STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest RHF
DATO:	21.02.2018
SAKSHANDSAMAR:	Erik M. Hansen
SAKA GJELD:	**Informasjonstryggleik i Helse Vest**
ARKIVSAK:	2018/202
STYRESAK:	**027/17**
STYREMØTE:	**07.03. 2018**

FORSLAG TIL VEDTAK
Styret tek saka til etterretning.

Oppsummering

Styret i Helse Vest IKT drøftet ved behandlingen av sak 079/17 i styremøtet 21.12.2017 behovet for en orientering til styret i Helse Vest RHF og styrene i helseforetakene om arbeidet med informasjonssikkerhet i lys av ulike saker knyttet til Helse Sør-Øst, mellom annet utfordringer knyttet til gjennomføring av tjenesteutsetting («outsourcing») i mai 2017. IKT-hendelsen i januar 2018 (datainnbrudd fra ekstern trusselaktør som etterforskes av E-tjensten og PST) har ytterligere aktualisert dette tema.

Saken er utarbeidet med utgangspunkt i Helse Vest IKTs tilnærming til arbeidet med IKT-sikkerhet, men det er i saken og gitt innspill til hvordan foretaksgruppen Helse Vest RHF må arbeide med disse viktige tema.

Fakta

Arbeidet med IKT-sikkerhet i foretaksgruppen Helse Vest tar utgangspunkt i det regionale «Styringssystemet for informasjonssikkerhet». Dette ble første gang etablert i 2004, det ble sist revidert i 2017, og det pågår en revisjon for å tilpasse styringssystemet til de nye kravene som følger av at *EUs forordning for personvern*, «The General Data Protection Regulation» (GDPR), blir norsk lov i mai 2018.

I foretaksgruppen Helse Vest RHF, med et regionalt helseforetak, egne helseforetak, et felles aksjeselskap innenfor IKT-området og samarbeid innenfor «sørge-for-ansvaret» med private, ideelle foretak, er fordelingen av *ansvar for* og *oppfølging av* oppgaver særlig viktig. Dette er søkt belyst i saken.

Risikostyring er et sentralt virkemiddel for å unngå uønskede hendelser relatert til informasjonssikkerhet. Det gjelder for å unngå tap av tilgjengelighet til relevant informasjon, konsekvenser for integriteten for informasjonen eller trusler knyttet til konfidensialitet.

Risikostyringen må baseres på systematiske vurderinger av *risiko- og sårbarhet*. Funn må følges opp av tiltak. Akseptabelt risikonivå må følges, samtidig som det er svært viktig å akseptere endringer som i sum fører til at situasjonen blir *bedre enn før*, selv om den ikke blir *«perfekt».*

Styrene i Helse Vest bør i første kvartal hvert år orienteres om hovedtrekkene i ledelsens årlige gjennomgang av informasjonssikkerhet, jfr. det regionale styringssystemet for informasjonssikkerhet. Styrene bør i annet halvår årlig gis en orientering om den samlede utviklingen innenfor IKT-området, med fokus på status og planer for viktige initiativ og sammenhengen mellom disse og den overordnede foretaksstrategien for Helse Vest.

Kommentarer
Helse Vest IKT mener det er viktig å arbeidet med risikostyring fra flere perspektiver. Dette gjelder helt fra det overordnede arbeidet med *Internkontroll* og *«Retningslinjer for risikostyring i Helse Vest»*, jfr. styresak 033/12 «Gjennomføring av risikostyring i føretaksgruppa i Helse Vest, revidering av retningslinjer».

Utgangspunktet for denne saken om informasjonssikkerhet er det regionale «*Styringssystemet for informasjonssikkerhet*».
1. Om det regionale «Styringssystemet for informasjonssikkerhet»
Lovgivningen krever at helse- og personopplysninger skal beskyttes tilfredsstillende mot *uberettiget* innsyn (*konfidensialitet*) og endringer (*integritet*). Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for disse (*tilgjengelighet*).

