Terveysteknologia ry

Lausunto

07.02.2025

Asia: VN/2104/2025-LVM-1

Lausuntopyyntö luonnoksesta hallituksen esitykseksi kyberturvallisuuslain muuttamisesta

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Terveysteknologia ry:n lausunto luonnoksesta hallituksen esitykseksi kyberturvallisuuslain muuttamisesta (Dnro VN/2104/2025-LVM-1)

Terveysteknologia ry kiittää liikenne- ja viestintäministeriötä mahdollisuudesta antaa lausunto hallituksen esityksestä kyberturvallisuuslain muuttamiseksi.

Terveysteknologian alalla kyberturvallisuus on kriittinen osa potilasturvallisuutta, liiketoiminnan jatkuvuutta ja alan kilpailukykyä. Terveysala on herkästi kyberturvallisuuskriisin kohteena, jos kiristysohjelmat ja tietomurrot kohdistuvat sairaaloihin ja terveydenhuollon tarjoajiin. Tietojemme mukaan 54 prosenttia terveydenhuollon kyberhyökkäyksistä liittyy kiristysohjelmiin ja 46 prosenttia potilastietojen tietomurtoihin. Nämä uhat vaarantavat potilasturvallisuuden, tietojen eheyden ja terveydenhuollon palveluiden jatkuvuuden.

Haluamme tässä lausunnossa kiinnittää erityistä huomiota lakiehdotuksen vaikutuksiin lääkinnällisten laitteiden valmistajiin ja muihin terveysteknologiayrityksiin, erityisesti suhteessa MD-asetuksen (Medical Device Regulation, EU 2017/745, MDR) ja IVD-asetuksen (In Vitro Diagnostics Regulation, EU 2017/746, IVDR) jo asettamiin kyberturvallisuusvaatimuksiin sekä muihin markkinavaatimuksiin, jotka heijastuvat yrityksiin hyvinvointialueiden ja terveydenhuollon toimintayksiköiden hankintavaatimusten kautta.

1. Soveltamisalan laajentuminen ja vaikutukset terveysteknologia-alalle

Kyberturvallisuuslain ehdotettu muutos laajentaa kyberturvallisuusvelvoitteita koskemaan myös keskisuurta pienempiin yrityksiin, jotka tultaisiin määrittelemään kriittisiksi toimijoiksi. Terveysteknologia ry toteaa, että MD- ja IVD-asetukset jo määrittävät lääkinnällisille laitteille ja niiden valmistajille tiukat kyberturvallisuusvaatimukset ihmisille kohdistuvien riskien ehkäisemiseksi. MD- ja IVD-asetukset eivät sisällä suoranaisesti kyberturvallisuutta koskevaa erillistä lukua tai määritelmää, mutta ne asettavat vaatimuksia, jotka efektiivisesti liittyvät kyberturvallisuuteen erityisesti lääkinnällisten laitteiden turvallisuuden ja suorituskyvyn näkökulmasta.

MD- ja IVD-asetusten mukaisesti lääkinnällisten laitteiden valmistajien on jo:

- Toteutettava riskienhallinta koko laitteen elinkaaren ajan
- Varmistettava ohjelmistojen ja laitteistojen kyberturvallisuus
- Raportoitava kyberuhkista ja turvallisuuspoikkeamista viranomaisille
- Toteutettava tietoturvapäivityksiä ja seurattava haavoittuvuuksia

Kyberturvallisuuslain ehdotuksen mukaan kriittisiksi toimijoiksi luettavat keskisuurta pienemmät yritykset tulevat uuden valvontajärjestelmän ja raportointivelvoitteiden piiriin. Tämä voi johtaa tilanteeseen, jossa terveysteknologiayritykset joutuvat noudattamaan sekä MD- ja IVD-asetusten että uuden kyberturvallisuuslain ilmoitusvelvoitteita erikseen, mikä lisää hallinnollista taakkaa ja kustannuksia. Ehdotamme, että terveysteknologian osalta lainsäädännössä tunnistetaan MD- ja IVD-asetusten fokusalue sekä vaatimukset ja varmistetaan, että sääntely on yhdenmukaista ja kohdistettu oikein. Uuden lain vaikutukset MD- ja IVD-asetusten piirissä oleviin yrityksiin tulee arvioida tarkasti, jotta vältytään päällekkäiseltä sääntelyltä ja kohtuuttomalta hallinnolliselta taakalta.

2. Hyvinvointialueiden ja terveydenhuollon yksiköiden vaatimusten vaikutukset toimittajiin

Hyvinvointialueet ja terveydenhuollon toimintayksiköt ovat uusien kyberturvallisuusvelvoitteiden alaisia, mikä vaikuttaa suoraan myös lääkinnällisten laitteiden ja terveysteknologian toimittajiin. Tämä tapahtuu erityisesti seuraavilla tavoilla:

- Hankintavaatimukset: Julkiset terveydenhuollon yksiköt voivat asettaa tiukempia kyberturvallisuusvaatimuksia laitetoimittajille, mikä voi edellyttää lisäsertifiointeja ja auditointeja.
- Sopimusperusteinen vastuu: Toimittajilta voidaan vaatia pitkäaikaisia tietoturvapäivityksiä ja poikkeamailmoituksia, jotka voivat ylittää MD- ja IVD-asetusten perusvaatimukset.
- Tietoturvastandardien harmonisointi: Yksityiskohtaisemmat standardit (esim. ISO 27001, IEC 62443) voivat tulla pakollisiksi hankintasopimusten kautta.

3. Yhteenveto

Terveysteknologia ry tukee kyberturvallisuuden kehittämistä ja ymmärtää sen tärkeyden terveysteknologia-alalla. Samalla kuitenkin korostamme, että uusi sääntely ei saa lisätä tarpeettomia hallinnollisia kustannuksia yrityksille, jotka jo noudattavat MD- ja IVD-asetusten mukaisia tiukkoja kyberturvallisuusvaatimuksia. Vaikka terveysteknologian yritykset eivät olisikaan suoraan uuden kyberturvallisuuslain kohteena, ne joutuvat noudattamaan sen periaatteita markkinavaatimusten kautta.

Ehdotamme, että liikenne- ja viestintäministeriö vahvistaa julkisen ja yksityisen sektorin kumppanuuksia, ja tarjoaa käytännön tukea sääntelyn noudattamisessa ja uhkien hallinnassa. Painopisteen tulisi olla olemassa olevien säädösten tehokkaassa täytäntöönpanossa uusien lainsäädäntöjen sijaan.

Keskeisiä suosituksiamme ovat muun muassa toimitusketjun kyberresilienssin vahvistaminen, kyberturvallisuuden parantaminen hankinnoissa, rahoituksen ja taitojen kehittämiseen investoiminen ja NIS2-direktiivin täytäntöönpanon selkeyttäminen.

Terveysteknologia ry on valmis tarjoamaan asiantuntemustaan, jotta laki saadaan toimimaan mahdollisimman hyvin terveysteknologian yritysten näkökulmasta.

Hassinen Saara
Terveysteknologian Liitto ry

Liede Sandra
Terveysteknologia ry