# TERVEYDENHUOLLON TIETOTURVA & KIRJAAMINEN

Ari Puolakka

# SISÄLLYS

# TIETOTURVA

Tietoturvalla tarkoitetaan erilaisten järjestelmien, palvelujen sekä tietojen suojaamista. Tietoturvallisuus perustuu ja rakentuu kolmesta ominaisuudesta - luottamuksellisuuden, käytettävyyden sekä eheyden turvaamisesta. [1]

*Luottamuksellisuus* tarkoittaa tietojärjestelmän tietojen olevan käytettävissä vain niille oikeutetuilla henkilöillä. Luottamuksellisuutta pyritään organisaatioissa ylläpitämään tietojärjestelmien ja sisäisten verkkojen salasanoilla, jotka usein ovat sidottuja myös henkilökohtaisiin salasanoihin. [2]

*Käytettävyydellä* tarkoitetaan tietojen saatavuutta oikeassa muodossa ja riittävän nopeasti. Tieto- ja tietoliikennejärjestelmien tulee olla tarpeeksi tehokkaita ja ohjelmistojen tulee sopia tallennettujen tietojen käsittelyyn. Käyttäjän tulisi myös saada tarvitsemansa tiedot hänelle sopivana tiedostomuotona. [2]

*Eheydellä* tarkoitetaan tietojärjestelmien sisältävien tietojen paikkansa pitävyyttä, jolloin tieto ei sisällä tahattomia tai tahallisia virheitä. Eheyttä ylläpidetään pääasiallisesti erilaisilla ohjelmointi ratkaisuilla. Tietojärjestelmän sovelluksiin voidaan ohjelmoida erilaisia tarkistuksia. Tietoliikenne sovelluksiin on paljon käytössä erilaisia protokollia sekä laitteita, jotka sisältävät erilaisia ohjelmia korjaus- ja virheentunnistusta varten. [2]

*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. Verkon kautta tulevien hyökkäyksien määrä on kasvanut erilaisten virusten sekä haitta sekä vakoiluohjelmien takia.[3] Terveydenhuollossa on käytössä pääasiassa julkinen verkkoyhteys, joka ajoittain hidastaa isoja tiedon siirtoja, kuten röntgenkuvien lähetystä. Julkinen verkko on toki sosiaali- ja terveysalalla tarkasti suojattu sekä valvottu, mutta se voi myös aiheuttaa tietoturva riskejä.[4]

## Haitta- ja vakoiluohjelmat

Haitta- sekä vakoiluohjelmilla tarkoitetaan ohjelmia, jotka aiheuttavat tietojärjestelmissä negatiivisia tapahtumia. Pääasiallisesti kyseessä olevat ohjelmat tulevat käyttäjän koneelle huomaamattomasti esimerkiksi toisena ohjelmana.[5] Haittaohjelmia torjutaan tietoturvaohjelmistoilla, tärkeimpinä viruksentorjuntaohjelmat sekä palomuurit.[6] Täytyy kuitenkin muistaa, että tekniset apuvälineet ovat ainoastaan apuvälineitä, tietoturvaa parhaiten edistää ihminen omalla käytännöllään [3]

Haittaohjelmat voivat tunkeutua tietokoneeseen pääasiassa viidellä eri tavalla, sähköpostin, käyttöjärjestelmän aukkojen, selaimen aukkojen, ActiveX-ohjelmien sekä muiden kanavien kautta.[7]

*Sähköpostissa* haittaohjelma voi olla saapuneissa liitetiedostoissa tai viestissä voi olla linkki Internet-sivulle, josta haittaohjelma latautuu tietokoneelle.[7]

*Käyttöjärjestelmän aukkojen* kautta voivat tulla erityisesti verkkomadot sekä muita ohjelmia, joiden tavoitteena on levittää itseään uusiin mahdollisiin kohteisiin. [7]

*Internet-selaimen aukot* ovat saattavat olla jopa vaarallisin kanava haittaohjelmille, edes käyttäjän omalla varovaisuudella ei voida poistaa kaikkia haittaohjelmariskejä. Haittaohjelma voi tulla tietokoneelle epämääräisiltä Internet-palveluilta esimerkiksi piraattiohjelmien levityspalvelimista. [7]