Informasjonssikkerhet dreier seg om å håndtere risikoen for at helse- og personopplysninger og blir ivaretatt på en tilfredsstillende måte.

Styringssystemet er en dokumentasjon på og en oversikt over konkrete og praktiske aktiviteter som databehandlingsansvarlige skal gjennomføre for å styre virksomheten når det gjelder informasjonssikkerhet ved behandling av helse- og personopplysninger.

Det danner grunnlag for etablering av nødvendige sikkerhetstiltak i den enkelte virksomhet ift relevant risiko og trusler som kan påvirke behandling av helse- og personopplysninger, slik at bruk og behandling av helse- og personopplysninger skjer iht krav i gjeldende lovgivning.

Styringssystemet er utarbeidet som grunnlag for lovlig, forsvarlig og nødvendig samhandling mellom virksomhetene. Systemet skal styre virksomhetenes sikkerhetsarbeid, og sikre at helse- og personopplysninger behandles i samsvar med lovpålagte krav. Styringssystemet er basert på Norm for informasjonssikkerhet i helse- og omsorgstjenesten og revideres i tråd med denne.

Styringssystemet inneholder en styrende del, en gjennomførende del og en kontrollerende del. I tillegg er det utarbeidet relevante dokumentmaler.

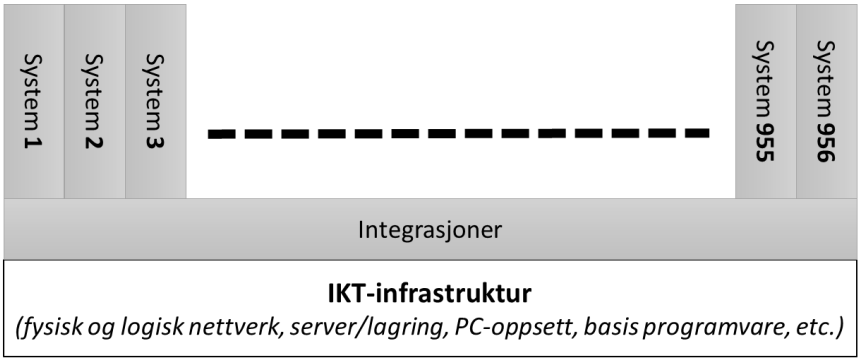
Ett element i den kontrollerende delen er kravet om ledelsens årlige gjennomgang som minimum skal inneholde følgende;

- *Referat fra forrige ledelsesgjennomgang*
- *Rapporten som oppsummerer resultat av avviksbehandling, sikkerhetsrevisjoner og risikovurderinger*
- *Vurdere om IKT-sikkerhetsmål og/eller den -strategi som gjelder for virksomheten fungerer etter hensikten*

- *Nivå for akseptabel risiko*
- *Ansvarsforhold og organisering mht. sikkerhet*
- *Formål med behandling av helse- og personopplysninger og oversikt over helse- og personopplysninger som behandles i virksomheten.*
- *Konfigurasjonskart over informasjonssystemene*
- *Kontroll og oppfølging av inngåtte avtaler*
- *Vurdering av ev. endringer utenfor virksomhetens kontroll – herunder endret risiko for sikkerhetsbrudd eller endringer i lovpålagte krav*

Det er viktig at helseforetakene implementerer og etterlever det *«Regionale styringssystemet for informasjonssikkerhet»*, og gjennom Ledelsens årlige gjennomgang fører nødvendig kontroll.

2. Om ansvar for og oppfølging av vurderinger av risiko og sårbarhet
Svært forenklet kan den totale IKT strukturen i Helse Vest deles i to; *IKT-infrastruktur* og samlingen av *system/applikasjoner* med tilhørende *integrasjoner* som benyttes av brukerne.



