Petri Tolonen
Pekka Vepsäläinen
kirjoittajat ovat projektipäällikköjä
Huoltovarmuuskeskuksen
Kyber-Terveys-hankkeessa

Vaarantuuko potilasturvallisuus kyberuhkien edessä?

Petri Tolonen Pekka Vepsäläinen

Digitalisaation aiheuttama nopea muutos on tuonut lääkärin työhön uuden huomioon otettavan asian – kyberturvallisuuden. Lääkinnälliset laitteet ja sairaaloiden tietojärjestelmät kytketään yhä useammin tietoverkkoihin, toisiin tietojärjestelmiin ja internettiin, mikä tehostaa hoitotyötä, mutta tuo samalla mukanaan kyberuhkia, jotka voivat vaarantaa niin potilasturvallisuuden kuin potilaiden yksityisyyden suojankin.

Huoltovarmuuskeskuksen vuonna 2017 käynnistämässä hankkeessa kehitetään yhdessä sairaanhoitopiirien kanssa terveydenhuollon sektorin varautumista erilaisiin kyberuhkiin. Kehittämisen keskiössä on potilasturvallisuuden varmistaminen kliinisessä työssä.

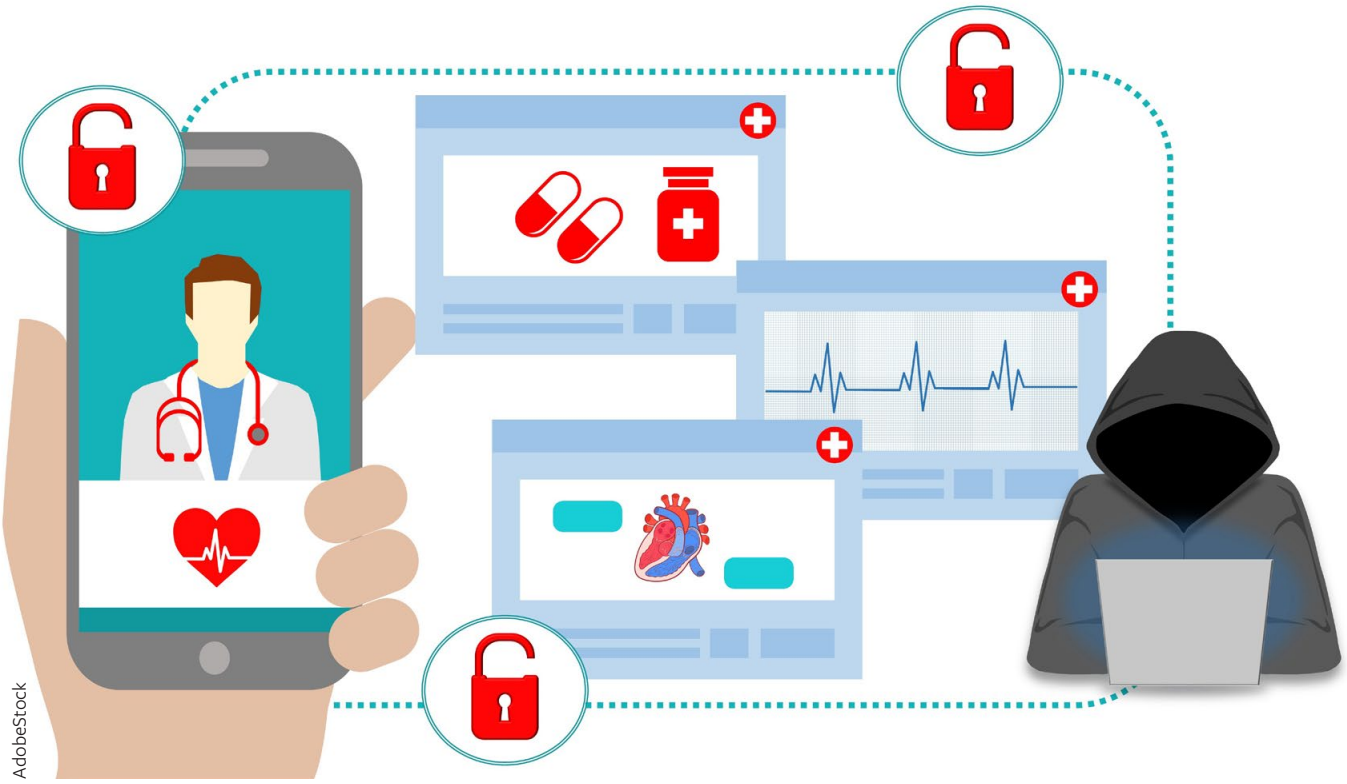
Digitaalinen murros muuttaa lääkärin työtä