*ActiveX-ohjelmat* latautuvat Internet-sivuilta, eikä niitä tavallisesti osata varoa. Syynä tähän voi olla esimerkiksi se että ohjelmat ovat yleensä varustettu digitaalisella allekirjoituksella. Allekirjoitus ei kuitenkaan kerro muuta kuin ohjelman alkuperän ja takaa muuttumattomuuden.[7]

*Muita kanavia* haittaohjelmille ovat esimerkiksi kaupalliset hyötyohjelmat tai jopa tavallinen cd-äänilevy. [7]

*Khalastelu (phishing)* on myös yksi tietoturvauhka. Khalastelu 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. [7]

**Huomaa! Älä ikinä paina ok/yes, mikäli et ymmärrä kysymystä![7]**

# Sähköinen asiointi

Sähköisellä asioinnilla tarkoitetaan tuotteen tai tiedon käsittelyä tietoverkossa.[8] Sähköinen asiointi terveydenhuollossa on keskittynyt ammattiryhmien tietojen hakuun tai tietojen tarkastamiseen. [9]

Terveydenhuollossa vuorovaikutteisia palveluja on kehitetty pääasiallisesti hoitotietojen jakamiseen tai välittämiseen eri hoitotahojen kesken sekä sähköiseen ajanvaraukseen. Sähköisestä asioinnista onkin muodostunut keskeinen asia terveydenhuollon palveluita tarvitseville potilaille sekä asiakkaille.[9]

Perusedellytyksenä sähköiselle asioinnille on asiakkaan ehdoton luottamus toimintaan, joka korostuu tiedon varmentamisella sekä korkealaatuisella tietoturvalla. Sähköinen asiointi myös mahdollistaa paljon riskejä, joita käyttäjän tulisi tietää ja ennen kaikkea osata ennaltaehkäistä.[4]

## Haittaohjelmien torjuminen

1. Älä vastaa OK tai klikkaa yes, ellet tiedä mihin vastaat

2. Älä lataa netistä ”turvaohjelmia”, jos et tiedä niiden todellista tarkoitusperää

3. Varmista aina, että palomuuri on toiminnassa

4. Nettipalvelu, jossa on paljon kirjoitusvirheitä, ei ole luotettava

5. Älä klikkaa saamiasi linkkejä esim. sähköpostissa

6. Älä luota sokeasti viruksentorjunta- tai Spywareohjelmiin, omalla toiminnalla estät suurimmat uhat [7]

# TERVEYDENHUOLLON TIETOTEKNINEN OSAAMINEN

Terveydenhuollon eri tahot, erityisesti hoitohenkilökunta on elektronisen potilastietojärjestelmän tultua käyttöön velvoitettu oppimaan paljon uutta. [10] Tietotekniikan käyttö vaikuttaa terveydenhuoltoon ja sen arvoihin ja täten vaikuttaa myös mm. potilaiden tasa-arvoon ja oikeudenmukaiseen kohteluun, itsenäisyyteen ja yksityisyyteen. [11]

Tietoturvallisuutta ja sitä vaarantavia tekijöitä on tutkittu paljon. **Ihmisen toiminta, joko tahaton tai tahallinen, on isoin yksittäinen tietoturvallinen riski**.[12] Työasemien käytön turvallisuus koostuu käyttäjän motivaatiosta sekä käyttäjän osaamisesta. Käyttäjän tulisi saada tarvittaessa riittävää ohjeistusta sekä koulutusta sovellusten ja työaseman käyttöön. [2]

Tero Tammisalon kirjoittamassa raportissa (Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi, STAKES) ilmenee kuinka tietoturvan toteutumisen riskinä ovat henkilöstön asenteet ja tietoturvan merkityksen ymmärtäminen sekä henkilöstön osaaminen. Tämän vuoksi henkilöstön kouluttaminen on oleellista tietoturvallisuuden hoidon ja kehittämisen kannalta. Henkilöstön lisäksi myös johto ja tietoturvaryhmä tarvitsevat koulutusta. [12]

# TERVEYDENHUOLLON KIRJAAMINEN

Tiedolla on merkittävä rooli potilaan hoidon toteuttamisessa sekä järjestämisessä. Terveydenhuollossa potilastietojen hallinta ja käsittely on tullut laajaksi järjestelmäksi, johon kuuluvat olennaisesti erilaisten tietojen tuottaminen, säilyttäminen, sekä eri menettelytavat ja ihmiset toimijoina. [13]