Med ***IKT-infrastruktur*** menes all maskinvare (nettverks-elektronikk, servere, lagringssystemer, PCer, nettbrett, mobiltelefoner) og basis programvare (nettverksoperativsystem, operativsystemer for servere, operativsystem for PCer, nettbrett, mobiltelefoner, epostsystem, brukerkatalog (AD), antivirusløsning, etc.) som benyttes for å operere maskinvare.

Omfanget av infrastrukturen kan illustreres med følgende tall; 160 eksterne nettverkssamband, 1.400 nettverkskomponenter, 34.000 aktive nettverksporter, 6.000 aksesspunkt for trådløst nett, 22.000 PCer, 2.150 servere (av disse er 1.800 «virtualiserte», dvs. mange server kjører sammen på en fysisk server), 6,5 PB med lagringskapasitet.

Med ***system/applikasjon*** og tilhørende ***integrasjoner*** menes her Elektronisk pasientjournal (DIPS), Kurve og legemiddelløsning (Meona), Digitalt media arkiv (Sectra), HR-system (Agresso), Økonomi og logistikksystem (SAP), etc.

Omfanget av system/applikasjoner i Helse Vest er **956** ulike systemer/applikasjoner. Disse fordeler seg på **240** store systemer, **127** mellomstore systemer og **589** små systemer.

Helse Vest IKT er av det syn at det må være en avklart *fordeling* av *ansvar* for IKT-infrastruktur og for system/applikasjoner. Dette er en *forutsetning* for å kunne følge opp arbeidet med informasjonssikkerhet på en tilfredsstillende måte.

Ved revisjon av Forretningsplanen for Helse Vest IKT er det lagt stor vekt på klargjøring av *ansvar og styringsmyndighet* innenfor IKT-området i Helse Vest. Basert på dette har Helse Vest IKT en to-delt funksjon;

1) *«Helse Vest IKT har ansvar og styringsmyndighet innenfor operative IKT-tjenester.*
2) *Helse Vest IKT gir bidrag til endring og forenkling hos helseforetakene gjennom strategiske og taktiske IKT-tjenester. Dette omfatter deltagelse i og leveranser til program/prosjekt, samt forvaltning av regionale prosesser, system og arkitektur.*

Ansvar og styringsmyndighet for infrastruktur innenfor IKT er i Helse Vest er lagt til Helse Vest IKT. Helse Vest IKT skal ha en systematisk oppfølging av risiko- og sårbarhet for IKT-infrastrukturen.

Følgende regionale styringsstrukturer er etablert for å håndtere *ansvar og styringsmyndighet* knyttet til de strategiske og taktiske tjenestene*;*

- Styringsstruktur for *forvaltning* av regionale system/applikasjoner.
  Omfatter regionale *føringer* for bruk og videreutvikling av felles IKT-løsninger som er tatt i bruk i Helse Vest. Med løsninger menes arbeidsprosesser og prosedyrer for bruk av løsningen, oppsett av programvare (konfigurasjon), relevante integrasjoner, etc. Forvaltningen av de regionale løsningene er organisert med styringsstrukturer innenfor noen hovedområder. Det mest omfattende området er Felles EPJ (felles kliniske løsninger). Styringsstrukturen styres av et Partnermøtet (adm. dir. for hver databehandlingsansvarlig (helseforetakene og de private, ideelle), arbeidet ledes av et strategisk styringsorgan (ledet av fagdirektør i Helse Vest RHF) og følges opp av et operativt styringsorgan (ledet av avd. leder Regionalt EPJ-fagsenter i Helse Vest IKT). Det er under etablering tilsvarende styringsstruktur for forvaltning av ny løsning for økonomi og logistikk (LIBRA).

- *Porteføljestyring*, her inkludert styring av *program og prosjekt.*
  Porteføljen omfatter de prosjektene og/eller programmene som er nødvendige for å oppnå de strategisk målene for Helse Vest. Porteføljestyring fokuserer på å gjøre de rette tingene, prosjekter fokuserer på å gjøre tingene rett og program er begge deler. Porteføljestyringen i Helse Vest styres av Porteføljestyret ledet av adm. dir. i Helse Vest RHF og sammensatt av adm. dir. i foretakene og Helse Vest IKT, og ledergruppen i

Helse Vest RHF. Porteføljestyringen understøttes av et virtuelt Regionalt porteføljekontor (RPK).

