TIETOTURVAN KEHITTÄMINEN SOSIAALI- JA TERVEYSTOIMESSA

Case: Hankasalmen sosiaali- ja terveystoimi

Marja Leena Hämäläinen

Toukokuu 2010

Tietojenkäsittelyn koulutusohjelma
Luonnontieteiden ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖN
KUVAILULEHTI

Tekijä(t)	Julkaisun laji	Päivämäärä
HÄMÄLÄINEN, Marja Leena	Opinnäytetyö	7.5.2010
	Sivumäärä 72	Julkaisun kieli Suomi
	Luottamuksellisuus ( ) saakka	Verkkojulkaisulupa myönnetty (X)

Työn nimi
TIETOTURVAN KEHITTÄMINEN SOSIAALI- JA TERVEYSTOIMESSA, Case: Hankasalmen sosiaali- ja terveystoimi

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Työn ohjaaja(t)
BISTER, Timo

Toimeksiantaja(t)
Hankasalmen sosiaali- ja terveystoimi

Tiivistelmä
Opinnäytetyön toimeksiantaja oli Hankasalmen sosiaali- ja terveystoimi. Opinnäytetyössä keskitytiin henkilöstön käsitykseen tietoturvasta ja siitä rajattiin pois ulkoiset - ja tekniset tietoturvauhat.

Tietoturvan merkitys on oivallettu kauan sitten. Jo Hippokrates lausui kuuluisan lääkärinvalansa 400 vuotta ennen ajanlaskumme alkua. Nykypäivänä PARAS-hanke edellyttää terveydenhuollon yksikköön vähintään 20 000 ihmisen väestöpohjan vuoden 2011 alkuun mennessä. Tietoturvan merkityksen selkiyttäminen ja sen tason nostaminen lain edellyttämälle tasolle on ensiarvoisen tärkeää yhä laajempien sosiaali- ja terveydenhuollon yksiköiden takia.

Työssä on esitelty keskeistä lainsäädäntöä ja keskeisiä tulkintoja tietoturvasta ja salassapidosta. Samoin käsiteltiin tietosuojavastaavan toimenkuvaa ja asemaa tietoturvan ylläpitäjänä. Tutkimusosiossa selvitettiin tietoturvan tasoa Hankasalmen sosiaali- ja terveystoimessa ja tulosta vertailtiin myös Etelä-Pohjanmaan sairaanhoitopiiristä saatuun vastaavaan tutkimukseen. Kysely toteutettiin Webropol-ohjelmistoa käyttäen ja se suunnattiin kaksiosaisena tutkimuksena henkilöstölle. Yleisiin tietoturvakysymyksiin vastasivat kaikki ja Effica tietojärjestelmää käyttävät lisäksi sitä käsittelevään osioon. Työn tavoitteena oli selvittää ne tietoturvan kohdat, joissa tarvitaan selkiyttämistä koulutuksen ja tiedotuksen avulla.

Tietoturvan taso oli tärkeimmissä kohdissa hyvä. Joissakin osioissa esiintyi molemmissa yksiköissä selvästi tietämättömyyttä. Yksiköiden vastaukset noudattivat samaa linjaa, vaikka toisessa yksikössä oli yli tuhat työtekijää ja toisessa noin sataviisikymmentä.

Kyselyn tuloksista pidetään koulutustilaisuuksia ja tämän jälkeen voidaan kysely uusia ja tutkia koulutuksen vaikuttavuutta. Kun terveystoimi yhdistyy vuoden 2011 alussa Jyväskylän isäntäkuntaan, voidaan myös siellä testata tietoturvan taso vastaavalla kyselyllä.

Avainsanat (asiasanat)
Tietoturva, salassapito, vaitiolovelvollisuus, henkilöstö, kyselytutkimus, koulutus

Muut tiedot

Author(s)
HÄMÄLÄINEN, Marja Leena

Type of publication
Bachelor´s Thesis

Date
7.5.2010

Pages
72

Language
Finnish

Confidential
( ) Until

Permission for web publication
(X)

Title
THE DEVELOPMENT OF DATA SECURITY IN SOCIAL- AND HEALTH BUSINESS Case: Hankasalmi`s social- and health care center

Degree Programmed
Business Information Systems

Tutor(s)
BISTER, Timo

Assigned by
Social- and health care center in Hankasalmi, Hankasalmi

Abstract
This Bachelor´s Thesis was assigned by the social- and health center in Hankasalmi. External and technical threats were out of the scope of this thesis and the focus was on the personnel´s opinion of security.

The purpose of data security has been understood far in history and already 400 years before the beginning of our chronology Hippocrates said his famous doctor oath. Presently PARAS-project requires that in the health care organization area there must be a 20 000 population by the beginning of year 2011. This is important because clarifying the meaning and raising the level of information security to meet the demands of legislation is vital due to larger and larger units of social and health care. This study presents central legislation and central prognoses of data security and confidentiality. Likewise it processes the job description and position of confidentiality administrator of data security. In the research part the level of data security in social- and health care in Hankasalmi was discussed and the result compared also with a similar survey of the Southern Ostrobothnia Health Care district. The enquiry was carried out with Webropol program and it was directed to the staff as a two-part research. The questions on the data security of the first part were answered by all and those using the Effica- information system answered also to the questions of the second part. The aim to this work was to clarify such cases of data security, where more knowledge is needed and can be obtained with education and information.

The level of the data security was good in the most important items. In some of parts there was clearly ignorance in both organizations. The answers of the units followed a similar pattern although in the first organization there are approximately one hundred and fifty employees and in the second organization has about one thousand employees. The outcomes of the survey result in training events and after those the survey can be repeated to study the effect of the training. When the health care of Hankasalmi merges with Jyväskylä at the beginning of 2011 the level of information security can be tested with the same survey also there.

Keywords
data security, concealment, professional secrecy, employees, enquiry, education, data security directions

Miscellaneous

SISÄLTÖ

KUVIOT

TAULUKOT

1 TIETOTURVA KIINTEÄKSI OSAKSI TYÖTÄ

Tietoturvalla terveydenhuollossa on todella pitkät perinteet. Jo Hippokrateen lääkärinvalassa vuodelta 400 ennen ajanlaskumme alkua vannotaan asiakassuhteen luottamuksellisuuden nimiin. ”Mikäli parannustyössäni tai sen ulkopuolella ihmisten parissa näen tai kuulen sellaista, mitä ei pidä levittämän, vaikenen ja pidän sen salaisuutena” (Solin 2005). Tältä ajalta aina 1900-luvulle on potilaan osallistumista hoitoon pidetty enemmän tarpeettomana ja häiritsevänä kuin hyödyllisenä. (Heiliö, Kattelus, Kaukonen, Kumpula, Narikka, Sintonen & Ylipartanen 2006, 633.)

Tultaessa nykypäivään on kunta- ja palvelurakenneuudistukseen tähtäävä PARAS-hanke käynnistynyt vuonna 2005. Tavoitteena on parantaa tuottavuutta kunnissa sekä kehittää palvelujen tuotantotapoja ja organisointia. Hankkeen tarkoitus on myös hillitä menojen kasvua. Laki kyseisestä palvelurakenneuudistuksesta tuli voimaan helmikuussa 2007. Lain edellyttämien muutosten tulee valmistua puitelain voimassaoloaikana vuoden 2012 loppuun mennessä. Myös sosiaalitoimea koskeva samankaltainen yhdistymisvelvoite on valmistelussa valtakunnan tasolla.

PARAS-hankkeessa edellytetään vähintään 20 000 asukkaan väestöpohjaa terveydenhuollon yksiköille vuoteen 2011 mennessä. Yhä suurempi joukko terveydenhuollon ammattilaisia näkee jokaisen ihmisen tiedot yhä suuremmalla alueella. Tässä tilanteessa on tärkeää terävöittää käytänteitä ja lisätä työntekijöiden tietoisuutta tietoturvasta, sen valvonnasta ja tarpeellisuudesta. Hankasalmen kunnan terveystoimen yhdistyminen Jyväskylän kaupungin isännöimään seudulliseen yhteistyöhön tapahtunee vuoden 2011 alussa.

Tässä opinnäytetyössä tutkitaan tietoturvan tasoa Hankasalmen sosiaali- ja terveystoimen henkilöstön keskuudessa kyselytutkimuksena. Tutkimuksen perusteella voidaan löytää mahdolliset puutteet tietoturvasta ja suunnata lisää tietämystä henkilökunnan keskuuteen koulutuksen avulla. Tähän opinnäytetyöhön liitetään sosiaali- ja terveystoimen henkilöstölle tarkoitettu tietoturvaohje, joka osaltaan palvelee tietoturvan tason nostamista lain edellyttämälle tasolle.

2 TIETOTURVA LAADUKKAAN PALVELUN OSANA

Tässä luvussa esitellään tietoturvan kehitykseen liittyviä tapahtumia sekä tutkimuksen toimeksiantaja ja kerrotaan tutkimuksesta. Luvun lopussa kerrotaan työssä käytetyistä tutkimusmenetelmistä ja esitellään tutkimuskysymykset.

