

**TERVEYDENHUOLLON  
TIETOTURVA JA  
KIRJAAMINEN**

Ari Puolakka

# Tietoturva

- Tarkoitetaan erilaisten järjestelmien, palvelujen sekä tietojen suojaamista.
- Tietoturvallisuus perustuu ja rakentuu kolmesta ominaisuudesta
  - luottamuksellisuuden
  - käytettävyyden
  - eheyden turvaamisesta.

# Tietoturva

- Tietoturvan merkitys painottuu aina, kun organisaatiolla tai yritykselle lisätään tietoverkkoon sovellus tai palvelu
- Tietoturva on aina jollakin tavalla uhattuna, mitä useampi sovellus tai palvelu toimii verkon kautta
- Julkinen verkko on sosiaali- ja terveysalalla tarkasti suojattu sekä valvottu, mutta se voi myös aiheuttaa tietoturva riskejä

# Haitta- ja vakoiluohjelmat

- Tarkoitetaan ohjelmia, jotka aiheuttavat tietojärjestelmissä negatiivisia tapahtumia
- Pääasiallisesti kyseessä olevat ohjelmat tulevat käyttäjän koneelle huomaamattomasti esimerkiksi toisena ohjelmana
- Haittaohjelmia torjutaan tietoturvaohjelmistoilla, tärkeimpinä viruksentorjuntaohjelmat sekä palomuurit
- Tietoturvaa parhaiten edistää ihminen omalla käytännöllään

# Haitta- ja vakoiluohjelmat

- Haittaohjelmat voivat tunkeutua tietokoneeseen pääasiassa viidellä eri tavalla
  - Sähköpostissa haittaohjelma voi olla saapuneissa liitetiedostoissa tai viestissä voi olla linkki Internet-sivulle, josta haittaohjelma latautuu tietokoneelle
  - Käyttöjärjestelmän aukkojen kautta voivat tulla erityisesti verkkomadot sekä muita ohjelmia, joiden tavoitteena on levittää itseään uusiin mahdollisiin kohteisiin

# Haitta- ja vakoiluohjelmat

- Internet-selaimen aukot: Haittaohjelma voi tulla tietokoneelle epämääräisiltä Internet-palveluilta esimerkiksi piraattiohjelmien levityspalvelimista.
- ActiveX-ohjelmat latautuvat Internet-sivuilta, eikä niitä tavallisesti osata varoa. Syynä tähän voi olla esimerkiksi se että ohjelmat ovat yleensä varustettu digitaalisella allekirjoituksella
- Muita kanavia haittaohjelmille ovat esimerkiksi kaupalliset hyötyohjelmat tai jopa tavallinen cd-äänilevy

# Haitta- ja vakoiluohjelmat

- Khalastelu (phishing) on myös yksi tietoturvauhka
  - pohjautuu käyttäjän huijaamiseen, jonka tarkoituksena on käyttäjän tietojen urkkiminen
  - haluttuja tietoja ovat mm. salasanat, käyttäjätunnukset, pin-koodit tai pankkitilin numerot
  - khalastelua yritetään yleensä sähköpostin tai väärennettyjen Internet-sivujen kautta

**Älä ikinä paina ok/yes, mikäli et ymmärrä kysymystä!**

# Sähköinen asiointi

- Tarkoitetaan tuotteen tai tiedon käsittelyä tietoverkossa
- Terveystieteidenhuollossa vuorovaikutteisia palveluja on kehitetty pääasiassa hoitotietojen jakamiseen tai välittämiseen eri hoitotahojen kesken sekä sähköiseen ajanvaraukseen
- Perusedellytyksenä sähköiselle asioinnille on asiakkaan ehdoton luottamus toimintaan
  - tiedon varmentaminen sekä korkealaatuinen tietoturva
- Mahdollistaa paljon riskejä, joita käyttäjän tulisi tietää ja ennen kaikkea osata ennaltaehkäistä



# Haittaohjelmien torjuminen

- Älä vastaa OK tai klikkaa yes, ellet tiedä mihin vastaat
- Älä lataa netistä ”turvaohjelmia”, jos et tiedä niiden todellista tarkoitusperää
- Varmista aina, että palomuuuri on toiminnassa
- Nettipalvelu, jossa on paljon kirjoitusvirheitä, ei ole luotettava
- Älä klikkaa saamiasi linkkejä esim. sähköpostissa
- Älä luota sokeasti viruksentorjunta- tai Spywareohjelmiin, omalla toiminnalla estät suurimmat uhat