- Regional styringsstruktur for *virksomhetsarkitektur*
  Virksomhetsarkitektur er en strukturert beskrivelse av virksomhetens organisering, styring, tjenester, arbeidsprosesser, informasjonsgrunnlag, IKT-systemer og teknologi. Arkitekturstyringen i Helse Vest styres ved at Direktørmøtet er «arkitektureier», mens Teknologirådet (ledet av eierdirektør i Helse Vest RHF og sammensatt av nivå 1 og 2 ledere fra Helse Vest RHF, helseforetakene og Helse Vest IKT) er Arkitekturstyre. Arkitekturstyret understøttes av et virtuelt Regionalt arkitekturkontor (RAK).

- Regionalt styringssystem for *informasjonssikkerhet».*
  Se egen beskrivelse over.

For Helse Vest IKT er det viktig å legge til grunn at innenfor disse områdene er Helse Vest IKT *«arbeidsgiver, men ikke oppdragsgiver».* Her arbeider tilsette i Helse Vest IKT i tråd med gjeldende *regionale styringsstrukturer*.

Risiko og sårbarhet knyttet til «IKT-infrastruktur»
Helse Vest IKT driver kontinuerlig arbeid med risiko- og sårbarhetsvurderinger av IKT-infrastrukturen innenfor selskapet ansvarsområde. Første sak om dette tema var risiko- og sårbarhetsvurderingen som ble presentert for styret i Helse Vest IKT i 2007. Administrasjonen har deretter rapportert til styret endringer i risiko- og sårbarhet, i perioder i hvert styremøte og minst ved en årlig gjennomgang. Sist gjennomgang var i desember 2017. De årlige ROS-vurderingene er oversendt i brevs form (u. off) til helseforetakene.

I tillegg gjennomfører HelseCERT hos Norsk Helsenett SF årlige inntrengningstester i Helse Vest IKT sin infrastruktur. Resultatene deles med helseforetakene, med unntak for tekniske detaljer som kan redusere sikkerheten dersom informasjonen kommer på avveie.

Risiko og sårbarhet knyttet til løsninger/systemer/applikasjoner
Det gjennomføres egne vurderinger av risiko og sårbarhet for system/applikasjoner. Dette gjennomføres primært ved endringer av systemene, dvs. ved første gangs innføring eller ved større oppgraderinger av systemer som allerede er i produksjon. ROS-vurderinger av løsninger som settes i produksjon sendes til programstyrer/styringsgrupper, endringer i løsninger som er i produksjon sendes til systemeier/systemeiergrupper. Risikovurderinger av løsninger som brukes av 2 eller flere foretak behandles alltid som «regionale» i Helse Vest, det vil si at regionalt sikkerhetsutvalg innkalles til arbeidsmøtene og foretar en gjennomgang og tilbakemelding på den endelige rapporten når den foreligger.

Endringsrisiko
Innenfor IKT-området er det erfaringsmessig risiko knyttet til at det gjennomføres endringer i infrastrukturen (nye komponenter eller endringer av oppsett), oppgraderinger av programvare eller endringer i oppsett for løsninger/systemer. Helse Vest IKT har implementert en *«Endringsprosess»* basert på det internasjonale rammeverket ITIL. ITIL er en samling av «best practise» prosesser for IKT driftsorganisasjoner.