Lääkärin työ on suuremmassa murroksessa kuin koskaan aiemmin johtuen digitalisaatiosta. Digitalisaation aiheuttama muutos näkyy lääkärin arjessa monella tapaa. Uudet lääkinnälliset laitteet, älykkäät sensorit ja ohjelmistot sekä robotiikka ja tekoäly yhdistettynä uusiin tehokkaampiin tietoverkkoihin ja pilvipalveluihin muodostavat yhä laajempia kokonaisuuksia ja muokkaavat merkittävästi lääkärin toimintaympäristöä. Niiden avulla voidaan monet työvaiheet automatisoida, jolloin ne on mahdollista tehdä ajasta ja paikasta riippumatta.

Nämä laajamittaiset muutokset edellyttävät jatkuvaa uuden oppimista. Uusien ohjelmistojen ja laitteiden käytön oppimisesta on saatava jatkuva prosessi, jonka avulla lääkäri voi mahdollisimman jouhevasti hyödyntää uutta toimintaympäristöä ja uusia teknologioita osana potilastyötä.

Tämä terveydenhuollon nopea tietotekninen murros edellyttää myös tietoturvan huomioimista uudella tavalla, koska heikko tietoturva vaarantaa potilasturvallisuuden monin eri tavoin. Potilastietojen muuttuminen tietojärjestelmissä vahingossa tai tahallisesti voi johtaa vääriin diagnooseihin. Tietoturvaa on myös se, että kaikki tarvittava potilastieto on saatavilla ja käytettävissä silloin, kun hoitotoimenpiteistä päätetään. Esimerkiksi tietojärjestelmän käyttökatkoksen aikana ei välttämättä saada hoitopäätöksiin tarvittavaa potilastietoa silloin, kun sitä tarvittaisiin. Terveydenhuollon toimintaympäristön murroksessa tietoturvasta onkin tullut yhä tärkeämpi osa potilasturvallisuutta. Sairaalaympäristössä joudutaan siten hallitsemaan yhä monimutkaisempia tietoteknisiä kokonaisuuksia tietoturvan eri näkökulmista niin lääkärien arjessa kuin taustalla toimivissa tukiprosesseissakin.

Tietoturvan asianmukainen varmistaminen edellyttää terveydenhuollon toimijoilta sekä arkipäivän tietoturvaosaamista että kyberturvallisuuden kokonaisuuden hallintaa organisaation kaikilla tasoilla. Jokaisen lääkärin on tutustuttava oman organisaation tietoturvaohjeisiin ja noudatettava niitä.



AdobeStock

Terveydenhuollon toimintaympäristön murroksessa tietoturvasta on tullut yhä tärkeämpi osa potilasturvallisuutta.

Jos jonkun tietoturvaohjeen noudattaminen ei vaikuta järkevältä tai kyseisessä työtehtävässä mahdolliselta, niin ohjeistuksesta poikkeamisesta tulee keskustella tietoturvayksikön kanssa.

Tietoturvasta onkin tullut tärkeä osa potilasturvallisuuden kokonaisuutta, jossa lääketieteellinen osaaminen ei enää yksin riitä. Erityisen tärkeää on varmistaa monien erilaisten tukiprosessien tietoturvallisuus.