Kirjaamisessa keskeistä on selkeä ilmaisu mitä on tehty, ketkä ovat olleet läsnä ja miten potilas reagoi tai millainen vointi potilaalla on. Hoitoon liittyvät tapahtumat tarkistetaan yleensä jälkikäteen, mikä voi tapahtua esimerkiksi itse potilaan, hänen läheistensä tai potilasvahinkolautakunnan aloitteesta. [14]

Suomessa hoitotyön kirjaamisen mallina on käytetty Maailman terveysjärjestön (WHO) päätöksenteon prosessimallia. Maailman terveysjärjestön prosessimalli voidaan eritellä kolmesta kuuteen vaiheeseen huomioiden toimintaympäristön. [13]

Hoitotyön prosessiin kuuluu hoitotyön suunnitelma, toteutus, arviointi ja yhteenveto. Hoitotyössä ydintietoihin kuuluvat ”hoidon tarve”, ”hoitotyön toiminnot”, ”hoidon tulokset” sekä ”hoitotyön yhteenveto”. Kirjaaminen eri hoitoprosessin vaiheissa voidaan tehdä pelkästään vapaamuotoisella tekstillä tai luokitusta käyttäen ja sitä täydentäen. [15]

Hoidon tuottajat ovat velvoitettu ylläpitämään potilasasiakirjoja. Hoidon tuottajia ovat esimerkiksi sairaanhoitopiirit, terveyskeskukset tai yksityiset terveyspalvelujen tuottajat. Potilaslaissa on määritelty, että potilaskohtaiset merkinnät eri tapahtumista tulee tehdä asiakirjoihin. [13]

*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. Lähetteitä voivat olla mm. erilaiset lausunnot eri ammattiryhmiltä, röntgen – tai laboratorio ja muut tutkimusasiakirjat.[13]

*Potilaskertomus* pitää sisällään tiedon potilaan kotihoito- ja avohoitokäynneistä sekä mahdollisista osastohoitojaksoista, joissa näkyy hoitoon osallistuneiden eri ammattiryhmien kirjatut tiedot. Potilaskertomuksesta täten muodostuu kronologisesti etenevä asiakirja. [13]

*Potilaskertomus elektronisessa muodossa* nojaa vahvasti rakenteelliseen tietoon. Elektroninen potilaskertomus näkyy käyttäjille erilaisina näkyminä, joille tietoa voidaan kirjata eri vaiheissa otsikoita käyttämällä. Otsikoita käyttämällä hoitoalalla voidaan tuottaa tietoa eri ammattiryhmien välillä nopeammin sekä reaaliaikaisemmin. [13]

*Hoitokertomuksella* tarkoitetaan eri ammattiryhmien sekä hoitohenkilökunnan yhteisesti laatimaa potilaskertomuksen osaa, joka sisältää potilaan hoidon arvioinnin, suunnittelun, seurannan sekä toteutuksen. Hoitokertomus on käytössä paljon potilailla, joiden hoito vaatii monen eri ammattiryhmän asiantuntijuutta sekä tietoa.[13]

**On oleellista muistaa, että mikä on kirjattu, on tehty mutta mitä ei ole kirjattu, ei ole myöskään tehty.** [14]

# TIETOTURVAAN LIITTYVIÄ JA KIRJAAMISTA OHJAAVIA SÄÄDÖKSIÄ

## 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. Laissa säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa."* 16 (SähkAsL 2003, 1§.)

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."* 16 (SähkAsL 2003, 4§.)

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.”* 16 (SähkAsL 2003, 5§.)

Laissa sähköisestä asioinnista viranomaistoiminnassa luku 3 käsittelee sähköisen viestin lähettämistä muun muassa seuraavalla tavalla.

> *”Viranomaiselle saapunutta sähköistä asiakirjaa ei tarvitse täydentää allekirjoituksella, jos asiakirjassa on tiedot lähettäjästä eikä asiakirjan alkuperäisyyttä tai eheyttä ole syytä epäillä"* 16 (SähkAsL 2003, 9§.)

Luvussa viisi käsitellään muun muassa sähköisen asiakirjan arkistointia.