En endring plasseres i en av følgende endringskategorier; *Lavrisiko, Ordinær, Omfattende, Forhåndsgodkjent, og Nødendring.* Det er gjøres risiko- og sårbarhetsvurderinger av endringer i kategoriene *Ordinær* og *Omfattende*. Ved særlig krevende omfattende endringer (f. eks. oppgraderinger av DIPS) setter Helse Vest IKT Grønn beredskap for å sikre tilgang til kompetanse og kapasitet for å følge opp uforutsette konsekvenser. Ved slike endringer skal representanter for helseforetakene godkjenne kritiske steg i gjennomføring av endringen i egne «*go/no-go*»-møter.

3. Om Tjenesteavtalen (SLA) og databehandleravtaler
Det inngår en egen Databehandleravtale mellom hvert helseforetak og Helse Vest IKT i Tjenesteavtalen (SLA). Det er gitt tilslutning til at Helse Vest IKT kan inngå Databehandleravtaler på vegne av helseforetakene (og omtalt som underdatabehandleravtaler), jfr. egen sak i Direktørmøtet. Mal for slike avtaler, samt prosedyre for utfylling og godkjenning av avtalene er utarbeidet av regionalt sikkerhetsutvalg og inngår i regionalt styringssystem for informasjonssikkerhet.

Helse Vest IKT er i ferd med å etablere slike avtaler for Leverandører som frem til nå har vært håndtert i henhold til tidligere praksis, dvs. der hvert helseforetak var ansvarlig. Helse Vest IKT prioriterer dette arbeidet etter «størrelsen» på løsningene som er i bruk.

4. Om tjenesteutsetting
Helse Sør-Øst RHF valgte i september 2016 å inngå kontrakt med Hewlett Packard Enterprise (HPE), nå DXC Technology om tjenesteutsetting av modernisering av IKT-infrastrukturen. Styret i Helse Vest IKT har gjort en egen vurdering av tjenesteutsetting, og konkludert i juni 2016 med ikke å gjøre tilsvarende i lys av at egen regi har tilfredsstillende kvalitet og at Helse Vest IKT er kosteffektive sammenlignet med tilsvarende tjenesteleveranser. Vurderingen av kosteffektivitet ble gjort ved en «benchmarking» utført av Gartner Norge. Kostnadssammenligninger utført av Direktoratet for e-helse av de 4 RHFene sine IKT-organisasjoner i 2014 og 2017 har bekreftet disse tallene.

I mai 2017 ble det reist flere spørsmål i media og Storting knyttet til tilgangsstyring og informasjonssikkerhet knytte til tjenesteutsettingen i Helse Sør-Øst RHF. Departementet ba da Direktoratet for e-helse om å vurdere hvilke tjenester som kan tjenesteutsettes. Rapporten ble levert i desember 2017. Direktoratet for e-helse mener det ikke er grunnlag for å konkludere med at noen typer tjenester aldri kan overlates til eksterne leverandører. Det

trenger altså ikke å være et motsetningsforhold mellom informasjonssikkerhet og tjenesteutsetting. Det må imidlertid alltid foreligge nødvendige risikovurderinger og databehandleravtaler for å ivareta hensynet til informasjonssikkerheten. I gjeldende rett er det ikke forbud mot at norske virksomheter benytter nasjonale eller utenlandske IKT-leverandører fra EU/EØS-området. Ved bruk av IKT-leverandører utenfor EU/EØS-området er det særskilte krav som må oppfylles.

5. Om tilgang for eksterne leverandører
Helse Vest hadde i desember 2017 avtaler om tilgang med 129 private, eksterne leverandører for å bidra til forvaltning, overvåkning og feilretting av hundrevis av ulike IKT-løsninger og medisinsk-tekniske systemer. Av de 129 leverandørene til Helse Vest har 51 av leverandørene tilgang til løsninger som inneholder sensitive personopplysninger. Dette innebærer imidlertid ikke at alle disse har tilgang til pasientjournaler. Det er ofte avgrensede, fragmenterte dataelementer som det er krevende å knytte til identifiserte pasienter og undersøkelser. Potensielt kan disse 129 private leverandørene ha til sammen opptil 467 autentiserte medarbeidere som ved behov kan gis tilgang til Helse Vest sine systemer.

