Sosiaali- ja terveydenhuollon resilienssi ja varautuminen: sisältö ja vastuut

12.6.2026

Resilient Botnia –hanke, jota rahoitti Interreg Aurora –ohjelma, keskittyi erityisesti Sosiaali- ja terveydenhuollon resilienssiin. On tärkeää varmistaa palvelujen jatkuvuus myös häiriötilanteissa, kuten pandemioissa, kyberhäiriöissä, henkilöstöpulassa tai muissa kriiseissä. Riittävän resilientti sosiaali- ja terveydenhuoltojärjestelmä pystyy

- säilyttämään toimintakykynsä paineen alla
- turvaamaan potilas- ja asiakasturvallisuuden
- kohdentamaan resurssit kriittisiin palveluihin
- reagoimaan nopeasti muuttuviin tilanteisiin
- suojaamaan henkilöstön jaksamista
- hyödyntämään tietoa päätöksenteossa ja ennen kaikkea
- oppimaan kriiseistä tulevaa varautumista varten.

Resilienssi tutkimuksen valossa

Sosiaali- ja terveydenhuollon resilienssillä viitataan siis terveysjärjestelmän kykyyn ylläpitää keskeisiä toimintojaan häiriötilanteissa, palauttaa toimintakykynsä häiriön jälkeen sekä mukauttaa rakenteitaan ja toimintamallejaan muuttuvien olosuhteiden perusteella. Resilienssi on moniulotteinen kokonaisuus, jossa yhdistyvät kriiseihin vastaaminen, toiminnallinen jatkuvuus, institutionaalinen oppiminen ja pitkän aikavälin uudistumiskyky. Näin ymmärrettynä resilienssi ei ole ainoastaan poikkeusoloihin liittyvä valmius, vaan terveysjärjestelmän rakenteellinen ominaisuus, joka ilmenee sekä häiriöihin reagoimisessa että niiden jälkeen tapahtuvassa kehittämisessä.

Resilienssin sisältö jäsentyy kirjallisuudessa tavallisesti ennakoinnin, varautumisen, reagoinnin ja oppimisen toisiaan täydentäviin kyvykkyyksiin. Näiden ulottuvuuksien avulla voidaan kuvata, miten järjestelmä tunnistaa riskejä, valmistautuu häiriöihin, ylläpitää päätöksentekokykyään paineen alla ja muuntaa kokemuksiaan myöhempää kehittämistä tukevaksi tiedoksi. Resilienssi ei rajaudu ainoastaan akuuttiin kriisinhallintaan, vaan kytkeytyy laajemmin terveysjärjestelmän hallintaan, palvelurakenteisiin, tiedon tuotantoon sekä institutionaalisiin käytäntöihin. Tämän vuoksi resilienssiä on mahdollista tarkastella sekä järjestelmän häiriönsietokykyä että sen kykyä uudistua muuttuvissa toimintaympäristöissä.

Varautuminen muodostaa resilienssin operatiivisen ulottuvuuden, jossa käsitteellinen valmius konkretisoituu organisatorisiksi ja toiminnallisiksi järjestelyiksi. Varautuminen ymmärretään sekä ennakoivana suunnitteluna että konkreettisina kyvykkyyksinä, kuten resurssien kohdentamisena, kapasiteetin joustavuutena, toimintaprosessien harjoitteluna ja kriittisten palvelujen jatkuvuuden turvaamisena. COVID-19-pandemia toi kuitenkin näkyväksi sen, että muodolliset suunnitelmat eivät yksin riitä, mikäli järjestelmältä puuttuu kyky mukauttaa toimintaansa nopeasti muuttuvissa olosuhteissa. Varautumisen arvioinnissa onkin perusteltua kiinnittää huomiota paitsi suunnitelmien olemassaoloon myös siihen, miten hyvin ne mahdollistavat toiminnan jatkuvuuden, priorisoinnin ja koordinaation todellisissa häiriötilanteissa.

