DigiFinland

AI/MDR-työryhmän näkökulmia riskienhallintaan

Riskienhallinnan webinaari 2.6.2026

Suvi Nevalainen (pj. AI/MDR-työryhmä)

pääjuristi, tietosuojavastaava, DigiFinland Oy

OTM, HTM, tradYAMK (tekoäly ja data), CIPP/E, CIPM

AI/MDR-työryhmä

Sotetekoälyn ekosysteemin alaryhmä.

- Kokoontuu 2-3 kertaa kaudessa: eri puolilta ekosysteemiä: yrittäjiä, alan järjestöjen edustajia, viranomaisia, valtio&sotejärjestäjien sidosyksikköjen edustajia.
- ”Ydinryhmä”: n. 10 AI/MDR -työryhmän asiantuntijaa. Pro bono -tukiklinikoita konkreettisille tapauksille sekä yksittäisiä tuotoksia ja yhteistyötä muiden sidosryhmien kanssa.

AI:ta sisältävien lääkinnällisten laitteiden (ohjelmistot) riskienhallinta

Riskienhallinta on vastuullisuutta

Riskienhallinta on keskeinen osa turvallista ja vastuullista AI:n käyttöönottoa sekä potilasturvallisuuden varmistamista sekä luottamuksen edistämistä.

Riskienhallinta työkaluna

Riskienhallinta toimii työkaluna päätöksenteossa ja strategisessa ohjauksessa AI/MDR-ratkaisuissa.

Sääntelyn velvoitteet riskienhallintaan

EU:n MD- ja AI-lainsäädäntö asettavat velvoitteita lääkinnällisille laitteille ja suuren riskin tekoälyjärjestelmille. Ne konkretisoituvat arjen riskienhallinnan käytännöissä.

Riskienhallinnan lähtökohtia sääntelyssä

High-risk: jos AI-järjestelmä MDR-tuote tai turvallisuuskomponentti ja laite edellyttää 3. osapuolen arviointia

Sisäänrakennettu riskienhallinta

Riskienhallinta on osa tuotteen elinkaarta ja laatujärjestelmää, ei erillinen prosessi.

Dual compliance

Lääkinnälliset laitteet (MDR) ja tekoälyjärjestelmät (AI act) vaativat samanaikaista sääntelyn noudattamista, mikä lisää kompleksisuutta. Huom! Muutosesitysten EU-käsittely kesken. Lisänä muu sääntely, kuten esim. GDPR ja kaikki vo-sääntely.

Systemaattinen dokumentointi

MD-asetus edellyttää valmistajalta dokumentoitua (ja auditoitavaa) riskienhallintaprosessia osoittamaan riskien tunnistaminen ja hallinnan. AI act edellyttää myös dokumentoitavaa riskienhallintaa suuririskisissä AI-järjestelmissä. Huom! Valmistaja, tarjoaja, käyttäjä **roolit** sekä **käyttötarkoitus** niin AI actin ja MDR:n mukaan

Monien toimijoiden vastuu

Riskienhallinta jakaantuu valmistajien, käyttäjäorganisaatioiden ja muiden roolien kesken.

Käyttäjäroolin merkitys

AI actin Käyttäjärooli korostaa organisaation vastuuta AI:n käytöstä ja riskien hallinnasta. (Käyttäjä myös yleensä tarjoaja jos MDR-valmistaja.)

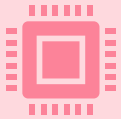
Yhteistyö ja juridinen ymmärrys

Toimijoiden tulee ymmärtää roolinsa ja tehdä yhteistyötä riskien hallitsemiseksi juridisen ja käytännön osaamisen pohjalta.

Integroitu : yksi runko, kaksi sääntelykerrosta

MDR: kliininen turvallisuus + suorituskyky + benefit-risk + PMS.

AI Act: elinkaaren aikainen AI-riskienhallinta + perusoikeudet + data + läpinäkyvyys + ihmisen valvonta + robustius.



Yhdessä: yksi QMS-pohjainen riskienhallinta, jossa AI Act täydentää MDR:ää – ei erillistä rinnakkaisjärjestelmää, vaan integroitu evidenssi ja seuranta.