Majoriteten av leverandørene i Helse Vest gis tidsbegrenset tilgang via kryptert VPN for å utføre avtalte oppgaver. VPN er et virtuelt privat nettverk, en datateknikk som anvendes for å skape sikre «punkt-til-punkt»-forbindelser gjennom internett. Noen få sentrale leverandører kan gis kontinuerlig kryptert VPN-tilgang for overvåkning og oppfølging av sine løsninger over tid eller for avtalte prosjektperioder. Helse Vest IKT har under etablering løsninger for kontinuerlig loggføring av krypterte VPN-tilganger, både tidsbegrensede og kontinuerlige.

Helse Vest IKT gir informasjon til helseforetakene om leverandører som kan gis VPN tilgang. Denne informasjonen håndteres i dag gjennom et verktøy utviklet av Helse Vest IKT for slik administrasjon av leverandører og brukere.

6. Noen refleksjoner relatert til sakene i Helse Sør-øst RHF
Som en følge av saken rundt tilgangsstyring i Helse Sør-øst i mai 2017, har Datatilsynet varslet ni helseforetak i Helse Sør-Øst om overtredelsesgebyr på 800 000 kr. Helseforetakene får gebyr for å ikke ha oppfylt pliktene til sikkerhetsledelse, risikovurderinger og tilgangsstyring i forbindelse med tjenesteutsetting av IKT-drift til utlandet.

Datatilsynet skriver blant annet:

Om eierskap til og kontroll med endringene knyttet til informasjonssystemene
Datatilsynet skriver i brev til helseforetakene i Helse Sør-Øst; «*De behandlingsansvarlige helseforetakene har ikke hatt tilstrekkelig eierskap til, eller kontroll med de planlagte endringene knyttet til informasjonssystemet.»*

Det er her viktig at helseforetakene implementerer og etterlever det «Regionale styringssystemet for informasjonssikkerhet», og gjennom Ledelsens årlige gjennomgang fører nødvendig kontroll. Tilsvarende gjelder også for Styringsstrukturen for Felles EPJ der foretakene ansvarliggjøres gjennom styringsstrukturen fra operativt styringsorgan, via strategisk styringsorgan og til partnermøtet (repr. ved adm. dir. for de samarbeidende virksomhetene).

Om sikkerhetsrevisjon av Sykehuspartner HF
Datatilsynet skriver følgende; *«I forbindelse med denne saken har vi fått opplyst at helseforetakene ikke har uført sikkerhetsrevisjoner av Sykehuspartener i forkant eller i etterkant av at det ble besluttet at virksomheten skulle være databehandler for alle foretakene. Vi har ikke hatt anledning til å undersøke forholdet mellom helseforetakene og Sykehuspartner som databehandler nærmere, men dersom det aldri er gjennomført sikkerhetsrevisjon –eller risikoanalyse for bruk av sykehuspartner som databehandler, kan dette også utgjøre avvik fra kravene i personopplysningsforskriften §§ 2-5 og 2-15 og pasientjournalloven § 22.»*

Det vises her til punkt over om ansvar for og oppfølging av vurderinger av risiko og sårbarhet for infrastruktur i Helse Vest. Helse Vest IKT gjennomfører risiko- og sårbarhetsvurderinger av IKT- infrastrukturen som Helse Vest IKT har ansvaret for og oversender resultatet til helseforetakene til informasjon.