# Terveydenhuollon tietotekninen osaaminen

- Tietoturvallisuutta ja sitä vaarantavia tekijöitä on tutkittu paljon. **Ihmisen toiminta, joko tahaton tai tahallinen, on isoin yksittäinen tietoturvallinen riski**
- Tietotekniikan käyttö vaikuttaa terveydenhuoltoon ja sen arvoihin ja täten vaikuttaa myös mm. potilaiden tasa-arvoon ja oikeudenmukaiseen kohteluun, itsenäisyyteen ja yksityisyyteen

# Terveydenhuollon kirjaaminen

- Tiedolla on merkittävä rooli potilaan hoidon toteuttamisessa sekä järjestämisessä
- Kirjaamisessa keskeistä on selkeä ilmaisu mitä on tehty, ketkä ovat olleet läsnä ja miten potilas reagoi tai millainen vointi potilaalla on
- Hoidon tuottajat ovat velvoitettu ylläpitämään potilasasiakirjoja

# Terveydenhuollon kirjaaminen

- Potilasasiakirja kertoo potilaan hoidon toteuttamisessa tai järjestämisessä, muualta saapuvia asiakirjoja tai tallenteita, jotka koskevat potilaan henkilökohtaisia ja terveydentilaan liittyviä tietoja
  - Potilasasiakirjaan kuuluvat ensisijaisesti potilaskertomus sekä potilaan mahdolliset lähetteet

# Terveydenhuollon kirjaaminen

- Potilaskertomus pitää sisällään tiedon potilaan kotihoito- ja avohoitokäynneistä sekä mahdollisista osastohoitojaksoista, joissa näkyy hoitoon osallistuneiden eri ammattiryhmien kirjatut tiedot
- Potilaskertomus elektronisessa muodossa nojaa vahvasti rakenteelliseen tietoon.
  - Elektroninen potilaskertomus näkyy käyttäjille erilaisina näkyminä, joille tietoa voidaan kirjata eri vaiheissa otsikoita käyttämällä

# Terveydenhuollon kirjaaminen

- Hoitokertomuksella tarkoitetaan eri ammattiryhmien sekä hoitohenkilökunnan yhteisesti laatimaa potilaskertomuksen osaa, joka sisältää potilaan hoidon arvioinnin, suunnittelun, seurannan sekä toteutuksen

**On oleellista muistaa, että mikä on kirjattu, on tehty mutta mitä ei ole kirjattu, ei ole myöskään tehty**

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Sähköisestä asioinnista säädetään lailla sähköisestä asioinnista viranomaistoiminnassa
  - ”.. lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa, tuomioistuimissa ja muissa lainkäyttöelimissä sekä ulosotossa edistämällä sähköisten tiedonsiirtomenetelmien käyttöä..” (SähkAsL 2003, 1§.)

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Laissa sähköisestä asioinnista viranomaistoiminnassa sähköisellä tiedonsiirtomenetelmällä tarkoitetaan
  - *”telekopiota ja telepalvelua, kuten sähköistä lomaketta, sähköpostia tai käyttöoikeutta sähköiseen tietojärjestelmään, sekä muuta sähköiseen tekniikkaan perustuvaa menetelmää, jossa tieto välittyy langatonta siirtotietä tai kaapelia pitkin; ei kuitenkaan puhelua.”*  
(SähkAsL 2003, 4§.)



# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Luvussa 2 käsitellään viranomaisen velvollisuuksia
  - *”Viranomaisen on pyrittävä käyttämään asiakkaan kannalta teknisesti mahdollisimman yhteensopivia ja helppokäyttöisiä laitteistoja ja ohjelmistoja. Viranomaisen on lisäksi varmistettava riittävä tietoturvallisuus asioinnissa ja viranomaisten keskinäisessä tietojenvaihdossa.”* (SähköAsL 2003, 5§.)
- Luvussa viisi käsitellään muun muassa sähköisen asiakirjan arkistointia
  - *”Sähköinen asiakirja on arkistoitava siten, että sen alkuperäisyys ja säilyminen sisällöltään muuttumattomana voidaan myöhemmin osoittaa.”* (SähköAsL 2003, 21§.)

