STYRESAK

GÅR TIL:	Styremedlemmer
FØRETAK:	Helse Vest RHF
DATO:	15.09.2021
SAKSHANDSAMAR:	Inger Cathrine Bryne og Erik M. Hansen
SAKA GJELD:	**Regional handlingsplan for Informasjonssikkerheit i Helse Vest**
ARKIVSAK:	2021/1010
STYRESAK:	**084/21**
STYREMØTE:	**30.09.2021**

FORSLAG TIL VEDTAK

1. Styret godkjenner Regional handlingsplan for Informasjonssikkerheit i Helse Vest.

2. Styret ber administrasjonen presentere Regional handlingsplan for Informasjonssikkerheit i Helse Vest til Helse- og omsorgsdepartementet i tråd med krav gitt i føretaksprotokollen av 14.01.2021.

3. Styret ber om at det blir lagt frem ein rapport om gjennomføring av den Regionale handlingsplanen for Informasjonssikkerheit ved utgangen av 2022.

Oppsummering
Riksrevisjonen gjennomførte i 2019/2020 ein forvaltingsrevisjon i alle dei 4 regionale helseføretaka for å kartlegge førebygging mot angrep mot sine IKT-system. Riksrevisjonen la fram sin rapport etter revisjonen 15.12.2020.

Helse- og omsorgsdepartementet fylgde opp Riksrevisjonen sin revisjon med krav knytt til dei regionale helseføretaka i føretaksmøtet 14.01.2021, jfr. fylgjande;
«Føretaksmøtet bad dei regionale helseføretaka om å:

- *utvikle ein regional handlingsplan for arbeidet med informasjonstryggleiksikkerheit som og omfattar langsiktige tiltak. Planen skal presenterast på felles tertialoppfølgingsmøte i oktober 2021.»*

Denne saka er inneheld forslag til Regional handlingsplan for arbeidet med informasjonssikkerheit i Helse Vest. Planen skal presenterast for departementet i felles tertialoppfølgingsmøte i oktober 2021.

Den regionale handlingsplanen for informasjonssikkerheit i Helse Vest er utarbeid av arbeidsgruppe for topp 5 risiko – Informasjonssikkerheit. Planen tek utgangspunkt i det kunnskapsgrunnlaget som er samla inn, primært gjennom revisjonen utført av Riksrevisjonen, men og basert på andre lokale, regionale og nasjonale kjelder.

Den regionale handlingsplanen, jfr. vedlegg 1, er synkronisert med den nasjonale strategien for digital sikkerheit i helse- og omsorgssektoren.

Fakta
Riksrevisjonen la fram sin rapport etter revisjonen 15.12.2020. For meir informasjon om handtering av revisjonen i Helse Vest, vert det vist til styresak 029/21 handsama av styret i Helse Vest RHF 24.03.2021.

Helse- og omsorgsdepartementet har gjennom oppdragsdokumentet for 2021 lagt stor vekt på å fylgje opp revisjonen utført av Riksrevisjonen. Helse Vest RHF har vidareført dette gjennom styringsdokumenta til helseføretaka og Helse Vest IKT AS.

Tekniske tiltak knytt til IKT-sikkerheit er i all hovudsak delegert til Helse Vest IKT. Tiltaka i regi av Helse Vest IKT vert gjennomført i samarbeid med helseføretaka. Ut frå ein risikobasert tilnærming har dei tekniske tiltaka hatt høg prioritet.

Det regionale arbeidet med informasjonssikkerheit[1] er i Helse Vest organisert som ein del av arbeidet med Topp 5 risiko. I det arbeidet er det etablert ei eiga arbeidsgruppe med deltakarar frå alle føretak i føretaksgruppa Helse Vest RHF, samt med representantar frå dei private, ideelle føretaka. Utkast til Regional handlingsplan for informasjonssikkerheit er utarbeid av denne arbeidsgruppa.

[1] *Informasjonssikkerheit* handlar om å sikre at informasjon i alle former; (1) ikkje vert kjent for uvedkommande (*konfidensialitet*), (2) ikkje vert endra utilsikta eller av uvedkommande (*integritet*), (3) er tilgjengelig ved behov (*tilgjengelegheit*). *IKT-sikkerheit* er ei delmengd av informasjonssikkerheit og fokuserer på teknisk sikring av IKT-infrastruktur og IKT-applikasjonar.