> *”Sähköinen asiakirja on arkistoitava siten, että sen alkuperäisyys ja säilyminen sisällöltään muuttumattomana voidaan myöhemmin osoittaa.”* 16 (SähkAsL 2003, 21§.)

> *” Arkistolaitos antaa tarkempia määräyksiä ja ohjeita sähköisen asioinnin kirjaamisesta tai muusta rekisteröinnistä sekä arkistoinnista. Valtiovarainministeriö antaa ohjeita ja suosituksia sähköisen asioinnin yhteentoimivuuden ja tietoturvallisuuden varmistamisesta sekä sähköisten asiointipalvelujen järjestämisestä.”* 16(SähkAsL 2003, 22§.)

Asioiden hoitamiseen on ennen käytetty puhelinta, nykyään kuitenkin asiointia tapahtuu myös Internetin ja sähköpostin kautta. [9] Tiedon varmentaminen ja tietoturva ovat oleellisia, jotta luottamus sähköiseen asiointiin on mahdollista. [4]

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."* [17] (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 1§.)

Laki käsittelee luvussa 4 sähköistä allekirjoitusta. Sähköisellä allekirjoituksella tarkoitetaan

> *"..sähköisessä muodossa olevaa tietoa, joka on liitetty tai joka loogisesti liittyy muuhun sähköiseen tietoon ja jota käytetään allekirjoittajan henkilöllisyyden todentamisen välineenä"* [17] (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 2§.)

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 allekirjoituksesta säädetään myös seuraavaa:

*”Turvallisen allekirjoituksen luomisvälineen on riittävän luotettavasti varmistettava, että:*

*1) allekirjoituksen luomistiedot ovat käytännössä ainutkertaisia ja että ne säilyvät luottamuksellisina;*

*2) allekirjoituksen luomistietoja ei voida päätellä muista tiedoista;*

*3) allekirjoitus on suojattu väärentämiseltä;*

*4) allekirjoittaja voi suojata allekirjoituksen luomistiedot muiden käytöltä; sekä*

*5) luomisväline ei muuta allekirjoitettavia tietoja eikä estä tietojen esittämistä allekirjoittajalle ennen allekirjoittamista.”* 17 (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 28§.)

*”Allekirjoittaja vastaa laatuvarmenteella varmennetun kehittyneen sähköisen allekirjoituksen luomistietojen oikeudettomasta käytöstä aiheutuneesta vahingosta..*

> *Kuluttajalla on kuitenkin 1 momentissa säädetty vastuu vain, jos:*
>
> *1) hän on luovuttanut luomistiedot toiselle;*
>
> *2) luomistietojen joutuminen niiden käyttöön oikeudettomalle on aiheutunut hänen huolimattomuudestaan, joka ei ole lievää; tai*
>
> *3) hän menetettyään luomistietojen hallinnan muulla kuin 2 kohdassa mainitulla tavalla on laiminlyönyt pyytää laatuvarmenteen peruuttamista..”* [17] (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 2009, 40§.)

Sähköisellä allekirjoituksella laaditun tekstin alkuperäisyys sekä allekirjoittaja varmistetaan. Tekstissä allekirjoitukseen on mahdollista liittää aikaleimapalvelulla tarkka ajan kohta. Allekirjoitettaviin asiakirjoihin terveydenhuollossa kuuluvat loppulausunnot, lääkemääräykset sekä erilaiset todistukset. Suomessa viranomaistahot määräävät milloin ja kenen aloitteesta sähköiset asiakirjat tulee allekirjoittaa. Sähköinen asiakirja on voimassa kolmesta viiteen vuotta. Potilasasiakirjojen muuttamattomuus on kuitenkin pystyttävä vahvistamaan vähintään kymmenen vuotta, mikä on asiakirjojen valitusaika. [18]

## 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. [22]

> *”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.”* [19] (JulkL 1999, 22§.)

> *”Viranomaisen palveluksessa oleva samoin kuin luottamustehtävää hoitava ei saa paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan 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. .. koskee myös sitä, joka harjoittelijana tai muutoin toimii viranomaisessa taikka viranomaisen toimeksiannosta tai toimeksiantotehtävää hoitavan palveluksessa taikka joka on saanut salassa pidettäviä tietoja lain tai lain perusteella annetun luvan nojalla, jollei laista tai sen perusteella annetusta luvasta muuta johdu.”* [19] (JulkL 1999, 23§.)