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Vuonna 2009 laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista korvasi vuonna 2003 säädetyn lain sähköisestä allekirjoituksesta
  - *”..laissa säädetään vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista sekä niihin liittyvien palveluiden tarjoamisesta niitä käyttäville palveluntarjoajille ja yleisölle.”* (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 1§.)

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Sähköisellä allekirjoituksella tarkoitetaan
  - ”..sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä” <sup>17</sup> (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 2§.)

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Kehittyneellä sähköisellä allekirjoituksella tarkoitetaan
  - *”..sähköistä allekirjoitusta:*
    - a) joka liittyy yksiselitteisesti sen allekirjoittajaan;*
    - b) jolla voidaan yksilöidä allekirjoittaja;*
    - c) joka on luotu menetelmällä, jonka allekirjoittaja voi pitää yksinomaisessa valvonnassaan; ja*
    - d) joka on liitetty muuhun sähköiseen tietoon siten, että tiedon mahdolliset muutokset voidaan havaita”* 17 (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 2§.)

# Sähköisestä asioinnista ja sähköisestä allekirjoituksesta

- Sähköisellä allekirjoituksella laaditun tekstin alkuperäisyys sekä allekirjoittaja varmistetaan
- Allekirjoitettaviin asiakirjoihin terveydenhuollossa kuuluvat loppulausunnot, lääkemääräykset sekä erilaiset todistukset
- Sähköinen asiakirja on voimassa kolmesta viiteen vuotta
- Potilasasiakirjojen muuttamattomuus on kuitenkin pystyttävä vahvistamaan vähintään kymmenen vuotta, mikä on asiakirjojen valitusaika

# Salassapidosta ja tietojen suojaamisesta

- Asiakirjasalaisuus ja vaitiolovelvollisuus liittyvät toisiinsa. Laissa viranomaisten toiminnan julkisuudesta luvussa 6 käsitellään salassapitovelvoitteita
- Näitä noudatetaan terveydenhuollossa siltä osin kuin asiasta ei ole erityissäännöksiä terveydenhuollon lainsäädännössä

# Salassapidosta ja tietojen suojaamisesta

- *”Viranomaisen asiakirja on pidettävä salassa, jos se tässä tai muussa laissa on säädetty salassa pidettäväksi tai jos viranomainen lain nojalla on määrännyt sen salassa pidettäväksi taikka jos se sisältää tietoja, joista on lailla säädetty vaitiolovelvollisuus. Salassa pidettävää viranomaisen asiakirjaa tai sen kopiota tai tulostetta siitä ei saa näyttää eikä luovuttaa sivulliselle eikä antaa sitä teknisen käyttöyhteyden avulla tai muulla tavalla sivullisen nähtäväksi tai käytettäväksi.”*  
(Julkl 1999, 22§.)

# Salassapidosta ja tietojen suojaamisesta

- *”Viranomaisen palveluksessa oleva samoin kuin luottamustehtävää hoitava ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutenkaan viranomaisessa toimiessaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saa paljastaa senkään jälkeen, kun toiminta viranomaisessa tai tehtävän hoitaminen viranomaisen lukuun on päättynyt...” (Julkl 1999, 23§.)*



# Salassapidosta ja tietojen suojaamisesta

- Laissa potilaan asemasta ja oikeuksista 13§:ssä potilasasiakirjojen salassapidosta määrätään mm. seuraavaa
  - *”Terveystieteiden ammattihenkilö tai muu terveydenhuollon toimintayksikössä työskentelevä taikka sen tehtäviä suorittava henkilö ei saa ilman potilaan kirjallista suostumusta antaa sivulliselle potilasasiakirjoihin sisältyviä tietoja.. Salassapitovelvollisuus säilyy palvelussuhteen tai tehtävän päättymisen jälkeen.”* (PotL 1992, 13§.)

# Salassapidosta ja tietojen suojaamisesta

- Tietojen suojaamisesta säädetään esimerkiksi henkilötietolaissa muun muassa seuraavalla tavalla
  - *”..lain tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista.”*  
(HetiL 1999, 1§.)