Om felles regionale systemer for tilgang til pasientinformasjon
Datatilsynet skriver følgende; *«Utviklingen i sektoren bidrar til at vi stadig ser større samlinger av pasientopplysninger lagret på ett sted. Historisk sett har risikoen for at opplysninger skal komme på avveie vært begrenset i den forstand at helseopplysninger om relativt få pasienter var spredd og lagret lokalt i ulike virksomheter. Nå er trenden at opplysningene samles i felles systemer. Det skjer i Helse Vest, Helse Midt og Helse Sør-Øst[1] i tillegg til at det skjer gjennom nasjonale systemer som reseptformidleren, kjernejournal, mv.*

Datatilsynets oppfatning er at modernisering som kan bidra til tilgjengeliggjøring av opplysninger som er nødvendige for å yte helsehjelp og dermed bedre kvalitet i helsetjenesten er positivt. Vi ønsker muligheter og initiativer velkommen, forutsatt at aktørene samtidig ivaretar sin plikt til å sørge for godt personvern gjennom blant annet å sørge for tilstrekkelige informasjonssikkerhetstiltak.»

Datatilsynet uttrykker her en *positiv* holdning til at modernisering og digitalisering ved bruk av *felles systemer* der disse kan bidra til tilgjengeliggjøring av opplysninger som er nødvendige for å yte helsehjelp og dermed bedre kvalitet i helsetjenesten. Dette er helt i tråd med det syn Helse Vest har arbeidet etter over en rekke år.

[1] *I brevet fra Datatilsynet nevnes ikke Helse Nord, men situasjonen er tilsvarende også der.*

7. Om datainnbrudd i Helse Sør-Øst RHF/Sykehuspartner
Helse Sør-Øst er i januar 2018 blitt utsatt for et omfattende hackerangrep fra en avansert og profesjonell aktør. Saken er politianmeldt og er under etterforskning. Så langt er det ingen tegn til at det har gått ut over pasientbehandlingen, pasientsikkerheten, eller at pasientinformasjon er på avveier, men det siste kan ikke utelukkes.

8. januar 2018 ble Sykehuspartner varslet av Norsk Helsenett om at det pågikk unormal aktivitet mot datasystemer i helseregionen Helse Sør-Øst. Norsk Helsenett har gjennom sin HelseCERT ansvaret for overvåkning av trafikken i det norske helsenettet. I denne saken har HelseCERT tett samarbeid med NorCERT i Nasjonal sikkerhetsmyndighet, NSM.

13. januar avdekket undersøkelsene ny informasjon som tilsa at angrepet var mer alvorlig enn tidligere antatt. Derfor ble Helsedirektoratet gitt ansvar for koordinering av beredskapsarbeidet på vegne av Helse- og omsorgsdepartementet, i tråd med Nasjonal helseberedskapsplan.

Datainnbruddet ble 14. januar politianmeldt av Sykehuspartner, og formell etterforskning ble innledet av PST. PST skal bl.a. avdekke om det kan innhentes opplysninger til fordel for en fremmed stat, og avdekke eventuelle konsekvenser av dette. Dette er et komplekst og sammensatt angrep, som det vil ta tid å få oversikt over.

Samme trusselaktør har gjennomført tilsvarende angrep mot Helse Vest IKT sin IKT-infrastruktur i samme perioden som angrepet i Helse Sør-Øst ble gjennomført. Helse Vest IKT har i hele perioden siden 8. januar 2018 samarbeidet tett med HelseCERT for å kartlegge og identifisere spor etter trusselaktøren, samt å forsterke mulige svakheter ytterligere. Det er per dags dato ikke funnet spor etter aktøren i Helse Vest IKT sin IKT-infrastruktur.

Konklusjon
Arbeidet med IKT-sikkerhet i foretaksgruppen Helse Vest tar utgangspunkt i det regionale *«Styringssystemet for informasjonssikkerhet»*. Foretakene i Helse Vest må sørge for implementering og etterlevelse av dette styringssystemet.

Risikostyring er et sentralt virkemiddel for å unngå uønskede hendelser relatert til informasjonssikkerhet. Det gjelder for å unngå tap av tilgjengelighet til relevant informasjon, konsekvenser for integriteten for informasjonen eller trusler knyttet til konfidensialitet.

Risikostyringen må baseres på systematiske vurderinger av *risiko- og sårbarhet*. *Funn* må følges opp av *tiltak*. Fordeling av *ansvar* innenfor risikostyring er viktig.