplysninger. Samtidig må det erkjennes at dette er et vanskelig område fordi det er svært mange ulike systemer med innbyrdes ulike oppsett.

- ➔ *I all hovedsak har ansatte IKKE tilgang utover tjenestebehov. Legerollen er i sin natur slik at utvidet tilgang må være tilgjengelig da det for enkelte situasjoner ikke vil være tid til å etablere/endre tilgang. Alt blir logget og det må aktualiseres (angi årsak) når utvidet tilgang benyttes.*
- ➔ *Kontroll kan forbedres, men vi har rutiner for avdelingsvis og sentral overordnet gjennomgang.*
- ➔ *Nasjonalt prosjekt «Mønstergjenkjenning» vil ytterligere styrke vår kontroll.*
- ➔ *Lovverket er implementert for de største journalsystem, men for mer fagspesifikke system er det registrert avvik. Ved alle nyanskaffelser blir det stilt særskilte krav som skal sikre etterlevelse av lov og gjeldende regelverk.*
- ➔ *Medisinsk utstyr er et område med egne utfordringer, men det pågår aktivt arbeid for etterlevelse.*

17.5.3 Styring og samhandling

Det er store forskjeller mellom de regionale helseforetakene med hensyn til løsninger og valg av teknologi, og det er ingen felles prosess for samordning av krav til leverandører.

- ➔ *Dette stemmer ikke for Helse Vest. Det er lokale forskjeller, men disse utgjør et mindretall og det er stadig fokus på regionalisering. Samordning av krav til leverandører foregår, men har forbedringspotensial.*

17.5.4 Kompetanseutfordringer når det gjelder IKT sikkerhet

Få akademiske miljøer i Norge forsker på IKT i helsesektoren (helseinformatikk). Samtidig er det i liten grad forsking på konsekvensene av de IKT tiltakene som innføres, og store IKT prosjekter blir i liten grad evaluert.

- ➔ *Informasjonssikkerhet har vært lite aktuelt i utdanningssammenheng frem til nyere tid. Det har ikke vært noe tilbud om studiesatsing innenfor informasjonssikkerhet, slik at kompetansenivået kan være veldig ulikt for IKT personell/sikkerhetspersonell i virksomheter.*
- ➔ *Styringsdokument 2016 tar opp dette og adresser bidrag til utvikling av Nasjonalt senter for e-helseforskning*

Det blir etterlyst en tettere involvering av helsepersonell, slik at de som har forståelse for arbeidsprosesser, strukturering av informasjon, og så videre, inkluderes.

- ➔ *Støttes, men det er en gjentakende utfordring som det fortsatt må arbeides med når helsepersonell tas ut av «drift».*

17.5.5 Særskilte personvernutfordringer

Mangelfull styring av tilgang er en problemstilling som sist ble påpekt av Riksrevisjonen i 2013, og som tidligere er påpekt i forbindelse med Datatilsynets kontroll av flere sykehus i 2008. Det er imidlertid viktig å bemerke at etablering av en forsvarlig tilgangsstyring i sykehusene er spesielt krevende, selv om det ikke kan frita for å etablere tilgangsstyring i samsvar med lovgiverens krav.

- ➔ *Det er et kontinuerlig fokus på tilgangskontroll. Det blir ved anskaffelser stilt krav til funksjonalitet som skal oppfylle lovens rammer.*

Høsten 2013 gjennomførte Datatilsynet 15 brevkontroller av fastleger, spesialister og helseforetak som utleverer helseopplysninger til de sentrale helseregistrene. En forutsetning for pasientenes mulighet til å ivareta sitt personvern er at de blir informert om at helseopplysningene om dem

videreformidles slik regelverket krever. Kontrollene viste at pasienten generelt ikke blir informert om at helseopplysninger blir utlevert til sentrale helseregistre.

- ➔ *Tilsyn har bidratt til at rutiner har blitt tydeliggjort og det har blitt et økt fokus på informasjon.*

I sum er det høyst betenkelig at helsetjenestene og næringsaktører ikke alltid informerer pasienter og brukere om hvordan opplysningene deres videreformidles og behandles for nye formål. Det kan være fare for at økende høsting av helseopplysninger kan undergrave den nødvendige tilliten til helsetjenestene og føre til at deler av befolkningene unngår å oppsøke det alminnelige helsehjelpstilbudet.

- ➔ *Sekundær behandling av person- og helseopplysninger baseres i stor grad på samtykke.*
- ➔ *Primærbehandling er i stor grad basert på implisitt samtykke og det er et uttalt mål å øke informasjon og tilgang til informasjon for våre pasienter. Innkallingsbrev er endret og vi deltar i regionalt prosjekt for helsetjenester på nett ved bruk av helsenorge.no.*
- ➔ *Vi ser fortsatt muligheter for forbedring og tilnærmer oss dette i samhandling med pasientene.*
- ➔ *PVO er sentral i oversikt over behandling av person- og helseopplysninger*

Dagens systemer (IKT systemer, organisering og kompetanse) har åpenbare mangler når det gjelder å understøtte innbyggernes rett til personvern. Helsepersonell gis for omfattende tilgang i forhold til hva de reelt sett har tjenstlig behov for. Det er avdekket store mangler i logging av tilganger som gis, hvilket gjør det vanskelig å gjennomføre etterkontroller for å avdekke urettmessig tilegning av opplysninger.