Vaikka tietoturvan juuret ovat kaukana menneisyydessä, teknistyvä yhteiskunta asettaa tietoturvalle suuria haasteita kolmesta näkökulmasta. Tietojärjestelmät eivät toimi ilman ihmisiä, he käyttävät ja valmistavat niitä. Laitteistot voivat myös vioittua, ja tämä aiheuttaa uhan tietoturvallisuudelle esimerkiksi mahdollisen tietojen häviämisen kautta. Kolmas uhka on ulkoinen. Tätä varten arkaluonteiset sosiaali- ja terveystoimen tiedot tarvitsevat mahdollisimman laadukkaan suojauksen. Suurin riski tietoturvalle aiheutuu kuitenkin organisaation sisällä.

2.1 Tietoturvan kehitykseen liittyviä tapahtumia

Sosiaali- ja terveysministeriö asetti vuonna 1995 työryhmän, jonka tehtävänä oli laatia sosiaali- ja terveysministeriön tietohallinnon toimintastrategia siten, että parannetaan uuden tietotekniikan avulla sosiaaliturvan saatavuutta, laatua ja tehokkuutta. Työryhmään nimettiin laaja joukko alan asiantuntijoita eri ministeriöistä ja mm. Stakesista ja Kansanterveyslaitokselta. (STM:n raportti 1999.)

Tämä hanke oli ensimmäinen sosiaali- ja terveydenhuollon kansallisen tietoteknologian hyödyntämisstrategiaa pohtiva hanke. Sen keskeiset linjaukset olivat mm. seuraavia:

- Tietoyhteiskunta kaikkien ulottuville
- Palvelujen porrastuksista saumattomaan palveluketjuun
- Verkostoitumisen perusta on kunta ja verkostoinnin edellytys on moniulotteiset tietoverkot
- Kansalaisten toimintamahdollisuudet paranevat
- Tietosuojan ja tietoturvan kehittäminen
- Tietojärjestelmien yhteensopivuuksien ja integraation parantaminen

- Tiedon ja osaamisen monipuolinen hyödyntäminen ja
- Osaava ja jaksava henkilöstö.

(STM:n raportti 1999.)

Tämä hanke asettaa tietosuojalle erityiset haasteet, koska tässä hankkeessa käsitellään asiakkaan arkaluonteisimpia tietoja (STM:n raportti 1999).

Kuin jatkumona tähän hankkeeseen Apteekin asiakaslehdessä 1 / 2010 on artikkeli Sähköinen resepti vihdoin käyttöön, jossa todetaan seuraavaa:

> Terveydenhuollon sähköinen uudistus alkaa tänä vuonna toteutua. EReseptin, eArkiston ja eKatselun käytännön testaukset ovat alkaneet. Potilastietojen valtakunnallista eArkistoa kokeillaan Kuopion terveyskeskuksessa ja Itä-Savon sairaanhoitopiirissä syksyllä. Muualla Suomessa sen soveltaminen alkaa aikaisintaan 2012. (Salo 2010.)

Sähköinen resepti tulee alkuvuonna käyttöön Kotkan ja Turun terveyskeskuksissa. Potilaat voivat tuolloin katsella omia lääkitystietojaan eKatselun kautta. (Kallio 2010.)

2.2 Tietoturvallisuus nykypäivänä

Tietoturvallisuus on nykyään yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys. Lainsäädäntö Suomessa lähtee siitä, että tietoturvallisuus on hoidettava asianmukaisesti. Suuria haasteita tietoturvallisuudelle asettaa meneillään oleva yhä laajempi siirtyminen sähköisiin järjestelmiin ja kansalaisten palvelu tietoverkkojen välityksellä alueella, jossa käsitellään salassa pidettävää ja arkaluonteista asiakas- ja potilastietoa. (Heikkilä, Rousku & Ruotsalainen, 2005, 2.)

Tietoturvallisuudella tarkoitetaan asiantilaa, jossa tietojen, tietojärjestelmien, tietoliikenteen luottamuksellisuuteen ja käytettävyyteen kohdistuvat uhkat eivät aiheuta merkittävää riskiä. Tietoturvallisuus on kiinteä osa jokaisen sosiaali- ja terveydenhuoltoalan toimijan ja organisaation toimintaa ja koskee koko henkilökuntaa. Tietosuojalla tarkoitetaan henkilötietojen suojaamista henkilöä vahingoittavalta käytöltä. (Heikkilä ym. 2005, 3.)

Nykyään myös eri sosiaali- ja terveydenhuollon ammattiryhmät ovat luoneet omia ammattieettisiä ohjeita, joissa on mukana asiakkaan tietosuojaa koskevia kohtia. Näiden menettelytapasäännösten tarkoituksena on luoda hyvää henkilötietojen käsittelytapaa ja ne tukevat samalla tietosuojan tavoitteita. (Heiliö ym. 2006, 633.)

Sosiaali- ja terveydenhuollon organisaatioiden toiminta perustuu yhä enemmän tietoon, joka on entistä yksityiskohtaisempaa. Lisäksi tämä tieto on useimmiten sähköisessä muodossa. (Tammisalo 2005, 2.) Tämä tietojen sähkömuotoisuus asettaa suuret vaatimukset turvallisuudelle ja toisaalta tekee mahdolliseksi monipuolisen ja varman käytön seurannan, valvonnan ja käyttäjien valtuuksien määrittelyn. Seuranta ja poikkeustilanteiden valvonta voidaan toteuttaa reaaliaikaisesti. (Heikkilä ym. 2005, 3.)

2.3 Tutkimusasetelma

2.3.1 Toimeksiantaja, tutkimuksen tarve ja rajaus

Tutkimus tehdään Hankasalmen kunnan sosiaali- ja terveystoimessa. Hankasalmen kunnassa on työntekijöitä hieman alle 400 ja sosiaali- ja terveystoimessa yhteensä noin 170 henkilöä. Terveydenhuollon ja sosiaalihuollon lainsäädännön piiriin kuuluvat kaikki nämä työntekijät tietosuojamääräysten osalta. Hoitohenkilöstöä tässä yksikössä on valtaosa, sairaanhoitajia parikymmentä sekä lähihoitajia loput hoitajista. Muita ammattiryhmiä ovat lääkärit, hammashuollon henkilöstö, toimistohenkilöstö ja sosiaalipuolella päiväkodeissa työskentelevät sekä laitosapulaiset. (Hankasalmen kunnan toimintakertomus v. 2008.)

Työskentelen terveystoimessa ja työnkuvaani kuuluvat tietoturvavastaavan tehtävät. Hankasalmella ei ole selvitetty tietoturvan tasoa millään tutkimuksella eikä terveyskeskuksessa ole myöskään tietoturvaohjetta. Tutkimuksen tarkoitus on saada kuva tämänhetkisestä tietoturvan tasosta sosiaali- ja terveystoimessa ja sen avulla saada selville myös tietoturvan kehittämis- ja koulutustarpeet. Tutkimus suunnataan hoitohenkilöstölle laajana tutkimuksena, johon kuuluvat omana osionaan Effica-tietojärjestelmää käyttävien kysymykset. Muut vastaavat kyselyn osioon ”Yleiset

tietoturvakysymykset”. Muita tietojärjestelmiä sosiaali- ja terveystoimessa ovat Pegasos-ohjelmat, joita käytetään taloushallinnon tehtäviin.

Tutkimuksessa on käytössä myös Etelä-Pohjanmaan sairaanhoitopiirin kyselyn tulos tietoturvasta. Tätä tulosta verrataan soveltuvin osin Hankasalmella tehtävään tutkimukseen. On mielenkiintoista nähdä ison ja pienen yksikön eroavaisuus tai samankaltaisuus tietoturvan tasossa.

Aihealue rajataan osin toimeksiantajan toiveesta nimenomaan käsittelemään tietoturvaa henkilöstön näkökulmasta. Tutkimuksesta jätetään lähes kokonaan pois ulkoiset ja laitteisto-uhat sekä niiden torjuntatavat.

2.3.2 Tutkimuskysymykset ja -menetelmät

Tutkimus on kaksijakoinen, koska niin terveys- kuin sosiaalitoimessakin on henkilöitä, jotka eivät käytä Effica-tietojärjestelmää. Lääkärit, hoitajat ja terveystoimiston toimistossa työskentelevät käyttävät tätä hoitotietojen tallennusjärjestelmää ja näille henkilöille suunnataan tutkimus laajana. Muut vastaavat kyselyn osioon ”Taustatiedot” ja ”Yleiset tietoturvakysymykset”.

Varsinaiset kysymykset ovat seuraavat:

- Miten henkilöstö ymmärtää tietosuojan vaatimukset?
- Mikä on tietoturvan taso henkilökunnan osalta?
- Mitkä ovat ne tietoturvan ongelmallisiksi koetut kohdat, joissa tarvitaan tietämyksen lisäämistä ja tämän kautta mahdollistetaan tietoturvan toteutuminen lain edellyttämässä tasossa?

Opinnäytetyö tulee olemaan Hankasalmen sosiaali- ja terveystoimea varten tehty kehittämistutkimus, jonka tarkoitus on saada selville tietoturvan taso tässä yksikössä. Tämän tutkimuksen tarkoituksena on selvittää puutteet tietoturvassa ja saada jatkossa henkilökunnan tietämys tietoturvasta mahdollisimman laajaksi.