Laissa potilaan asemasta ja oikeuksista 13§: ssä potilasasiakirjojen salassapidosta määrätään mm. seuraavaa.

> *”Terveydenhuollon 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.”* [20] (PotL 1992, 13§.)

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.”* [21] (HetiL 1999, 1§.)

> *”Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.”* [21] (HetiL 1999, 23§.)

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”* [19] (JulkL 1999, 18§.)

Tekniset ja organisaatioon liittyvät määräykset antaa työnantajan eli rekisterinpitäjän ylin johto. Johdon tulee esimerkiksi kouluttaa työntekijät tietosuoja-asioissa ja henkilötietojen käsittelyssä, antaa työntekijälle käyttöoikeudet tarpeellisiin potilasrekisteritietoihin, poistaa käyttöoikeudet sekä antaa jokaiselle työntekijälle oma käyttäjätunnus ja salasana. Tietojen käsittelyä pitäisi pystyä seuraamaan, kuten kuka on käsitellyt mitäkin tietoja. Lisäksi tietokoneessa pitäisi olla erittäin tehokas suojaus, mikäli tietokoneella on potilastietojen lisäksi Internet-yhteys. [22]

## 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"* 23 (PotasiakA 2009, 1§.)

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, 3§.) *"Potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvat saavat käsitellä potilasasiakirjoja vain siinä laajuudessa kuin heidän työtehtävänsä ja vastuunsa sitä edellyttävät.. Sähköisten potilastietojärjestelmien käyttäjä tulee yksilöidä ja tunnistaa siten, että käyttäjä todennetaan yksiselitteisesti."* 23 (PotasiakA 2009, 4§.)

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.. Muutoin terveydenhuollon opiskelijan tekemät merkinnät hyväksyy hänen esimiehensä, ohjaajansa tai tämän valtuuttama henkilö. .. Terveydenhuollon ammattihenkilö vastaa sanelunsa perusteella tehdyistä potilasasiakirjamerkinnöistä.” 23* (PotasiakA 2009, 6§.)

*”Potilasasiakirjoihin tulee merkitä potilaan hyvän hoidon järjestämisen, suunnittelun, toteuttamisen ja seurannan turvaamiseksi tarpeelliset sekä laajuudeltaan riittävät tiedot. Merkintöjen tulee olla selkeitä ja ymmärrettäviä ja niitä tehtäessä saa käyttää vain yleisesti tunnettuja ja hyväksyttyjä käsitteitä ja lyhenteitä. Potilasasiakirjamerkinnöistä tulee ilmetä tietojen lähde, jos tieto ei perustu ammattihenkilön omiin tutkimushavaintoihin tai jos potilasasiakirjoihin merkitään muita kuin potilasta itseään koskevia tietoja. .. Niissä lausunnoissa ja todistuksissa, jotka laaditaan esitettäväksi muulle organisaatiolle tai taholle, tulee olla asiakirjan laatijan allekirjoitus.” 23* (PotasiakA 2009, 7§.)

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..”* [23] (PotasiakA 2009, 22§.)

Potilasasiakirjat tulee laatia salassapitosäädökset huomioiden sekä henkilötietolaissa säädettyjen suunnittelu-, suojaamis- ja huolellisuusvelvoitteiden mukaisesti ja laissa viranomaisten toiminnan julkisuudesta säännökset huomioiden. Potilasasiakirjat on mahdollista laatia manuaalisesti tai tekniikan avulla. Potilasasiakirjojen tulee olla tarkoituksen mukaisia huomioiden potilaan neuvonta, hoito ja niiden jatkuvuus. Potilastiedot ovat yksityisyydensuojan ydinaluetta. [22]

# Lähteet


1 Viestintävirasto 2009. Palvelut aiheittain. Tietoturva ja -suoja. Tietoturvalliseen yhteiskuntaan. Osoitteessa
http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html. 16.9.2009.