Lääkinnällisten laitteiden kyberturvallisuus

Verkkoon kytketyt lääkinnälliset laitteet ovat uudenlainen uhka potilasturvallisuudelle. Tietoverkkoihin kytkettyihin lääkinnällisiin laitteisiin voi levitä erilaisia haittaohjelmia myös muista verkon laitteista. Tästä on esimerkkinä vuonna 2017 myös terveydenhuollon sektorilla maailmalla vahinkoja aiheuttanut WannaCry-kiristyshaittaohjelma, joka johti myös Suomessa läheltä piti -tilanteisiin. Taustalla oli se, että kuvantamislaitteen toiminta sairaalan verkkoympäristössä oli liian heikosti suojattu ulkopuolisilta kyberuhkilta.

Lääkinnällisten laitteiden kyberuhkiin varautuminen ei kuitenkaan rajoitu vain sairaalan tietoverkoissa tehtäviin suojaustoimenpiteisiin. Kyberuhkat pitää huomioida myös laitteiden jokapäiväisessä käytössä. Laitteisiin voi tartuttaa viruksen huonolla kyberhygienialla, esimerkiksi käyttämällä varomattomasti USB-muistitikkuja eri laitteiden ja tietojärjestelmien välillä. Kun potilastyöhön käytetyn laitteen tai ohjelmiston tietoturva pettää käyttäjän huolimattomuuden vuoksi, se vaikuttaa usein myös suoraan potilasturvallisuuteen. Lääkinnällisten laitteiden tietoturva tarkoittaakin yhä enemmän niiden koko elinkaaren huomioimista, laitteiden hankinnasta käyttöönottoon, käyttöön ja lopulta käytöstä poistoon.

Lääkärin työssä voidaan parantaa

laitteiden ja järjestelmien turvallisuutta monin eri tavoin. Omaa arjen tietoturvaosaamista voi kehittää esimerkiksi Duodecim Oppiportin tietoturvakurssien avulla. Laite- tai järjestelmähankintoihin lääkärit taas saavat tietoturvaan liittyvää tukea oman organisaationsa tietoturva-asiantuntijoilta. Huolehtimalla laitteiden tietoturvasta jo hankintavaiheessa, voidaan niiden käytön aikaisen turvallisuuden tasosta pitää paremmin huolta. Tietoturvan kokonaisvaltainen toteuttaminen vaatiikin loppujen lopuksi koko terveydenhuollon organisaation yhteispeliä.

Tunnista kriittiset kohdat

Sairaalan toimintaympäristö on monimutkaistunut uusien tietojärjestelmien, laitteiden ja ohjelmistojen tultua osaksi potilastyötä. Järjestelmien ja laitteiden lisääntyessä on tärkeää ymmärtää, mitkä niistä ovat välttämättömiä hoidon onnistumisen kannalta. Lääkärin rooli korostuu, kun arvioidaan toimintojen ja tietojärjestelmien merkitystä. Jokaisen lääkärin tulee tunnistaa oman työnsä näkökulmasta ne kriittiset toiminnot ja tietojärjestelmät, jotka vaikuttavat potilaan hoidon onnistumiseen ja välittää tieto edelleen prosesseista ja tietojärjestelmistä vastaaville. Näin pystytään varautumaan ennalta tilanteisiin, joissa käytössä oleva toimintamalli tai tietojärjestelmä ei toimi.

> **Lääkärin on tärkeä tunnistaa oman toimintaympäristönsä kriittiset kohdat ja olla mukana luomassa varautumissuunnitelmia häiriötilanteiden varalta.**

Liian usein ajatellaan, että potilastietojärjestelmä on ainoa kriittinen osa potilastyötä ja että siitä vastaa järjestelmätoimittaja tai IT-palveluntuottaja. Potilastyössä jokin muu tietojärjestelmä tai laite voi kuitenkin olla samalla tavoin välttämätön potilasturvallisuuden ja hoitotyön onnistumisen näkökulmasta. Jos palveluntuottajalla ei ole ajantasaista tietoa siitä, miten tärkeä merkitys kyseisellä tietojärjestelmällä on kliinisen yksikön toimintaan, ei sen toimintavarmuuteen ole välttämättä kiinnitetty tarpeeksi huomiota. Häiriöt tällaisten järjestelmien toiminnassa voivat pahimmillaan aiheuttaa potilasturvallisuuteen liittyvien riskien toteutumisen.