Resilienssiin liittyvät vastuut jakautuvat useille hallinnan tasoille ja toimijoille, minkä vuoksi ilmiötä ei voida palauttaa yksittäisten organisaatioiden tai toimijoiden ominaisuudeksi. Makrotasolla korostuvat strateginen ohjaus, sääntely, rahoitus ja kansallisen valmiuden koordinointi, kun taas organisaatiotasolla keskeisiä ovat johtaminen, resurssien hallinta, henkilöstön osaamisen turvaaminen sekä palvelujen jatkuvuuden varmistaminen. Viimeaikaiset katsaukset osoittavat, että resilienssi rakentuu monitoimijaisessa verkostossa, jossa julkisen hallinnon, palveluntuottajien ja muiden sidosryhmien välinen koordinaatio vaikuttaa ratkaisevasti siihen, miten tehokkaasti järjestelmä kykenee vastaamaan häiriöihin, ylläpitämään toimintakykyään ja uudistumaan kriisien jälkeen.

Sosiaali- ja terveydenhuollon henkilöstö

Henkilöstöön liittyvät ulottuvuudet ovat resilienssin kannalta keskeisiä, koska palvelujärjestelmän toimintakyky on viime kädessä riippuvainen henkilöstön saatavuudesta, osaamisesta, työhyvinvoinnista ja kyvystä toimia pitkittyneissä kuormitustilanteissa. Häiriötilanteissa henkilöstön suojaaminen, työn organisoinnin joustavuus, tehtävien uudelleenjärjestely sekä riittävä johtamisen tuki ovat olennaisia tekijöitä järjestelmän kestokyvyn ylläpitämisessä. Näin ollen henkilöstöä ei ole perusteltua tarkastella pelkästään resurssina, vaan resilienssin toteutumisen ehtona, jonka heikkeneminen voi heijastua suoraan palvelujen jatkuvuuteen ja laatuun.

Resilienssiin sisältyy lisäksi oppimisen ja institutionaalisen kehittämisen ulottuvuus, joka erottaa sen pelkästä kriisinkestävyydestä. Resilienssi-tilanteessa häiriöistä tuotettu tieto muokkaa järjestelmän rakenteita, käytäntöjä ja päätöksenteon mekanismeja. Järjestelmällinen arviointi, kokemusten analysointi ja havaittujen puutteiden muuntaminen pysyviksi kehittämistoimiksi ovat siten keskeisiä pitkäjänteisen varautumisen edellytyksiä. Tässä mielessä resilienssi kytkeytyy myös organisaation ja koko järjestelmän kykyyn institutionalisoida oppimista osaksi normaalia toimintaa.

Edellä esitetyn perusteella sosiaali- ja terveydenhuollon resilienssi ja varautuminen voidaan jäsentää toisiinsa

kytkeytyväksi kokonaisuudeksi, jossa strateginen ohjaus, operatiivinen valmius, henkilöstö, tiedonhallinta ja institutionaalinen oppiminen muodostavat vastavuoroisesti toisiaan tukevia osa-alueita. Tarkastelu osoittaa, että varautuminen ei ole vain yksittäisten häiriöiden hallintaa, vaan laajempi järjestelmätason ominaisuus, jonka kautta määrittyvät palvelujen jatkuvuuden, sopeutumiskyvyn ja uudistumisen edellytykset.

Tiedonhallinta ja resilienssi

Yksi resilienssin keskeisistä ulottuvuuksista liittyy tiedon, tilannekuvan ja päätöksenteon tietoperustan hallintaan. Tiedon saatavuus, laatu, ajantasaisuus ja yhteentoimivuus vaikuttavat olennaisesti siihen, kuinka nopeasti ja tarkoituksenmukaisesti järjestelmä kykenee tunnistamaan häiriöitä, kohdentamaan resursseja ja mukauttamaan toimintaansa. Tiedonhallinnan puutteet voivat puolestaan heikentää johtamisen laatua, hidastaa koordinaatiota ja lisätä epävarmuutta päätöksenteossa. Tästä näkökulmasta tietojärjestelmien toimintavarmuus ja tiedolla johtamisen käytännöt eivät ole ainoastaan hallinnollisia tukitoimintoja, vaan resilienssin institutionaalista perustaa rakentavia tekijöitä.