Kvantitatiivisen tutkimusmenetelmän keskeisiä piirteitä ovat mm. johtopäätökset aiemmista tutkimuksista, aiemmat teoriat, aineiston keruun suunnittelu, jossa on

tärkeää, että aineisto soveltuu määrälliseen ja numeeriseen mittaamiseen. Lisäksi tähän menetelmään kuuluu olennaisena osana tutkittavien henkilöiden valinta, tästä otoksen ottaminen, muuttujien muodostaminen taulukkomuotoon ja aineiston saattaminen tilastolliseen muotoon. Lopuksi havaintoaineistosta tehdään päätelmiä tilastolliseen analysointiin perustuen, mm. tulosten kuvailua prosenttitaulukoiden avulla. (Hirsjärvi, Remes & Sajavaara 2009, 140.)

Edellä kuvatun perusteella kvantitatiivinen tutkimusmenetelmä soveltuu parhaiten selventämään tietoturvakysymyksiä Hankasalmen sosiaali- ja terveystoimessa tehtävässä tutkimuksessa. Tutkimukseen on määritelty tietty joukko, jolle kysely on suunnattu. Tässä menetelmässä voidaan vertailla tietoa ja voidaan myös tehdä kuvaavia taulukoita ja kuvioita tuloksista. (Hirsjärvi ym. 2009, 140.) Tämä menetelmä sopii hyvin aloittelevalle tutkimuksen tekijälle. Tutkimustyökaluna käytetään Webropol-ohjelmaa, joka on Hankasalmella käytössä.

3 TIETOTURVALAINSÄÄDÄNTÖÄ

Useissa eri laeissa käsitellään tietoturvaa ja salassapitoa niin terveys- kuin sosiaalitoimenkin ammattilaisten suhteen. Merkittävimpiä tätä tutkimustyötä ajatellen ovat mm. laki terveydenhuollon ammattihenkilöstöstä, laki sosiaalihuollon asiakkaan asemasta ja oikeuksista sekä laki potilaan asemasta ja oikeuksista. Näitä selvennetään tässä luvussa.

Tähän lukuun sisältyy myös rajanvetoa julkisen ja salaisen tiedon välillä, sosiaalihuollon lakien erityispiirteitä salaisuudesta, salassa pidettävistä tiedoista, perheen salaisuudesta ja vaitiolovelvollisuudesta. Samoin käsitellään arkaluonteisten tietojen käsitteitä.

3.1 Julkinen/salainen tieto

Sananvapautta ja julkisuutta koskeva lainsäädäntö sisältyy Suomen perustuslain 12 pykälään. Pykälän 2 momentin mukaan jokaisella on oikeus saada tietoonsa julkiset asiakirjat tai tallenteet, jotka ovat viranomaisen hallussa. (Heiliö ym. 2006, 735.)

Laki viranomaisten toiminnan julkisuudesta sääntelee viranomaistoimintaa ja erityisesti asiakirjojen käsittelyyn liittyvää julkisuutta. Lain tarkoituksena on lisätä viranomaistoiminnan avoimuutta ja tehostaa julkisuusperiaatteen ja hyvän tiedonhallintatavan toteutumista julkisissa yhteisöissä. Yleisenä tarkoituksena on antaa yksilöille ja yhteisöille tiedonsaantimahdollisuus oikeuksistaan ja eduistaan, parantaa tiedonsaantioikeutta käsittelyssä olevista asioista sekä valvoa julkisen vallan ja julkisten varojen käyttöä. Viranomaisten on vastaavasti autettava tiedonsaantioikeuksien toteutumisessa. Sen on tuotava julki tekemiään päätöksiä ja myös huolehdittava siitä, että toimintaa koskevat tiedot ja asiakirjat ovat helposti saatavilla. (Heiliö ym. 2006, 735.)

Julkisuuslain 4 §:ssä määritellään edellä mainitut viranomaiset. Viranomaisille tarkoitetaan valtion hallinnonviranomaisia sekä muita valtion virastoja ja laitoksia, tuomio-

istuimia ja muita lainkäyttöelimiä, valtion liikelaitoksia, kunnallisia viranomaisia, itsenäisiä julkisoikeudellisia laitoksia, eduskunnan virastoja ja laitoksia sekä Ahvenanmaan maakunnan viranomaisia. Viranomaisena pidetään myös tiettyä tehtävää suorittamaan asetettua lautakuntaa, neuvottelukuntaa, komiteaa, toimikuntaa, työryhmää, toimitusmiestä tai kunnan ja kuntayhtymän tilintarkastajaa sekä muita näihin verrattavia toimielimiä. (Heiliö ym. 2006, 736.)

Julkisuuslain 1 pykälän julkisuusperiaatteen mukaan viranomaisten asiakirjat ovat pääperiaatteen mukaan julkisia. Sosiaali- ja terveydenhuollon hallinnonalalla käsiteltävät asiakirjat ovat arkaluonteisuuden vuoksi salassa pidettäviä ja näillä aloilla on säädetty laajoja poikkeuksia julkisuusperiaatteesta. (Heiliö ym. 2006, 735.)

3.2 Tietoturvaa koskevat keskeiset lait

Laki terveydenhuollon ammattihenkilöstöstä

Lain 3. luku 16 § käsittelee potilasasiakirjojen laatimista, säilyttämistä ja näiden tietojen salassapitoa (L 28.6.1994/559).

Saman luvun 17 §:ssä määritellään terveydenhuollon henkilöstön potilastietojen salassapitovelvollisuus. Terveydenhuollon piirissä työskentelevät eivät saa ilmaista sivulliselle luvatta perheen salaisuutta, josta hän on saanut tiedon harjoittaessaan ammattiaan. Tämä velvollisuus tietojen salaamiseen säilyy senkin jälkeen, kun ammatinharjoittaminen on lakannut. (L 28.6.1994/559.)

Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista

Tässä laissa määritellään asiakirjojen salassapito ja työntekijän vaitiolovelvollisuus sosiaalihuollossa. Lain 3. luvussa 14 §:ssä todetaan salaisiksi sellaiset asiakirjat, jotka käsittelevät sosiaalihuollon asiakkaan tai muun yksityisen henkilön tietoja. Saman pykälän 2. momentissa säännöstä tarkennetaan vielä salassa pidettävän asiakirjan säännöstä. Asiakirjaa ei tämän mukaan saa kopioida, näyttää tai luovuttaa ulkopuoliselle eikä antaa sitä myöskään minkään teknisen ulkoyhteyden tai muun sellaisen kautta ulkopuoliselle taholle nähtäväksi tai käytettäväksi. 3. luvun 15 §:ssä säädetään

ammattihenkilön vaitiolovelvollisuudesta ja tietojen hyväksikäyttökiellosta. (L 22.9.2000/812.)

Laki potilaan asemasta ja oikeuksista

Tähän lakiin sisältyvät potilasasiakirjojen salassapitosäännökset. Laissa 4. luvussa 13. pykälässä sen ensimmäisessä momentissa todetaan, että potilasasiakirjoihin sisältyvä tieto on salassa pidettävää. Terveydenhuollon ammattihenkilö tai muu terveydenhuollon toimintayksikössä työskentelevä ei saa antaa potilasasiakirjoista tietoa sivullisille ilman asianomaisen potilaan lupaa. Jos potilas ei itse voi arvioida luvan antamista terveydentilastaan johtuen, voi tietojen luovuttamiseen luvan antaa myös potilaan laillinen edustaja. (L 17.8.1998/785.)

Tässä laissa määritellään myös sivullinen. Sivullisella tarkoitetaan muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon liittyviin tehtäviin osallistuvia henkilöitä. Salassapitovelvollisuus säilyy palvelussuhteen tai tehtävän päättymisen jälkeenkin. (L 17.8.1998/785.)

3.3 Arkaluonteisten tietojen käsittelykielto sekä sitä koskevat poikkeukset

Henkilötietolain mukaan arkaluonteisten tietojen käsittely ja kerääminen on pääasiassa kiellettyä. Arkaluonteisten tietojen käsittelykiellosta voidaan poiketa. Laissa säädetään, että terveydenhuollon asiakkaaksi tulevan henkilön tietoja voidaan kerätä, tallentaa ja käsitellä, jos tehtävien hoito sitä edellyttää. Rekisterinpitäjän (hoitava yksikkö) ja asiakkaan välille muodostuu tällöin henkilötietolain tarkoittama asiallinen yhteys eli asiakassuhde, ja tällä perusteella asiakas saa tietää itseään koskevien tietojen tallentamisen. Vaikka asiakassuhdetta ei olisikaan, voidaan asiakkaan suostumuksella käsitellä hänen tietojaan. Rekisterinpitäjä voi myös käsitellä näitä tietoja ilman asiakkaan lupaa, jos se hoidon kannalta on välttämätöntä. (Heiliö ym. 2006, 639–640.)

Arkaluonteisina pidetään tietoja, jotka koskevat:

- henkilön rotua tai etnistä alkuperää, yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista,
- rikollista tekoa tai muuta rikoksen seuraamusta tai näistä saatavaa rangaistusta,
- henkilön terveydentilaa, sairautta tai vammaisuutta tai näistä johtuvia hoitotoimenpiteitä tai niihin verrattavia toimia,
- henkilön seksuaalista suuntautumista,
- henkilön sosiaalihuollon tarvetta tai muita tällaisia tukitoimia tai etuuksia.

(Heiliö ym. 2006, 639.)

Sosiaalihuollon puolella on samankaltainen säännös siitä, että sosiaalihuollon viranomainen tai sosiaalietuuksia myöntävä viranomainen tai muu vastaava voi saada tiedon rekisteröidyn sosiaalihuollon tarpeesta tai hänen saamistaan sosiaalipalveluista ym. tukitoimista, jos tiedot ovat huollon kannalta välttämättömiä. (Heiliö ym. 2006, 640.)