Kommentarar

Kunnskapsgrunnlag

Det er over tid utvikla mykje kunnskap om dette den aukande trusselsituasjonen knytt til informasjonssikkerheit. Revisjonen utført av Riksrevisjonen utgjer såleis ei viktig kjelde i kunnskapsgrunnlaget. Riksrevisjonen sine *vurderingar* er difor lagt ved i vedlegg 2.

Helse Nord IKT HF og Sykehuspartner HF har utarbeid ein felles trusselvurdering for Helse Nord RHF og Helse Sør-Øst RHF for 2021. Helse Vest RHF har fått tilgang til denne, og vurdere trusselvurderinga som godt dekkande også for Helse Vest sin del. Trusselvurdering for Helse Nord og Helse Sør-Øst (jfr. vedlegg 3) vert difor lagt fram som ein sentral del av kunnskapsgrunnlaget. Dokument gir eit godt kunnskapsgrunnlag for å kunne vurdere risiko knytt til informasjonssikkerheit også i Helse Vest.

Statens Helsetilsyn har gjennomført ei kartlegging av kritiske system, risikovurderingar og naudrutinar for IKT-system i 17 verksemder i spesialisthelsetenesta. Denne gjennomgangen viser i noko grad mogelege *konsekvensar* av truslar knytt til informasjonssikkerheit. Samandrag av rapport frå Statens helsetilsyn om forsvarlig pasientbehandling utan IKT er lagt ved i vedlegg 4.

Det vert arbeid med måling av Informasjonssikkerheitskulturen i føretaksgruppa Helse Vest. Eit sett av spørsmål vert sendt til alle tilsette. Kartlegginga er basert på ein mal utarbeid av Direktoratet for digitalisering (DigDir). Basert på resultata frå kartlegginga, må det utviklast relevante tiltak å styrke sikkerheitskulturen og for å auke kompetansen om informasjonssikkerheit.

Relevante dokument for innspel til handlingsplanen

I arbeidet med den regionale handlingsplanen er det ei rekkje dokument som er av relevans for handlingsplanen i Helse Vest. Det vert her særleg vist til «Tiltaksoversikt digital sikkerhet. Helse- og omsorgssektorens oppfølging av Nasjonal strategi for digital sikkerhet».

Regional handlingsplan for informasjonssikkerheit i Helse Vest

Den regionale handlingsplanen er strukturert i tråd med Nasjonal sikkerhetsmyndighet (NSM) sine tilrådde grunnprinsipp for informasjonssikkerhet versjon 2.0.

Utfordringsbildet i Helse Vest

Det er nedanfor gitt ei kort oppsummering av utfordringsbiletet for informasjonssikkerheit i Helse Vest.

Manglar i grunnsikring i felles IKT infrastruktur, jfr. revisjon utført av Riksrevisjonen og kartlegging av gap med NSM sine grunnprinsipp. Slike manglar gjeld særleg:

- *Oversikt over utstyr og tenester, særlig når det gjeld omfang og innhald i lokal IKT*
- *Overvaking, deteksjon og handtering av uønskte hendingar og truslar*
- *Beredskapsplanar og øvingar knytt til hendingar innanfor informasjonssikkerheit*
- *Handtering av IKT-sikkerheit ved anskaffing og utvikling av IKT-løysingar*

Det er varierande omfang av lokal IKT i helseføretak, med uklar fordeling av ansvar og oppgåver mellom Helse Vest IKT og helseføretaka. Dette tema er handtert i eiga styresak.

Den regionale felles IKT-infrastrukturen har relativt få tryggingstiltak *mellom* ulike kundegrupper, ulik informasjon og ulike tenester.

Det vert gjennomført mange vurderingar av risiko- og sårbarheit innan informasjonstryggleiksområdet, men det er krevjande gjere bruk av resultata i risikostyringa, mellom anna å sikre eigarskap til risiko og tiltak, samt samanstilling av risiko på føretaksnivå.

Auka digitalisering og innovasjon, mellom anna knytt til pasientretta sky-løysingar, medisinsk utstyr og ved behandling av pasientar heime, vil gje nye tenester som er eksponert *eksternt* og komplekse verdikjeder med ny risiko.