Terveydenhuollon digitalisaatio on lisännyt palvelujärjestelmän tehokkuutta ja mahdollistanut uusia toimintamalleja, mutta samalla se on syventänyt riippuvuutta sähköisistä potilas- ja asiakastietojärjestelmistä, etäpalveluista, kliinisestä päätöksenteosta tukevista ratkaisuista sekä laajasti verkottuneista tietoinfrastruktuureista. Tämän vuoksi digitaalista varautumista on perusteltua tarkastella osana terveysjärjestelmän kokonaisresilienssiä eikä erillisenä teknisenä osa-alueena. Kyberhyökkäykset, palvelunestot, käyttökatkot ja tiedon eheyteen kohdistuvat häiriöt voivat heijastua suoraan hoidon jatkuvuuteen, potilasturvallisuuteen ja organisaation kykyyn ylläpitää kriittisiä toimintoja. Digitaalinen varautuminen edellyttää siten riskiperusteista hallintaa, tietojärjestelmien jatkuvuus- ja palautumissuunnittelua, käyttövaltuuksien hallintaa, tietoturvakulttuurin vahvistamista sekä poikkeamien tunnistamiseen ja hallintaan liittyviä organisatorisia menettelyjä. Olennaista on, että digitaalinen turvallisuus ymmärretään osaksi palvelujärjestelmän ydintoimintaa eikä pelkästään tukifunktion vastuulle kuuluvaksi kysymykseksi.

Teknologiaan ja teknologia-infraan liittyvä varautuminen ulottuu yksittäisiä tietojärjestelmiä laajemmalle ja kohdistuu koko palvelutuotannon teknisiin riippuvuuksiin. Näihin kuuluvat esimerkiksi tietoliikenneyhteydet, palvelin- ja pilviympäristöt, lääkintälaitteisiin integroidut ohjelmistot, sähkö- ja varavoimaratkaisut, laitteiden elinkaaren hallinta, ohjelmistopäivitykset sekä toimittaja- ja alihankintaketjujen toimintavarmuus. Viimeaikainen tutkimus korostaa, että terveydenhuollon infrastruktuurinen resilienssi rakentuu samanaikaisesti teknisistä ja organisatorisista mekanismeista, kuten verkkojen segmentoinnista, palautumiskyvykkyyksistä, simulaatioista ja häiriöharjoituksista, vastuiden täsmällisestä määrittelystä sekä turvallisuus- ja jatkuvuusvaatimusten ulottamisesta koko toimitusketjuun. Näin tarkasteltuna teknologia-infran varautuminen ei rajaudu laitteiden ja järjestelmien suojaamiseen, vaan liittyy laajemmin siihen, miten palvelujärjestelmä hallitsee teknologisia riippuvuuksiaan ja niiden aiheuttamia jatkuvuusriskejä. Tältä osin myös eurooppalainen sääntely vahvistaa näkemystä siitä, että kriittisillä toimialoilla teknologia-infran varautuminen on osa laajempaa yhteiskunnallista turvallisuutta ja palvelujen jatkuvuuden turvaamista.

Lopuksi

Sosiaali- ja terveydenhuollon resilienssi on tärkeää, koska ilman sitä sosiaali- ja terveydenhuoltojärjestelmä voi häiriötilanteissa menettää kykynsä tarjota välttämättömiä palveluja turvallisesti ja oikea-aikaisesti. Tämä taas saattaa johtaa siihen, että ihmiset menettävät luottamuksensa sosiaali- ja terveydenhuollon lisäksi myös muihin yhteiskunnan toimintoihin.

Artikkeli on osa Resilient Botnia (Interreg Aurora) hanketta, joka on Euroopan unionin osarahoittama.