Henkilötietolain tarkoittamia arkaluonteisia tietoja ei pääsääntöisesti saa merkitä lainkaan asiakastietoihin. Jos tällaisia tietoja tallennetaan, on siihen aina esitettävä syy, joka on tehtävien hoidon kannalta välttämätön ja hyväksyttävä. Henkilötietolain käsittelyn tarkoituksen kannalta tarpeettomia tietoja ei saa tallentaa rekisteriin edes asiakkaan suostumuksella. (Heiliö ym. 2006, 640.)

3.4 Salassapitovelvollisuus ja vaitiolovelvollisuus sosiaalihuollossa

Kuten edellä on jo mainittu, julkisuuslailla säädellään myös salassapitoa. Salassapidolla suojellaan joko yleistä tai yksityistä etua. Yksityinen etu voi liittyä esimerkiksi taloudellisiin etuihin. (Sorvari 2001, 44—45.)

Sosiaalihuollon toimintaympäristössä painottuu erikoisesti, että suojelukohteena voi olla yksilön tai koko perheen salaisuus. Leimautuminen on esimerkiksi syy, minkä takia henkilöä tai perhettä koskeva tieto on luokiteltu salaiseksi (Sorvari 2001, 45). Sosiaalihuollon asiakaslakiin sisältyvät sekä julkisiin että yksityisiin sosiaalipalveluihin sovellettavat erityissäännökset salassapitovelvoitteista ja poikkeuksista niihin. (Heiliö ym. 2006, 660.)

Sosiaalihuoltolaissa 57 §:ssä on määritelty salassa pidettäväksi yksilön tai perheen salaisuus. Salaisuus on yksityiselämään kuuluva ydinalueen tieto. Lakitekstissä ei enää ole termiä salainen tieto, mutta edelleen voidaan kutsua yksityisyyden piiriin kuuluvaa tietoa salaisuudeksi ja toisaalta salaisuutta salassa pidettäväksi tiedoksi. Salaisuus ja salassapito ovat erityyppisiä käsitteitä. Asia, joka ei sinänsä ole salainen, voi jossain asiayhteydessä olla salassa pidettävä tieto. Tällainen on esimerkiksi henkilön nimi. Se ei itsessään ole salaisuus, mutta jollain edellytyksillä siitä tulee sellainen. Asiakkaan nimi on sosiaalihuollon asiakaslain mukaan salassa pidettävä tieto. Nimi voi olla riittävän paljastava tieto kertomaan palvelun tarpeesta eli itse salaisuudesta. (Sorvari 2001, 45—46.)

Sosiaalihuollon asiakaslaissa todetaan salassa pidettäväksi myös asiakirjat, jotka sisältävät tietoa sosiaalihuollon asiakkaasta tai muusta yksityisestä henkilöstä. Salassapito ei näin ollen ole sidottu pelkästään sosiaalihuollon asiakkuuteen, vaan salassa pidettävä on asiakirjassa oleva henkilötieto asiakassuhteesta riippumatta. Sivullisilla ei ole oikeutta millään tavalla saada tietoonsa kyseessä olevia asioita. Joskus voi syntyä tilanteita, joissa henkilö on sosiaalihuollon asiakirjan sisällön kannalta osittain asianosainen ja osittain sivullinen. Tällöin toimitaan tapauskohtaisesti arvioimalla, missä laajuudessa hänelle on mahdollista antaa tietoa asiakirjasta. (Sorvari 2001, 50—51.)

Sosiaalihuollon asiakaslaissa säädetään myös vaitiolovelvollisuudesta. Se on laajempi käsite kuin salassapito. Vaitiolovelvollisuus käsittää muunkin kuin asiakirjatiedon. Vaitiolo tarkoittaa, että siihen velvoitettu ei voi millään tavoin paljastaa tietoa. Vaitiolovelvollisuus ulottuu kaikkiin viranomaisen palveluksessa työskenteleviin ja myös esimerkiksi viranomaista valvoviin luottamushenkilöihin. Vaitiolovelvollisuutta on noudatettava myös eri työyksiköiden kesken ja samoin työyksiköissä työskentelevien työntekijöiden kesken. (Sorvari 2001, 51—53.)

4 NYKYPÄIVÄN TIETOSUOJAN HAASTEET, NIIHIN VASTAAMINEN JA TIETOTURVA KÄYTÄNNÖSSÄ

Jos ajatellaan esimerkin avulla aikaa hieman taaksepäin, niin vuonna 2004 Hankasalmen terveyskeskuksessa potilastiedot olivat vain kansien välissä arkistossa paperiversioina. Tietoturvariskit olivat vain siinä, kuka henkilöstöstä luki mahdollisesti toisen henkilön tietoja luvatta. Tällä hetkellä tilanne on aivan toinen. Kaikki potilastiedot ovat sähköisessä potilastietojärjestelmässä. Paperitulosteita ei enää juuri käytetä. Tietoturvan riski on aivan sama henkilöstön suhteen kuin paperiaikanakin, joskin sitä on helpompi valvoa. Nyt ovat tulleet mukaan kuitenkin huomattavasti laajemmat uhat, kuten tietojärjestelmän pettäminen, esimerkiksi tästä johtuva tietojen häviäminen, tietojärjestelmää kohtaan tehdyt mahdolliset ulkoiset hyökkäykset ja niin edelleen. Tässä luvussa kuvataan tietoturvan uhkia ja yhteiskunnan vastaamista niihin sekä tietoturvan varmistamista käytännössä.

4.1 Tietoturvaan kohdistuvia uhkia

Kuten jo vuosituhansia sitten myös nykyään sosiaali- ja terveydenhuollon asiakassuhteissa korostuu luottamuksellisuuden periaate. Asiakkaiden on voitava luottamuksellisesti hakeutua erilaisiin hoitoihin, tutkimuksiin ja muihin palveluihin. Tarvitaan aina asiakkaan suostumus, jos tarpeellisia tietoja kerätään muista tietolähteistä kuin asiakkaalta itseltään. (Heiliö ym. 2006, 628.)

Sosiaali- ja terveydenhuollossa käytetään nykyään entistä enemmän sähköisiä järjestelmiä. Palvelut ovat entistä enemmän riippuvaisia tietojen saatavuudesta ja luotettavuudesta ja tämä asettaa sosiaali- ja terveydenhuollon yksiköille velvoitteita tietojen salassapidosta. Salassa pidettävillä henkilötietojen käsittelyllä tarkoitetaan mm. henkilötietojen keräämistä, tallentamista, käyttöä, siirtämistä toiseen yksikköön, luovuttamista, poistamista ja tuhoamista. (Heiliö ym. 2006, 628.)

Sosiaali- ja terveydenhuollon tietosuojan tarkoituksena on henkilötietojen hyvän käsittelytavan luominen ja toteuttaminen kaikissa henkilötietojen eri vaiheissa. Lisäksi tietosuojaan kuuluvia peruspilareita ovat henkilöiden oikeuksien kunnioittaminen ja toteuttaminen sekä sosiaali- ja terveystoimen yksikköjen oikeusturvan varmistaminen. (Heiliö ym. 2006, 628.)

Tietosuojassa ei ole kyse vain tiedon konkreettisesta suojaamisesta, vaan suojaamisen kohteena olevan ihmisen yksityisyyden suojasta, luottamuksellisesta asiakassuhteesta, itsemääräämisoikeudesta, minäkuvasta ja sosiaalisista suhteista. Esimerkiksi sairaalan lääkäri- tai hoitajakierrolla keskusteluja potilaan terveydentilasta ei saa käydä sivullisten kuullen ilman potilaan lupaa. (Ylipartanen 2004, 24.)

Yhteiskunnan toiminnot ovat riippuvaisia tietojenkäsittelystä. Tällaisessa verkottuneessa ympäristössä enää harva yksikkö vastaa vain omasta tietoturvallisuudestaan. Tietoturva kattaa hyvin suuren osan sosiaali- ja terveyspalvelujen tehtävistä, ja tämä asettaa tietojärjestelmien käyttäjille vaatimuksia. (Witick & Meriläinen 2009, 3.)

Potilasturvallisuus voi vaarantua monella eri tavalla. Potilas voi saada esimerkiksi väärää tai puutteellista hoitoa ja hänen yksityisyyden suojansa voi vaarantua. Huolimatta virheestä vaikutus potilaaseen on samanlainen. Jokainen erilainen uhka vaatii omanlaisensa torjuntatoimenpiteen. Vahingon toteutumisen mahdollisuus on kussakin tapauksessa erilainen, ja kaikkiin riskeihin ei tarvitse varautua yhtä voimakkain toimenpitein. (Tammisalo 2005, 5.)

Jos esitetään tietoturvaa numeroina, tietoturvasta 20 % koostuu teknologiasta ja 80 % on ihmisen toimintaa, asenteita, menetelmiä ja osaamista. Vastaavasti tietoturvauhista ja niiden aiheuttamista haitoista rahalla mitaten 25 % aiheutuu organisaation ulkopuolelta ja 75 % organisaation sisältä. (Tammisalo 2007, 17.)