- ➔ ***[REF. 17.5.2 Infrastruktur og tjenester]***
- ➔ *I all hovedsak har ansatte IKKE tilgang utover tjenestebehov. Legerollen er i sin natur slik at utvidet tilgang må være tilgjengelig da det for enkelte situasjoner ikke vil være tid til å etablere/endre tilgang. Alt blir logget og det må aktualiseres (angi årsak) når utvidet tilgang benyttes.*
- ➔ *Kontroll kan forbedres, men vi har rutiner for avdelingsvis og sentral overordnet gjennomgang.*
- ➔ *Nasjonalt prosjekt «Mønstergjenkjenning» vil ytterligere styrke vår kontroll.*
- ➔ *Lovverket er implementert for de største journalsystem, men for mer fagspesifikke system er det registrert avvik. Ved alle nyanskaffelser blir det stilt særskilte krav som skal sikre etterlevelse av lov og gjeldende regelverk.*
- ➔ *Medisinsk utstyr er et område med egne utfordringer, men det pågår aktivt arbeid for etterlevelse.*

17.7.1 Sterkere styring av IKT sikkerhet fra Helse- og omsorgsdepartementet

Utvalget mener det er behov for sterkere nasjonal styring for å identifisere og styrke felles behov og for å unngå divergerende løsninger i regionene. I helsesektoren er det et sterkt behov for beslutningsevne hos HOD og for at det gis klare føringer for hvilke standarder som skal gjelde, hvilke IKT områder RHF-ene må samkjøre, og så videre.

- ➔ *Helse Vest som region har høy grad av samkjøring.*
- ➔ *Det er i ulike rapporter gitt uttrykk for helseforetakene som databehandlingsansvarlig i større grad må være/bli sitt ansvar bevisst og i større grad utøve dette.*

Flere har uttrykt at evnen til å lære av tidligere utredninger ikke alltid er tilstede, og at man i stor grad «finner opp hjulet på nytt». Utvalget har ikke vurdert hvorvidt dette skyldes manglende gjennomføringsevne, økonomi, eller styringsevne og vilje. Utvalget mener imidlertid at det er viktig med en tydeligere prioritering av forebyggende tiltak for å redusere de identifiserte sårbarhetene, og at det sikres gjennomføringskraft for disse. Som en del av dette foreslår utvalget at det nye

Direktoratet for e-helse utarbeider en årlig statusrapport om tilstanden for IKT sikkerhet i helsesektoren.

- ➔ *Forslag til årlig statusrapport støttes da dette kan gi dokumentasjon for å understøtte om denne oppfatningen er korrekt.*

På bakgrunn av innspill mener utvalget likevel det bør vurderes forenklinger i Normen for de minste helseforetakene i den grad det er mulig uten at det bidrar til å øke sårbarheten.

- ➔ *Forenklinger imøtekommes også av større foretak da ressurser som arbeider med informasjonssikkerhet gjerne er få og har stort ansvarsområde.*

17.7.4 Gjennomføre flere IKT øvelser der kritiske systemer er ute av funksjon

Utvalget mener det bør gjennomføres flere IKT øvelse der kritiske systemer ute av funksjon.

- ➔ *Det gjennomføres IKT øvelser i Helse Vest, men vi er positive til økt frekvens og rekkevidde/omfang ved øvelsene.*

Del IV – Kapittel 23

23.5 Redegjørelse for IKT sikkerhet bør inngå i årsmeldinger

Ansvaret for IKT sikkerhet ligger hos den øverste ledelsen både i privat og i offentlig virksomhet. Utvalgets undersøkelser tyder på at arbeidet med IKT sikkerhet ikke alltid får den prioriteten det bør ha. For å sikre at arbeidet med IKT sikkerhet prioriteres høyere, bør det innføres et krav til at ivaretakelse av IKT sikkerhet beskrives i virksomhetenes årsmelding.

- ➔ *Vi ser positivt på en ytterligere forankring og et økt fokus på hvor viktig det er med fokus på informasjonssikkerhet. Ved økt tilgang og eksponering på nett er det sentralt at vi øker fokus og med dette bidrar til ytterligere tillit hos våre pasienter og ansatte.*
- ➔ *Presisering av databehandlingsansvarlig sin rolle er sentral.*

23.6.4 IKT sikkerhet som hinder for verdiskaping

IKT sikkerhet som hinder for verdiskapning?

- ➔ *IKT sikkerhet og pasientsikkerhet blir ofte trukket frem som motstridende elementer, men det er her helsepersonell og deres skjønnsmessige vurderinger skal ligge til grunn for førende beslutninger.*

HELSE STAVANGER
Stavanger universitetssjukehus
Fag- og foretaksutvikling

Helse Vest RHF
Postboks 303, Forus
4066 Stavanger

Deres ref:	Vår ref:	Saksbehandler:	Dato:
	2016/1218 - 26087/2016	Brad Folsom	10.03.2016

Svarbrev til høringen om digital sårbarhet - sikkert samfunn (NOU 2015:13)

Viser til invitasjon fra Elisabeth Meland om å sende inn innspill til ovennevnt sak.

Helse Stavanger er enig i det meste i NOU 2015:13, og vil uttrykke støtte på utvalgets forslag om sterkere nasjonal styring av IKT i helsesektoren.

Nasjonale helseløsninger vil gjøre det lettere å samarbeide på tvers av institusjonene i alle nivåer i helsesektoren. I tillegg vil nasjonal forankring hjelpe den enkelte institusjon med å unngå forvirring rundt tolkning av lovkrav og beste praksis ved implementering av IKT løsninger.

Vennlig hilsen
Seksjon for informasjonssystemer

Brad Folsom
IT Sikkerhetsleder
Helse Stavanger HF

Postadresse:
Helse Stavanger HF
Postboks 8100
4068 Stavanger

Elektronisk adresse:
post@sus.no
www.helse-stavanger.no

Besøksadresse:

Generell informasjon:
Sentralbord: 0 51 51
Org.nr: 983 974 678