Sami Perälä
Projektipäällikkö & kehittämispäällikkö, Hyvinvointi ja luovuus
ORCID 0000-0002-0853-3747
SEAMK

Jari Alanko
Erityisasiantuntija, kansainvälinen TKI
SEAMK

Lähteet

Atighechian, G., Rahimi, A., Sattari, M., & Mohammadi, M. (2024). Dimensions of hospital resilience emphasized during the COVID-19 pandemic response: A systematic review. *Health Science Reports, 7*(8), e2300. https://doi.org/10.1002/hsr2.2300

Biddle, L., Wahedi, K., & Bozorgmehr, K. (2020). Health system resilience: A literature review of empirical research. *Health Policy and Planning, 35*(8), 1084–1109. https://doi.org/10.1093/heapol/czaa032

Clarke, M., & Martin, K. (2024). Managing cybersecurity risk in healthcare settings. *Healthcare Management Forum, 37*(1), 17–20. https://doi.org/10.1177/08404704231195804

Dixit, A., Quaglietta, J., Nathan, K., Dias, L., & Nguyen, D. (2023). Cybersecurity: Guiding principles and risk management advice for healthcare boards, senior leaders and risk managers. *Healthcare Quarterly, 25*(4), 35–40. https://doi.org/10.12927/hcq.2023.27019

Dsouza, S. M., Katyal, A., Kalaskar, S., Kabeer, M., Rewaria, L., Satyanarayana, S., Nallamalla, K. R., & Chokshi, M. (2024). A scoping review of health systems resilience assessment frameworks. *PLOS Global Public Health, 4*(9), e0003658. https://doi.org/10.1371/journal.pgph.0003658

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). (2022). *Official Journal of the European Union, L 333*, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

El-Jardali, F., Kanth, P. D., Nguyen, S.-N., Varkey, S., & Duran, D. (2025). Emergency preparedness and health system resilience assessment tool: Development and initial validation. *BMJ Global Health, 10*(8),

e016459. DOI: 10.1136/bmjgh-2024-016459

Emami, S. G., Lorenzoni, V., & Turchetti, G. (2024). Towards resilient healthcare systems: A framework for crisis management. *International Journal of Environmental Research and Public Health, 21*(3), 286. https://doi.org/10.3390/ijerph21030286

Hasegawa, K., O'Brien, N., Prendergast, M., Ajah, C. A., Neves, A. L., & Ghafur, S. (2024). Cybersecurity interventions in health care organizations in low- and middle-income countries: Scoping review. *Journal of Medical Internet Research, 26*, e47311. https://doi.org/10.2196/47311

Kramer, D. B., & Fu, K. (2024). Promoting the resilience of health care information systems—The day hospitals stood still. *JAMA Health Forum, 5*(11), e243968. https://doi.org/10.1001/jamahealthforum.2024.3968

Luidold, C., & Jungbauer, C. (2024). Cybersecurity policy framework requirements for the establishment of highly interoperable and interconnected health data spaces. *Frontiers in Medicine, 11*, 1379852. https://doi.org/10.3389/fmed.2024.1379852

Mustafa, S., Zhang, Y., Zibwowa, Z., Seifeldin, R., Ako-Egbe, L., McDarby, G., Kelley, E., & Saikat, S. (2022). COVID-19 preparedness and response plans from 106 countries: A review from a health systems resilience perspective. *Health Policy and Planning, 37*(2), 255–268. https://doi.org/10.1093/heapol/czab089

Tynkkynen, L.-K., Karreinen, S., Satokangas, M., Viita-Aho, M., Keskimäki, I., Zimmermann, J., Haywood, P., Cylus, J., & Karanikolos, M. (2025). Resilience testing in action: Piloting the health system resilience testing tool with a pandemic scenario in Finland. *BMC Health Services Research, 25*, 793. https://doi.org/10.1186/s12913-025-12864-w

Witter, S., Thomas, S., Topp, S. M., Barasa, E., Chopra, M., & Cobos, D. (2023). Health system resilience: A critical review and reconceptualisation. *The Lancet Global Health, 11*(9), e1454–e1458. DOI: 10.1016/S2214-109X(23)00279-6