Asiakirjahallinto tarkoittaa työyksikön ja koko organisaation toimintaan sisältyvien asioiden ja asiakirjojen käsittelyä niiden koko olemassaolon ajan. Tiedoilla tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää ja siirrettävää organisaation omaa tietoa. Se voi olla yksittäisessä asiakirjassa, tietokoneen muistissa ja vaikkapa yksittäisen työntekijän muistissa. Tietoturvan näkökulmasta jo edellä mainitut tiedon käsittelyvaiheet ovat merkityksellisimpiä. (Witick & Meriläinen 2009, 5–6.)

Stakesin näkemyksen mukaan turvalliseen tietoyhteiskuntaan kuuluu myös se, ettei kansalaisista kerätä tarpeettomasti tietoa heidän sähköisistä asioinneistaan ja että kansalaisilla on oikeus päättää, kuka heidän tietojaan kerää ja mihin tarkoituksiin niitä käytetään. Kansalaisilla tulee olla myös oikeus kieltää heidän luottamuksellisten tietojensa käyttö. Tietoyhteiskunta muodostaa kasvavan riskin kansalaisen yksityisyydelle. Nykyään kaikesta sähköisestä asioinnista jää jälkiä erilaisille palvelimille ja rekistereihin. Lisäksi yhä laajempi joukko viranomaisia yhdistelee ja käyttää kansalaisten tietoja erilaisia tarkoitusperiä varten. Erityinen riski muodostuu silloin, kun ovat kyseessä kansalaisten terveyteen, hyvinvointiin ja elintapoihin liittyvät tiedot. (Heikkilä ym. 2005, 1.)

Tietoturvallisuuden kehittäminen on vaativa haaste, joka edellyttää käyttäjien tietotaitotason kasvattamista, teknologisten torjuntakeinojen kehittämistä edelleen ja koulutusta, tiedotusta ja viestintää. Kaikenkattavaa ratkaisua ongelmiin on mahdotonta laatia, kun otetaan huomioon vaikkapa olemassa oleva lainsäädäntö, markkinoilla olevat erilaiset tietojärjestelmät ja laitteet sekä tietoliikenne. Usein on todettu, että tietoturvallisuus on yhtä hyvä kuin sen ”heikoin lenkki”. Tulevaisuudessa on tärkeää löytää nämä lenkit ja saada niitä vahvistettua, että koko tietojärjestelmän taso kohentuisi. (Heikkilä ym. 2005, 13.)

4.2 Rekisterinpitäjän määritelmä

Henkilötietolain mukaan henkilötietoja saa kerätä vain lain tarkoittama rekisterinpitäjä. Henkilötietojen käsittelyn avoimuus on rekisteripitäjän toiminnan avoimuutta rekisteröityyn. Rekisterinpitäjällä on informaatiovelvoitteita. Passiivisen informaatiovelvoitteen mukaan on rekisterinpitäjän laadittava henkilörekisteristä rekisteriseloste ja pidettävä se jokaisen saatavilla. Aktiivi informaatiovelvoite tarkoittaa, että rekisterinpitäjän tulee aktiivisesti ja oma-aloitteistesti informoida rekisteröityä tai asiakasta henkilötietojen käsittelyn keskeisistä seikoista ja hänen oikeuksistaan rekisteröitynä. (Heiliö ym. 2006, 696.)

Rekisterinpitäjällä voidaan tarkoittaa yhtä tai useampaa henkilöä, laitosta tai säätiötä, jonka käyttöä varten perustetaan henkilörekisteri ja jolla on oikeus käyttää tätä

rekisteriä. Rekisterinpitäjiä terveydenhuollossa voivat olla terveyskeskukset, erikoissairaanhoidon yksikkö tai sairaanhoitopiirin kuntayhtymä, yksityinen lääkäriasema tai hammaslääkäriasema ja itsenäisenä ammatinharjoittajana toimiva lääkäri tai hammaslääkäri tai muu terveydenhuollon ammattihenkilö. (Ylipartanen 2004, 43—44.)

4.3 Tietosuojavastaava

Useat eri lait edellyttävät, että sosiaali- ja terveydenhuollossa tulee toimia tietosuojavastaava. Tällaisia lakeja ovat henkilötietolaki (523/1999), laki viranomaisten toiminnasta julkisuudessa (621/1999) ja laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/207). Näissä laeissa on lisäksi salassapitosäännöksiä. (Hyvä tietää -julkaisu 2008, 2)

Tietosuojavastaavan nimeäminen on kuulunut sosiaali- ja terveydenhuollon lakisääteisiin tehtäviin jo 1.7.2007 lukien. Noin vuoden kuluttua eli kesällä 2008 kuitenkin vain 57 % organisaatioista oli nimennyt tehdyn kyselyn mukaan tietosuojavastaavan. (Kinnunen 2008.)

Tietosuojavastaavan toimenkuva

Tietosuojavastaavan tehtävänä on sosiaali- ja terveystoimen yksikön erikoisasiantuntijana antaa yksikön henkilökunnalle ja itse organisaatiolle asiantuntija-apua. Tällaisia asioita ovat mm. hyvä henkilötietojen käsittelytapa ja lakien edellyttämä korkea tietosuojan taso, jonka avulla voidaan rakentaa luottamus eri toimijoiden ja asiakkaiden välille. (Hyvä tietää -julkaisu 2008, 2.)

Seuraavassa luettelossa on esitetty tietosuojavastaavan tehtävät tyhjentävästi:

Tätä rekisterinpitäjän toimintaa tukevaa tarkoitusta varten, tietosuojavastaava

- *osallistuu organisaation henkilötietojen käsittelyä koskevaan suunnittelutoimintaan,*
- *osallistuu rekisterinpitäjän hyväksymiä tietosuoja- ja tietoturvaohjeita koskevaan valmisteluun ja ylläpitoon,*
- *seuraa ja valvoo henkilötietojen käsittelyä ja niiden suojausmenetelmiä,*

- *osallistuu rekisterinpitäjän henkilöstölle annettavan tietosuojakoulutuksen toteuttamiseen,*
- *tukee henkilökuntaa ja rekisteröityjä tietosuoja-asioissa,*
- *toimii yhdyssiteenä valvontaviranomaisiin,*
- *raportoi organisaation johdolle tietosuojan (ja tietoturvallisuuden) tilasta ja kehittämistarpeista (sisäiset auditoinnit ja käytönvalvonta),*
- *vastaa organisaation johdon osoittamista muista tietosuojaa tukevista tehtävistä.*

(Hyvä tietää -julkaisu 2008, 3.)

Tietosuojavastaavan asema

Tietosuojavastaava voi toimia usean organisaation yhteisenä toimijana. Lainsäädäntö ei tätä kiellä. Näin meneteltäessä on kuitenkin huolehdittava siitä, että tietosuojavastaavalla on mahdollisuudet hoitaa tätä tehtävää. Ongelmakohtia laajassa tehtävänkuvassa voivat olla tosiasialliset vaikutusmahdollisuudet ja mahdollisuudet perehtyä eri organisaatioiden henkilötietojen käsittelyyn käytännössä sekä todelliset mahdollisuudet toimia yhteistyössä eri organisaatioiden johdon ja henkilöstön apuna. (Hyvä tietää -julkaisu 2008, 3.)

4.4 Tietoturva käytännössä

Tietoturvassa on aina huomioitava potilaan oikeuksien ja rekisterinpitäjän velvollisuuksien toteuttaminen käytännössä. Arkaluonteisten tietojen käsittelyyn, suojaamiseen ja hävittämiseen on kiinnitettävä aina erityistä huomiota. Nämä asiat ovat rekisterinpitäjän vastuulla. Salassa pidettävien asiakirjojen käsittely on suunniteltava ja toteutettava niin, että ulkopuoliset eivät missään tilanteessa saa niistä tietoa. Myös samassa yksikössä oleva työntekijä, joka ei käsittele kyseisiä tietoja työssään, on sivullinen. (Heiliö ym. 2006, 662–663.)

Asiakirjojen ja niihin sisältyvien tietojen suoja, eheys ja laatu on rekisterinpitäjän toimesta turvattava asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin. Turvallisuuskysymyksissä on huomioitava myös tietojen merkitys ja käyttötarkoitus. Rekisterinpitäjän on etukäteen selvitettävä tietoaineistoonsa sisältyvien tietojen saa-

tavuus, käytettävyys ja laadun merkitys sekä tietojärjestelmään kohdistuva uhkatekijät ja turvallisuustoimenpiteistä aiheutuvat kustannukset. Asiakirjat on muodostettava rekisterinpitäjän toimesta rakenteellisesti sellaisiksi kokonaisuuksiksi, että tietoja ei joudu luvatta ulkopuolisille. Tässä toteutuu hyvä tietohallintatapa. Tällä tavoin varmistutaan myös siitä, että vain ne työntekijät, jotka osallistuvat asiakkaan palveluun, saavat tehtäviensä kannalta tarpeelliset asiakastiedot. Erityisen tärkeää on varmistaa, ettei talletettuja asiakastietoja voi ilman asianmukaista ja kontrolloitua järjestelmää muuttaa. (Heiliö ym. 2006, 663.)