2 Hakala, M. – Vainio, M. – Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

3 Hämeen- Anttila, T. 2003. Tietoliikenteen perusteet. Jyväskylä: Docendo Finland Oy.

4 Tietoyhteiskuntaneuvosto 2005. Tulevaisuuden verkottuva Suomi. Tietoyhteiskuntaneuvoston raportti. Helmikuu 2005. Valtioneuvoston kanslia. Osoitteessa
http://www.tietoyhteiskuntaohjelma.fi/tietoyhteiskuntaneuvosto/fi_FI/kokousmateriaali/index.html.

5 Mäkinen, O. 2006. Internet ja etiikka. Helsinki: BTJ kirjastopalvelu Oy.

6. Tietoturvaopas 2008. Uhat ja niiden torjunta. Haitoilta suojautuminen. Miten haittaohjelmilta suojaudutaan? Osoitteessa
http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haitoiltasuojautuminen.html. 12.11.2008.

7 Järvinen, P. 2006. Paranna tietoturvaasi. Jyväskylä: Docendo Finland Oy.

8 Kansallisarkisto 2005. Sähköinen asiointipalvelu – toimenpiteet ja kulku asiakirjahallinnon näkökulmasta. Arkistolaitos. Osoitteessa http://www.narc.fi/asiointikaavio/. 8.2.2005.

9 Saranto, K. 2007. Sähköinen asiointi terveydenhuollossa. – Teoksessa Hoitotietojen systemaattinen kirjaaminen (Saranto, K. – Ensio, A. – Tanttu, K. – Sonninen, A.L.), 232–240. Helsinki: WSOY.

10 Ensio, Anneli 2007. Tavoitteena toiminnan ja palvelujen kehittäminen. – Teoksessa Hoitotietojen systemaattinen kirjaaminen (Saranto, K. – Ensio, A. – Tanttu, K. – Sonninen, A.L.), 149–165. Helsinki: WSOY.

11 Hautala, L. – Seiko-Vänttinen, M. – Salanterä, S. 2001. Eettisiä pohdintoja hoitotyön tietotekniikasta. Sairaanhoitaja 7 vol. 74, 22–24.

12 Tammisalo, T. 2007. Sosiaali- ja terveydenhuollon organisaatioiden tietoturvan hallinnointi. Stakesin raportteja 5/2007.

13 Saranto, K. – Sonninen, A.L. 2007 Systemaattisen kirjaamisen tarve. – Teoksessa Hoitotietojen systemaattinen kirjaaminen (Saranto, K. – Ensio, A. – Tanttu, K. – Sonninen, A.L.), 12–16. Helsinki: WSOY.

14 Hallila, L. – Graeffe, R. 2005 Hoitotyön kirjaamista sääntelevät lait, asetukset ja ohjeet. – Teoksessa Näyttöön perustuva hoitotyön kirjaaminen (toim. Hallila, L.), 16- 22. Helsinki: Kustannusosakeyhtiö Tammi.

15 Tanttu, K. – Ikonen, H. 2007. Ydintietojen käyttö hoitokertomuksessa – Teoksessa Hoitotietojen systemaattinen kirjaaminen (Saranto, K. – Ensio, A. – Tanttu, K. – Sonninen, A.L.), 209–212. Helsinki: WSOY.

16 SähkAsL 2003. Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13. Valtion Säädöstietopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/2003/20030013. 15.9.2010.

17 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617. Valtion säädöstiedostopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/2009/20090617. 15.9.2010.

18 Ensio, Antero 2007. Potilaskertomuksen tietoturvaratkaisut. – Teoksessa Hoitotietojen systemaattinen kirjaaminen (Saranto, K. – Ensio, A. – Tanttu, K. – Sonninen, A.L.), 134–142. Helsinki: WSOY.

19 JulkL 1999. Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621. Valtion Säädöstietopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990621. 15.9.2010.

20 PotL 1992. Laki potilaan asemasta ja oikeuksista 17.8.1992/785. Valtion Säädöstietopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1992/19920785. 15.9.2010.

21 HetiL 1999. Henkilötietolaki 22.4.1999/523. Valtion Säädöstietopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. 5.10.2010.

22 Ylipartanen, A. 2001. Tietosuoja terveydenhuollossa. Helsinki: Tietosanoma Oy.

23 PotasiakA 2009. Sosiaali- ja terveysministeriön asetus potilasasiakirjoista 30.3.2009/298. Valtion Säädöstietopankki. Osoitteessa http://www.finlex.fi/fi/laki/ajantasa/2009/20090298. 15.9.2010.