Kriittisyyden arviointia tulee tehdä yhteistyössä muiden yksikössä työskentelevien kanssa. Kun moniammatillinen tiimi tarkastelee olemassa olevaa hoitoprosessia yhdessä, saattaa paljastua yllättäviä kohtia, joita muuttamalla voidaan tehostaa toimintaa ja saada lopputuloksena myös tietoturvallisempi toimintaympäristö. Arvioinnista kannattaa tehdä osa yksikön toimintaa ja tehdä se vähintään kerran vuodessa ja lisäksi aina silloin, kun toiminnassa tai toimintaympäristössä tapahtuu muutoksia. Tällaisia muutoksia voivat olla esimerkiksi uusien tietojärjestelmien, laitteiden tai tilojen hankinta- ja/tai käyttöönotto.

Lopuksi

Digitalisaatio muuttaa lääkärin työtä merkittävästi tehostaen toimintaa ja tuoden uudenlaisia lääkinnällisiä laitteita ja tietojärjestelmiä osaksi potilastyötä. Laitteiden ja järjestelmien ollessa enemmän kytköksissä tietoverkkoihin, nousee tietoturva yhä merkityksellisempään asemaan, jotta potilastyössä käytettävän tiedon luottamuksellisuus, eheys ja saatavuus voidaan turvata. Tämä vaatii uudenlaista osaamista niin lääkäriltä kuin organisaation tukiprosesseista vastaaviltakin. Lääkinnällisten laitteiden ja tietojärjestelmien hankintavaiheessa voidaan vaikuttaa niiden koko elinkaaren aikaiseen turvallisuuteen. Lääkärin on tärkeä tunnistaa oman toimintaympäristönsä kriittiset kohdat ja olla mukana luomassa varautumissuunnitelmia häiriötilanteiden varalta. Tietoturvallinen toiminta vaatii terveydenhuollon organisaatioissa yhteistyötä, jotta potilasturvallisuus voidaan varmistaa myös tietoturvariskien osalta.

Kirjallisuutta:

Ahuja A-S. (2019). The impact of artificial intelligencein medicine on the future role of the physician. Peerj. https://peerj.com/articles/7702/

Arun S & Khalid M. (2018). Protection of Healthcare information: Adding Cyber Resilience and Recovery. IEEE Conference Publications. IEEE Journal & Magazines. Doi: 10.1109/CSCI46756.2018.00033

Aysha A & Wael E-M. (2017). The Effects of Cyber-Security on Healthcare industry. IEEE Conference Publications. IEEE Journal & Magazines. Doi: 10.1109/IEEEGCC.2017.8448206

Cauševic A, Fotouhi H, Lundqvist K. (2017) Data Security and Privacy in Cyber-Physical Systems for Healthcare. John Wiley & Sons Ltd. https://doi.org/10.1002/9781119226079.ch15

ENISA. (2016). Cyber security and resilience for Smart Hospitals. Haettu osoitteesta https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

Helovuo A, Kinnunen M, Kuosmanen A., Peltomaa K. (2015). Potilasturvallisuus ja riskien hallinta – opas sosiaali- ja terveydenhuollon asiantuntijoille ja johdolle. Suomen Potilasturvallisuusyhdistys ry. ISBN 978-952-93-6301-8

Hummelholm A. (2019). E-Health Systems in Digital Environment. European Conference on Cyber Warfare and Security; Reading : 641-649,XIV. Reading: Academic Conferences International Limited.

Lääkärilehti (8.6.2017). WannaCry-haittaohjelmisto löytyi Tyksistä. (Keränen T.) Haettu osoitteesta https://www.laakarilehti.fi/ajassa/ajankohtaista/wannacry-haittaohjelma-loytyi-tyks-sta/