Tietosuojaohjeiden laatiminen, niiden ajan tasalla pitäminen, ohjeiden noudattamisen valvonta ja henkilöstön kouluttaminen on syytä ottaa osaksi työnantajan laatujärjestelmää. Seuraavia teknisiä ja organisaatioon liittyviä määräyksiä voi työnantaja antaa henkilötietojen käsittelyssä:

- Kouluttaa ja ohjeistaa työntekijät tietosuoja-asioissa.
- Antaa kullekin työntekijälle määritellyt käyttöoikeudet niihin henkilörekisteritietoihin, jotka ovat työn hoidon kannalta tarpeellisia.
- Kun työntekijän palvelussuhde päättyy, hänen käyttöoikeutensa asiakastietoihin poistetaan.
- Työtehtävien muuttuessa työntekijän entiset käyttöoikeudet tulee poistaa ja antaa tarvittaessa uuden tehtävän vaatimat oikeudet.
- Antaa henkilökohtaiset salasanat ja käyttäjätunnukset.
- Luo menettelytavat, joilla seurataan tietojen käsittelyä.
- Jos tietokoneesta, jolla asiakastiedot ovat, on Internet-yhteys, tulee järjestelmään rakentaa niin tehokkaat suojaukset, etteivät ulkopuoliset pääse asiakastietoihin käsiksi.
- Pitää huoli siitä, että hyviä henkilötietojen käsittelytapoja noudatetaan ja annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan. (Heiliö ym. 2006, 663–664.)

Tietojärjestelmiin ja tietoverkon laitteisiin tallentuvat lokitiedot järjestelmien käytöstä. Näitä tietoja käytetään järjestelmien ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Lokitiedostoja voidaan tarkastaa asiakkaan pyynnöstä, säännönmukaisessa seurannassa ja myös väärinkäyttöepäilysten yhteydessä. Säännönmukaisten tarkastusten tavoitteena on varmistaa henkilötietolain ja potilaan asemasta ja oikeuksista annetun lain noudattaminen. (Witick & Meriläinen 2009, 6.)

Tietoturvallisuudesta huolehtiminen ja siihen liittyvä osaaminen on jokaisen työyksikössä ja organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden ongelmat liittyvät yleiseen kiireeseen, huolimattomuuteen, osaamattomuuteen ja muihin tietojärjestelmän käytön laadullisiin tekijöihin. Puutteellinen tietoturvallisuus vaarantaa yhteisöjen ja ennen kaikkea asiakkaiden etuja ja aiheuttaa myös lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta. (Witick & Meriläinen 2009, 4.)

Esimerkkeinä tietoturvan murtumisesta ovat seuraavat kaksi erimerkkiä:

- Espoossa Karakallion neuvolassa työskennellyt terveydenhoitaja tuomittiin sakkoihin vuonna 2006 kollegansa terveystietojen urkkimisesta. Tuomio tuli henkilörekisteririkoksesta.

- Useat poliisit olivat käyneet perusteetta tutkimassa Myyrmannin pommin räjäyttäjän henkilötietoja, vaikka he eivät olleetkaan tapausta tutkimassa. Poliisi sai keväällä 2003 huomautuksen asiasta.

Näistä on uutisoitu lehdissäkin. (Nikkilä 2009.)

5 TUTKIMUKSEN TOTEUTUS

Opinnäytetyön yhteydessä tehtiin tutkimus Hankasalmen sosiaali- ja terveystoimessa. Siinä kartoitettiin henkilöstön tietämystä tietoturvasta. Tutkimus suoritettiin kyselytutkimuksena Webropol-ohjelmistoa käyttäen ja kysely lähetettiin 152 työntekijälle. Tutkimus oli jaettu kahteen osioon: yleiset tietoturvakysymykset ja Effica-tietojärjestelmää käyttävien kysymykset. Tässä yhteydessä haluttiin kartoittaa myös niiden henkilöiden tietoturvan tasoa, jotka eivät käytä potilastietojärjestelmää, mutta joita lain edellyttämät tietojen salassapitovelvoitteet koskevat. Tässä luvussa esitellään, mistä kysymykset saatiin, mitä ja miten tutkittiin, ja myös yhteenveto tutkimuksesta.

5.1 Kysymykset

Kysymykset ensimmäiseen osioon otettiin Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskuksen tutkijan Tero Tammisalon laajasta koulutusmateriaalista. Hän oli tehnyt nimenomaan sosiaali- ja terveystoimen henkilöstölle suunnatun kyselyn, jota pienen kunnan sosiaali- ja terveystoimeen soveltuvin osin käytettiin tässä tutkimuksessa. Effica-tietojärjestelmästä tehdyt kysymykset saatiin Etelä-Pohjanmaan sairaanhoitopiirin lakimies Johanna Sorvettulalta. Hän oli tehnyt kyselyn omassa organisaatiossaan ja tätä kyselyä muutettiin vain vähän terveyskeskukseen, kotihoitoon ja palveluasumiseen sopivaksi. Tarkoituksena on jatkossa tässä työssä vertailla kahden eri yksikön tietoturvan tasoa. (Tammisalo 2007, 54; Sorvettula 2009.)

5.2 Mitä tutkittiin

Laki edellyttää erittäin laajan tietosuojatason sosiaali- ja terveystoimessa. Tutkimuskysymykset on suunniteltu siten, että mahdollinen tietämyksen tason puute saadaan selville ja koulutuksen ja tiedottamisen avulla saadaan asia lain edellyttämälle tasolle.

Yleisissä kysymyksissä kartoitettiin henkilöstön salasanatietämystä, sähköpostin käyttöä ja virustorjuntaan liittyviä asioita. Tietojärjestelmäosiossa kyseltiin aivan arkipäivän menettelytapoja eri tilanteissa, kuten hoitotietojen luovuttamiseen, katseluun ja yleiseen käyttäytymiseen liittyviä kysymyksiä. Tutkimus koettiin henkilöstön keskuudessa erittäin tarpeelliseksi. Lähes puolessa vastauksista oli tästä maininta.

5.3 Miten tutkittiin

Kysymykset lähetettiin sähköpostitse ja myös pyydettäessä paperiversioina eri yksiköihin. Sähköpostissa oli suora linkki Webropol-ohjelmaan. Kaikilla työntekijöillä ei ole kunnan sähköpostiosoitetta, joten paperivastausmahdollisuus täytyi antaa. Sähköposteja lähetettiin 102 kpl ja paperisia vastauslomakkeita jokaiseen yksikköön. Tutkimus toteutettiin kolmen viikon aikana maaliskuussa 2010. Toisen ja kolmannen viikon lopussa lähetettiin muistutusviesti vastaamisesta.

Tämä tutkimus oli ensimmäinen tietoturvatason mittaus Hankasalmen sosiaali- ja terveystoimessa. Tutkimuksen alussa oli ohje siitä, millä tavalla tutkimukseen piti suhtautua. Siinä oli maininta, että on hyvä vastata oman tuntemuksen mukaan. Miten toimit? Tämä oli tarpeen siksi, että kukaan ei olisi kokenut tutkimusta liian vaikeaksi. Tutkimuksessa tähdennettiin nimenomaan sitä, mikä käsitys henkilöstöllä tällä hetkellä kysytyistä asioista on. Kyselyssä sallittiin myös vastaamatta jättäminen niihin kysymyksiin, jotka tuntuivat henkilöstölle liian vaikeilta. Arvata ei tarvinnut. Taustatietoina kyselyssä kysyttiin ikää ja toimipaikkaa. Toimipaikka oli tärkeä selvittää tulevan koulutuksen takia. Ohjelmisto mahdollistaa vastausten seulonnan työyksiköittäin. Koulutusta kyselyyn pohjautuen tullaan järjestämään jo tämän kevään aikana eri työyksikköpalavereissa.

5.4 Tutkimusvastukset

Tutkimus jakautuu siis kahteen osioon, yleiset tietoturvakysymykset, joihin vastasivat kaikki, ja Effica-osio, johon vastasivat vain tätä tietojärjestelmää käyttävät. Vastausten arviointi perustuu Tero Tammisalon tutkimuksessaan antamiin vastauksiin. Osas-

sa kysymyksistä on maininta, että organisaatiokohtaisesti voidaan poiketa Stakesin suosituksesta. Jos organisaatiossa on käytössä jokin muu mahdollinen käytäntö tai mahdollinen laitteisto tai ohjelma asettaa rajoituksia suosituksiin, vastaukset voidaan hyväksyä näiden mukaisena. Tietojärjestelmäosuuden vastausvaihtoehtojen selvitys on pääosin Sorvettulan antamien valmiiden vastausten mukainen. Vastausten selostukseen lisättiin lainkohdat, joihin vastaukset perustuivat.

Seuraavassa on esitetty vastausten määrä toimipaikoittain taulukkomuodossa:

TAULUKKO 1. Vastausten määrä toimipaikoittain

Työyksikkö	Henkilöstö	Vastausten määrä	Vastaus- %
Avoterveydenhuolto	25	20	80
Terveyskeskussairaala	35	28	80
Kotihoito	27,5	15	55
Palvelukoti Päiväranta	20	10	50
Palvelukoti Metsätähti	4	2	50
Muut yksiköt	41	22	54
Yhteensä	152	97	64

Yllä olevassa taulukossa vastaukset kerrotaan työyksiköittäin. Ensimmäisessä sarakkeessa on työyksiköt, toisessa se henkilöstömäärä, jolle kysely lähetettiin. Vastausten määrä sarakkeessa on näistä yksiköistä saadut kappalemääräiset vastaukset ja viimeinen sarake kertoo vastausprosentit. Muut yksiköt kohtaan kuuluvat sosiaali- ja terveystoimen hallinto, mielenterveystyö ja hammashuolto sekä sosiaalitoimesta päiväkodit. Terveydenhuollon yksiköitä ovat avoterveydenhuolto ja terveyskeskussairaala ja sosiaalitoimen yksiköitä ovat kotihoito, Palvelukoti Päiväranta ja Palvelukoti Metsätähti.