Forslag til overordna tiltak

Basert på utfordringsbiletet er det tilrådd ein regional handlingsplan med tiltak innanfor fylgjande områder;

1. *Roller, ansvar og oppgåver.*
   Føretaksgruppa Helse Vest må gjennomføre tiltak for å revidere og forankre korleis roller, ansvar og oppgåver er fordelt når det gjelder informasjonssikkerheit og IKT-sikkerheit. Det er særskilt behov for å avklare dette når det gjeld IKT-sikkerheit for medisinsk utstyr (MU) , teknisk utstyr (TU) og lokal IKT.

2. *Oversikt, rapportering og oppfylging.*
   Handlingsplanen inneheld tiltak for betre risikostyring gjennom betre oversikt over risiko, tilstand og avvik. Helse Vest vil bidra til det inter-regionale samarbeidet om årlege trusselvurderingar, jfr. rapport utarbeid av Sykehuspartner HF og Helse Nord IKT HF. Plan for revisjon av det regionale styringssystemet for informasjonssikkerheit, og plan for kontrolltiltak av etterleving av styringssystemet bør utarbeidast.

3. *Kultur og kompetanse innanfor informasjonssikkerheit.*
   Føretaksgruppa Helse Vest vil hausten 2021 kartlegge korleis sikkerheitskulturen er mellom tilsette. Basert på resultata av denne kartlegging, vil det verte arbeid vidare med tiltak knytt til sikkerheitskultur og kompetanse om informasjonssikkerheit for ulike grupper av tilsette.

4. *Informasjonssikkerheit i anskaffing og utvikling.*
   Det er viktig at arbeidet med informasjonssikkerheit er koordinert med anskaffing av utstyr og system eller med utvikling av nye løysingar. Når det gjeld inter-regionale og nasjonale løysingar, må dette gjerast i samarbeid med Sykehusinnkjøp HF og Norsk Helsenett SF.

5. *Applikasjonar, infrastruktur og teknisk sikkerheit.*
   Helse Vest IKT har ansvar og styringsmyndigheit for IKT-sikkerheit i den regionale IKT-infrastrukturen. Arbeidet med sikring av applikasjonar og IKT-infrastruktur må vidareførast, og helseføretaka må haldast oppdatert med omsyn til risiko og tiltak. Helse Vest IKT bør etablere kompetanse og kapasitet for å kunne gjennomføre sikkerheitsrevisjonar.

Detaljar om det einskilde tiltaket i den tilrådde regionale handlingsplanen er vist i vedlegg 1.

Gjennomføring av Handlingsplanen må organiserast slik at Helse Vest sikrar at alle føretaka i føretaksgruppa Helse Vest RHF bidrar til og gjennomfører sine tiltak. Handlingsplanen må for

ei rekkje av tiltaka involvere og krevje gjennomføring av tiltak i dei føretak som inngår i det regionale styringssystemet for Felles EPJ.

Det er difor tilrådd at gjennomføringa vert organisert som eit regionalt prosjekt for Informasjonssikkerheit i Helse Vest. Prosjektet må organiserast slik at det kan gjennomføre tiltaka i den regionale handlingsplanen.

Det må avklarast at det er tilstrekkeleg med kompetanse og kapasitet innanfor informasjonssikkerheit til å kunne gjennomføre tiltaka i handlingsplanen. Prioritering av dette må sjåast i samanheng med den overordna risikostyringa knytt til topp 5 risiko i Helse Vest.

Finansiering av gjennomføring av handlingsplanen må innarbeidast i budsjett for det enkelte føretaka, også i budsjettet for Helse Vest IKT.

Konklusjon

Trusselbiletet for informasjonssikkerheit er aukande og i endring. Arbeidet med informasjonssikkerheit er eit *kontinuerleg* arbeid for å sikre at relevant personell har tilgang til relevant informasjon på rett tid og stad, for å sikre integriteten i informasjonen og for å unngå truslar knytt til konfidensialitet for informasjonen.

Administrasjonen er av det syn at Regional handlingsplan for informasjonssikkerheit må gjennomførast for å vidareføre ei tilfredsstillande sikring av informasjonen i føretaksgruppa Helse Vest RHF, og for dei private, ideelle føretaka som inngår i samarbeidet om Felles EPJ.