AI-MDR-lääkintälaiteohjelmiston riskienhallinta
MDR-runko → AI Actin lisäkerros → integroitu riskienhallinta

-- provider/valmistaja-tasoinen compliance-rakenne, ei ensisijaisesti deployer-tason käyttöohjeistus

1. MDR-runko

Kliininen turvallisuus ja suorituskyky

- Riskienhallintajärjestelmä koko elinkaarelle
- Riskit poistetaan tai pienennetään niin pitkälle kuin mahdollista
- Hyöty–haitta-suhteen on oltava hyväksyttävä
- GSPR + QMS + PMS muodostavat perusrungon
- ISO 14971: suunnitelma → vaarat → arviointi → kontrollit → jäännösriskit
- V&V + IFU + käyttörajat osoittavat kontrollien toimivuuden

2. AI Actin lisäkerros

AI-spesifit riskit + perusoikeudet

- Jatkuva ja iteratiivinen riskienhallinta koko elinkaarelle
- Riskit terveydelle, turvallisuudelle ja perusoikeuksille
- Mukana myös kohtuudella ennakoitava väärinkäyttö
- Datahallinta, läpinäkyvyys, lokitus ja human oversight
- Tarkkuus, robustisuus ja kyberturvallisuus
- Post-market monitoring kytketään riskien päivitykseen

3. Integroitu riskienhallinta

Yksi runko, kaksi sääntelykerrosta

- Ei kahta rinnakkaista järjestelmää, vaan yksi yhteinen prosessi
- Yksi riskirekisteri, QMS ja evidenssirunko
- MDR = potilasturvallisuuden ja suorituskyvyn perusta
- AI Act = AI-spesifit kontrollit ja perusoikeuskerros
- Testaus, dokumentaatio ja seuranta samaan malliin
- Tuloksena tehokkaampi, auditointikelpoinen kokonaisuus

AI-MDR-tuotteessa MDR-valmistaja ei yleensä jää AI Actissa pelkäksi käyttäjäksi: Jos toimija tuo AI-järjestelmän markkinoille tai ottaa sen käyttöön omalla nimellään, se on tarjoaja. Lääkintälaitekontekstissa **AI actin mukaan jos suuren riskin AI on liitteen I -tuotteen** (kuten MDR-laitteen) **turvallisuuskomponentti tai osa tuotetta**, tuotteen **valmistajaa pidetään AI actin tarjoajana**, jos AI saatetaan markkinoille tai otetaan käyttöön valmistajan nimellä.

(Julkisella toimijalla on käyttäjän perusvelvoitteet ja lisäksi tietyissä liitteen III / artikla 6(2) -tilanteissa fundamental rights impact assessment (FRIA) ennen ensimmäistä käyttöä; arvioinnissa kuvattava mm. käyttökonteksti, riskit ja riskien toteutumisen hallintatoimet.)

Nämäkin sisälle riskienhallintaan - nostoja

Sääntelyn asettamien vaatimusten epäselvyys tai tulkintaerot

Toimintaympäristön epävarmuutta lisää sääntelyn keskeneräisyys, erilaiset tulkinnat ja luokittelukysymykset.

Tekoälyn erityisriskit

Tekoälyyn liittyy vaikeasti havaittavia riskejä kuten datavinoumat ja selitettävyyden puute.

Nopea teknologian kehitys

Teknologian nopea muutos vaikeuttaa riskien ennakointia turvallisuuden ja luotettavuuden suhteen ja vaatii jatkuvaa sopeutumista.

Jatkuva sopeutuminen

Kyky oppia ja reagoida nopeasti on keskeistä tehokkaassa riskienhallinnassa epävarmuuden keskellä.

Sopimukset

Ymmärrys, mistä sovitaan ja mistä tulee sopia, vastuukysymykset, **käyttötarkoitus**, **muutostarpeet**, enemmän yhteistyötä ja kumppanuutta partien välillä, **dataan** liittyvät omistus- ja luottamuskysymykset

Selkeytä! Standardit hyödynnettäväksi; rakenna aiemman pohjalle; osallistu - jaa ja ota oppia muilta

Standardien merkitys

Konkretisoivat riskienhallintaa sääntelyn vaatimusten mukaisesti. Yhdistävät toimijat ja tukevat yhtenäistä tulkintaa, arviointeja, käsitteistöä ja terminologiaa.

Keskeiset standardit MDR

ISO 14971 määrittelee MDR-riskienhallintaprosessin ja ISO 13485 muodostaa laadunhallintajärjestelmän rakenteen.

Tekoälyn standardointi ja sertifiointi

Tekoälyn standardointi etenee, keskittyen datan laatuun, algoritmien luotettavuuteen ja valvontaan. ISO 42001:2023 (uusin 42001/2026) hallintamalli (AIMS), ISO/IEC 22989:2022 konseptit ja termit sekä ISO 23894:2023 riskienhallinta. Tekoälyn hallintamallin sertifiointi: ISO 42006:2025:ssa kuvataan ISO-standardit, jotka pohjana ISO 42001-sertifikaatille.**= vaatimustenmukaisuus**

ISO-perheeseen on rakennettu MDR:n ja AI actin vaatimukset.

EU:lta tulossa EN-standardeja (CENCENELEC)

Ilmoitettujen laitosten auditointivalmius Suomessa??

Medical Device Coornination Group – ohjeet; muut EU-ohjeet

Tukea mm.: AI-Regu: sääntelypolku ja asiantuntijalista; AI/MDR –työryhmä: tukiklinikka ja AI/MDR tarkistuslista

Kiitos!