6 TUTKIMUKSEN TULOKSET

Tässä luvussa käsitellään tutkimuksen tulokset, ensin Yleiset tietoturvakysymykset, johon kaikki vastaajat vastasivat, ja sen jälkeen Effica-tietojärjestelmää koskevat kysymykset, johon vastasivat tätä järjestelmää käyttävät. Ensimmäisen ryhmän kysymykset olivat pääosin monivalintoja, joista yksi tai useampi oli oikein. Effica-osion kysymykset olivat suurelta osin oikein väärin -valinnalla tehtyjä.

Yleisenä huomiona voidaan todeta tästä kyselyssä, että tietoutta tietoturvasta tulee lisätä koulutuksen ja muun tiedotuksen avulla. Useisiin kysymyksiin eivät kaikki olleet vastanneet lainkaan ja oli myös suhteellisen paljon puutteellisia ja lähinnä Effica-osion kysymyksissä väärin valittuja vastauksia. Tietoturvaopas tulee myös palvelemaan näiden ongelmien ratkaisuissa.

6.1 Yleiset tietoturvakysymykset

6.1.1 Salasana

Aluksi käsitellään sanasanojen problematiikkaa. Miten pitkä salasanan tulee olla, millainen sen tulee olla muodoltaan, mihin salasanan voi laittaa muistiin, milloin se täytyy vaihtaa ja vielä salasanan käyttöön liittyvä kysymys.

1 Mikä seuraavista on vähimmäisvaatimus hyvälle salasanalle?

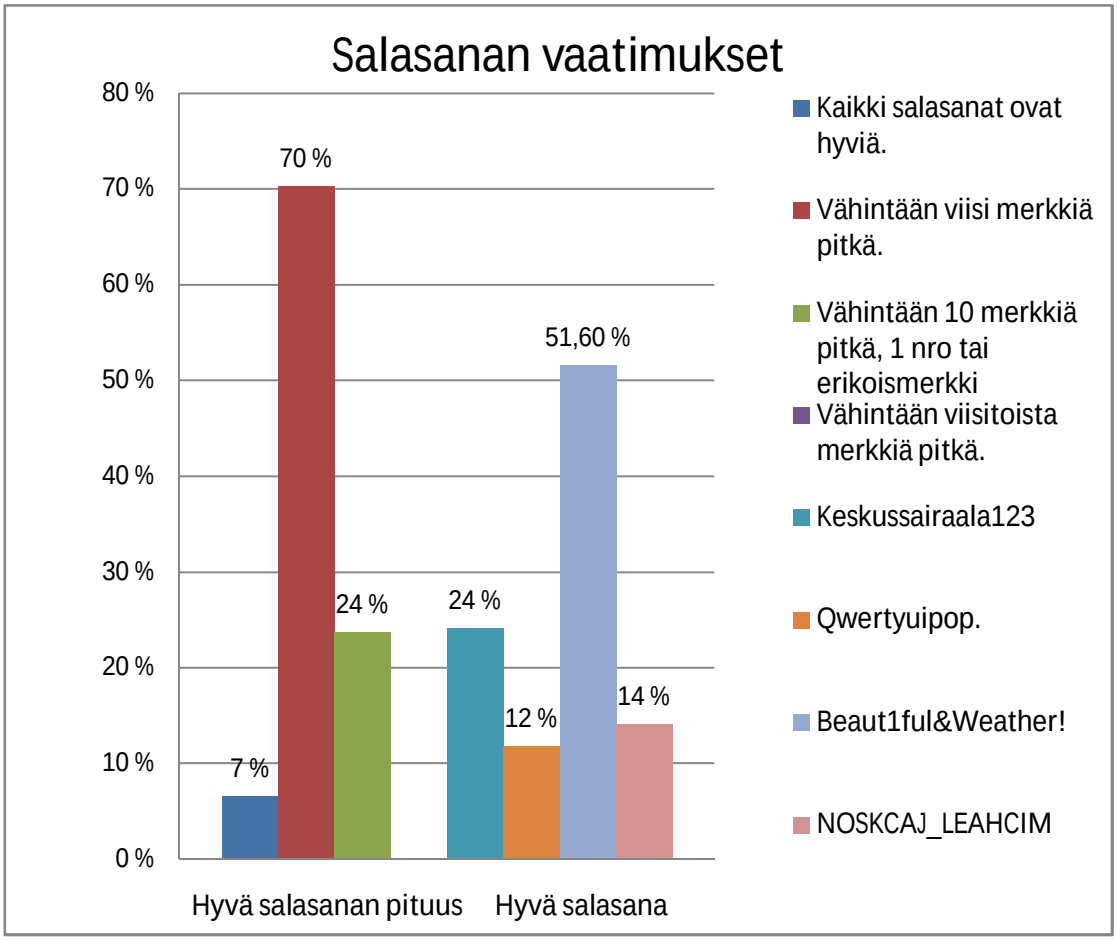
2 Mikä seuraavista on laadukas salasana?

Ensimmäiseen näistä kysymyksistä vastasi 91 työntekijää eli kaikki kyselyyn vastanneista ja toiseen kysymykseen 85 työntekijää. Hajontaa oli jonkin verran salasanan pituuden määrityksessä. Vastaukseen vaikutti Effica-tietojärjestelmän viiden merkin vaatimus, kuten seuraavalla sivulla olevasta taulukosta ilmenee.

Yleinen vaatimus salasanalle on vähintään kymmenen merkin pituus ja siinä täytyy olla yksi numero tai erikoismerkki. Siinä tulee olla myös isoja ja pieniä kirjaimia. Koska salasanan täytyy olla sellainen, että se voidaan muistaa, viidentoista merkin sala-

sana on liian pitkä. Samoin ensimmäinen vaihtoehto, että mikä tahansa salasana on hyvä, on väärä.

Kyselyssä olleet salasanat olisivat monelle työntekijälle vaikeita muistaa käytännössä, koska kolme viimeistä oli vieraskielisiä tai vain kirjaimia peräkkäin.



KUVIO 1. Salasanan vähimmäisvaatimukset (N= I 91 ja II 85)

Kuviossa toisena asiana kuvattiin käytännön salasanavaihtoehtoja. Edellä olleen määritelmän mukaan ensimmäinen vaihtoehto Keskussairaala123 on aivan liian helposti arvattavissa. Kuitenkin yli 24 % eli 22 vastaajaa piti tätä vaihtoehtoa hyvänä. Laadukkain luetelluista salasanoista on kolmas vaihtoehto eli Beaut1ful& Weather!. Siinä on vaadittavia isoja ja pieniä kirjaimia ja mukaan mahtuu myös pari erikoismerkkiä ja numerokin. Lisäksi tämä salasana on helppo muistaa. Ehkäpä se olisi saanut vielä enemmän kannatusta, jos se olisi ollut Kaunis&Ilma!. Oli kuitenkin hyvä, että se sai

eniten kannatusta kyselyssä. Kaksi muuta vaihtoehtoa ovat kyllä vaikeita arvata, mutta niissä ei kummassakaan ole laadukkaan salasanan ominaisuuksia.

Laadukkaiden ja helposti muistettavien salasanojen löytäminen jokaiseen ohjelmaan voi joskus tuntua työläältä. Salasana ei saa olla liian vaikea muistettavaksi, mutta kuitenkin liian vaikea arvattavaksi.

Edellä olevien lisäksi kysyttiin kolme kysymystä salasanasta. Kysymykset ja vastaukset avataan kappaleina ja prosentteina kokonaisvastausten määrästä:

3 Sinun kuuluu vaihtaa salasanasi etenkin

- kun epäilet, että salasanasi on paljastunut (63 kpl, 65 %)
- kun järjestelmä käskee (62 kpl, 64 %)
- kerran kuukaudessa, esimerkiksi 1. arkipäivä (12 kpl, 12 %)
- kun kollegasi pyytää sinua vaihtamaan salasanasi (2kpl, 2 %).

Salasana on vaihdettava aina, kun on epäilys sen paljastumisesta. Samoin joihinkin järjestelmiin on ohjelmoitu salasanan vaihtoväli. Potilastietojärjestelmässä salasana edellytetään vaihdettavaksi noin kuukauden välein. Tämän takia vastaukset oli useimmiten laitettu kahteen ensimmäiseen vaihtoehtoon. Vapaaehtoinen vaihtaminen kerran kuukaudessa ei sekään ole väärä vastaus, mutta jos se on jossain organisaatiossa käytössä ja se ennakolta tiedetään, voi salasanan vaihto luoda pienen väärinkäytön mahdollisuuden. Ainoa erheellinen käsitys on vain noin kahdella prosentilla vastaajista. Tämä on ehdottoman väärin ja tästä tulee ilmoittaa jopa Tietohallintoyksikköön ja tätä voidaan verrata myös ensimmäiseen vaihtoehtoon.