# Salassapidosta ja tietojen suojaamisesta

- Myös laissa viranomaisten toiminnan julkisuudesta säädetään tietojen suojaamisesta.
  - *”Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä”* (Julkl 1999, 18§.)

# Salassapidosta ja tietojen suojaamisesta

- Tekniset ja organisaatioon liittyvät määräykset antaa työnantajan eli rekisterinpitäjän ylin johto
- Johdon tulee esimerkiksi
  - kouluttaa työntekijät tietosuojassa ja henkilötietojen käsittelyssä,
  - antaa työntekijälle käyttöoikeudet tarpeellisiin potilasrekisteritietoihin
  - poistaa käyttöoikeudet
  - antaa jokaiselle työntekijälle oma käyttäjätunnus ja salasana
- Tietojen käsittelyä pitäisi pystyä seuraamaan, kuten kuka on käsitellyt mitään tietoa
- Tietokoneessa pitäisi olla erittäin tehokas suojaus, mikäli tietokoneella on potilastietojen lisäksi Internet-yhteys

# Potilasasiakirjojen laatimisesta ja säilyttämisestä

- Sosiaali- ja terveysministeriön asetus potilasasiakirjoista on annettu 30.3.2009
  - *”..asetusta sovelletaan potilaan hoidon järjestämisessä ja toteuttamisessa käytettävien asiakirjojen laatimiseen sekä niiden ja muun hoitoon liittyvän materiaalin säilyttämiseen”* (PotasiakA 2009, 1§.)

# Potilasasiakirjojen laatimisesta ja säilyttämisestä

- Asetuksessa käydään läpi yleisistä periaatteista ja vaatimuksista mm. seuraavaa
  - *”Potilasasiakirjat tulee laatia ja säilyttää sellaisia välineitä ja menetelmiä käyttäen, että asiakirjoihin sisältyvien tietojen eheys ja käytettävyys voidaan turvata tietojen säilytysaikana”.* (PotasiakA 2009, 4§.)
  - *”Potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvat saavat käsitellä potilasasiakirjoja vain siinä laajuudessa kuin heidän työtehtävänsä ja vastuunsa sitä edellyttävät..”* (PotasiakA 2009, 4§.)

# Potilasasiakirjojen laatimisesta ja säilyttämisestä

- Asetus määrittelee myös esimerkiksi kuka saa tehdä merkintöjä potilasasiakirjoihin ja mitä potilasasiakirjoihin tulee merkitä
  - *”Potilasasiakirjoihin saavat tehdä merkintöjä potilaan hoitoon osallistuvat terveydenhuollon ammattihenkilöt ja heidän ohjeidensa mukaisesti myös muut henkilöt siltä osin kuin he osallistuvat hoitoon. Potilaan hoitoon osallistuvat terveydenhuollon opiskelijat saavat tehdä merkintöjä toimiessaan laillistetun ammattihenkilön tehtävässä.. ”* (PotasiakA 2009, 6§.)

# Potilasasiakirjojen laatimisesta ja säilyttämisestä

- Asetuksen 22§ käsittelee potilasasiakirjojen säilytystä.
  - *”Potilasasiakirjojen ja hoitoon liittyvän muun materiaalin säilyttämisestä vastaa se terveydenhuollon toimintayksikkö tai itsenäisesti ammattiaan harjoittava terveydenhuollon ammattihenkilö, jonka toiminnassa ne ovat syntyneet, jollei sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä annetusta laista muuta johdu..”* <sup>23</sup> (PotasiakA 2009, 22§.)



# Potilasasiakirjojen laatimisesta ja säilyttämisestä

- Potilasasiakirjat tulee laatia salassapitosäädökset huomioiden sekä henkilötietolaissa säädettyjen suunnittelu-, suojaamis- ja huolellisuusvelvoitteiden mukaisesti ja laissa viranomaisten toiminnan julkisuudesta säännökset huomioiden.
- Potilasasiakirjojen tulee olla tarkoituksen mukaisia huomioiden potilaan neuvonta, hoito ja niiden jatkuvuus.
- Potilastiedot ovat yksityisyydensuojan ydinaluetta