4 Taataksesi, että muistat salasanasi, etkä hukkaa niitä voit

- kirjoittaa salasanasi paperille (42 kpl, 51 %)
- säilyttää salasanoja tiedostossa koneellasi (4 kpl, 5 %)
- säilyttää salasanojasi matkapuhelimesi muistissa (37 kpl, 45 %)

- vaihtaa salasanasi lähimmän kollegasi kanssa (0 kpl, 0 %).

Tähän kysymykseen sisältyi kompa. Kuten yllä olevasta ilmenee, tähän kysymykseen vastasi 82 työntekijää. Vastaamatta jättäneiden vastaus oli oikea. Salasanan on säilytettävä vain jokaisen työntekijän muistissa. Toinen positiivinen asia tässä on se, että kukaan ei ole valmis kertomaan salasanaansa kellekään.

On ensiarvoisen tärkeää saada tietojärjestelmien käyttäjät havaitsemaan vaarat. Henkilön oma oikeusturva on uhattuna, jos joku ulkopuolinen pääsee kyseessä olevan henkilön tunnuksilla tietojärjestelmään. Henkilö itse vastaa siitä, että salasana on sellainen, että vain hän itse tietää sen ja muilla ei ole mahdollisuutta sitä selvittää.

5 On hyvä

- käyttää samaa salasanaa sekä koti- että työsähköpostissa, jotta ne on helpompi muistaa (6 kpl, 6 %)
- käyttää salasanaa, jota sivullisen on vaikea arvata (86 kpl, 91 %)
- uudelleen käyttää hyväksi koettuja salasanoja, koska niiden kirjoittaminen on nopeaa (9 kpl, 10 %)
- lähettää salasana tietohallintoyksikköön virheiden välttämiseksi (1 kpl, 1 %).

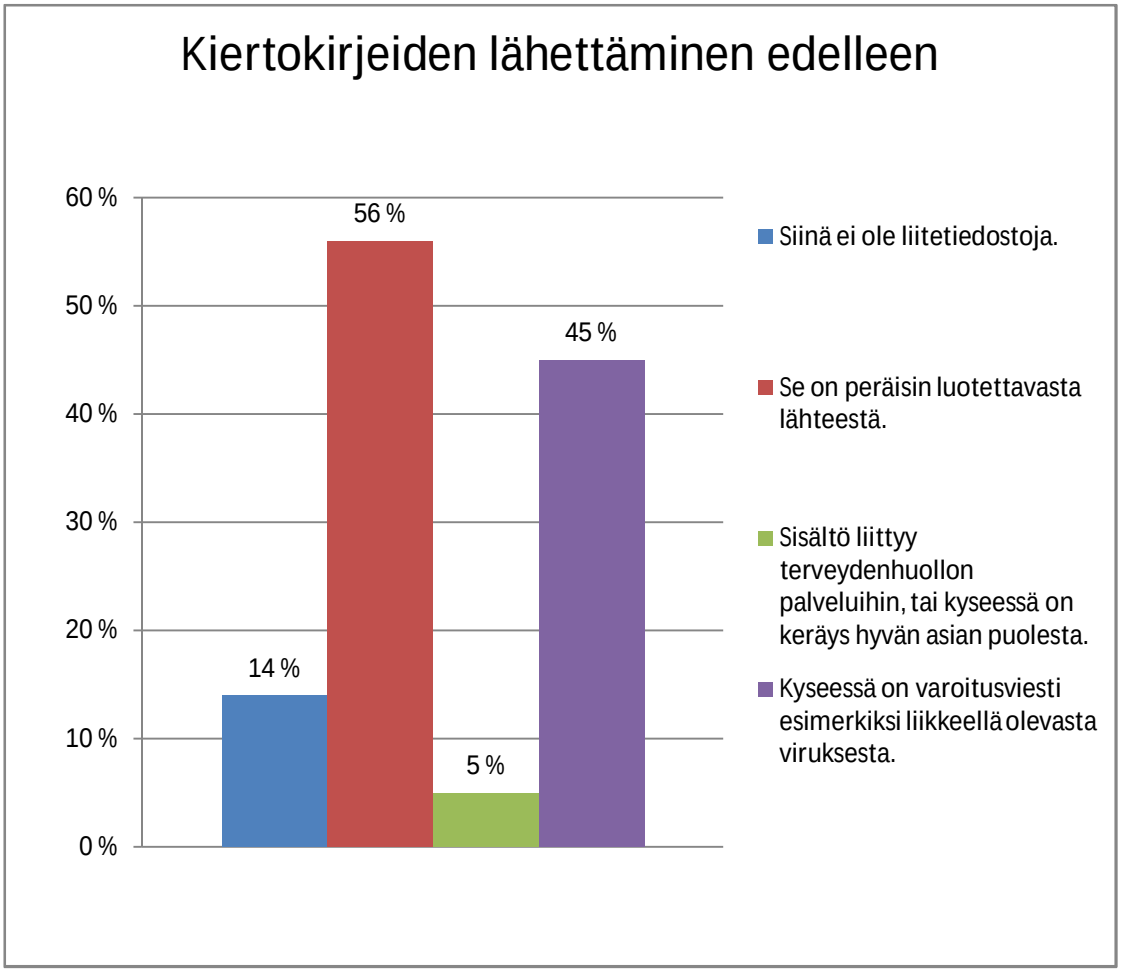
Toinen vaihtoehto tässä kysymyssarjassa oli aivan oikein ja enemmistä vastaajista oli sen tiennyt. Samaa salasanaa ei tule käyttää uudelleen eikä useammassa koneessa, koska näihin molempiin sisältyy tietoturvariski. Saman salasanan käyttö useammassa koneessa on ehdottomasti kiellettyä. Tosin voidaan ajatella, että kohdan kolme vaihtoehto voisi olla käytössä siten, että hyvät salasanat muunneltuina ja tarpeeksi suurella kierrolla vähentävät salasanojen ylös kirjaamista ja edesauttavat sen muistamista.

Tietohallintoyksikkö on samalla tavalla sivullinen osapuoli salasanan suhteen kuin esimerkiksi kollega. Salasanoista on muistettava, että käyttäjätunnus ja salasana = henkilö itse. Työntekijä vastaa, että salasana on sellainen, että vain hän itse sen tietää ja muilla ei ole mahdollisuutta sitä selvittää.

6.1.2 Sähköposti

1 Voin edelleen lähettää kiertokirjeenä kulkevan sähköpostin, jos

Alla -olevassa kuviossa esitetyistä vaihtoehdoista kaikki ovat väärin. Kiertokirjeitä ei tule lähettää missään tapauksessa eteenpäin. Oikeat varoitusviestit esimerkiksi liikkeellä olevasta viruksesta tulevat suoraan siltä taholta organisaatiossa, joka virustorjunnasta vastaa. Kiertokirjeen mukana voi kulkea viruksia, suuria liitetiedostoja, linkkejä arveluttaville sivuille tai yrityksiä saada haltuun organisaatio sisäistä tietoa.



KUVIO 2. Kiertokirjeiden lähettäminen edelleen (N=87)

Tähän kysymykseen vastasi 87 henkilöä, joten kymmenen oli jättänyt vastaamatta ja he olivat oikeassa.

Sähköpostista kysyttiin vielä kaksi muuta väittämää:

2 Mikä seuraavista väittämistä on oikea?

- Voit liittää kollegasi sähköpostiosoitteen postituslistalle, jossa käsitellään asioita, jotka auttavat kollegaasi hänen työtehtäviensä hoidossa, vastauksia tähän vaihtoehtoon (43 kpl, 49 %) vastaajista.

- Voit tallentaa sähköpostissa saamasi liitetiedoston oman tietokoneesi kovalevylle, vastauksia tähän (48 kpl, 55 %) vastaajista.

- Voit vaihtaa henkilökohtaisen tunnuksesi ja salasanasi lähimmän kollegasi kanssa hänen vastaavaan tunnukseensa ja salasanaansa, jotta voitte toimia toistenne varahenkilöinä, vastauksia (1 kpl, 1 %).

Näistä kolmesta vaihtoehdosta vain toinen vaihtoehto on oikea. Joissakin organisaatioissa liitetiedoston tallentaminen omalle kovalevylle voi kuitenkin olla kiellettyä. Ensimmäisessä vaihtoehdossa kysyttäessä on tarkoitettu yleisiä postituslistoja. Jokainen voi toki omassa sähköpostissaan säilyttää kollegojensa osoitteita. Salasanojen vaihtaminen on tietysti kiellettyä, kuten jo edellä selitettiinkin. Se on henkilökohtainen, eikä sitä pidä kertoa kenellekään.

3 Minkä seuraavista väittämistä voit tehdä?

Tähän kysymykseen vastasi 81 henkilöä.

- Voit lähettää sähköpostilla liitetiedostoja välittämättä niiden koosta, koska vastaanottajan sähköpostijärjestelmä huolehtii liian suurien liitetiedostojen oikeanlaisesta käsittelystä, (15 kpl, 18 %) vastaajista valitsi tämän vaihtoehdon.

- Sähköpostiohjelmistoissa löytyy ominaisuus, jonka avulla voit lähettää sähköpostiviestin useille henkilöille yhtä aikaa ilman, että vastaanottajat näkevät toistensa sähköpostiosoitteet, vastauksia tähän väittämään (65 kpl, 80 %).

- Voit pitää rajattoman määrän sähköpostiviestejä sähköpostipalvelimellasi. Väittämän valitsi 4 työntekijää, joka on 5 % vastauksista.

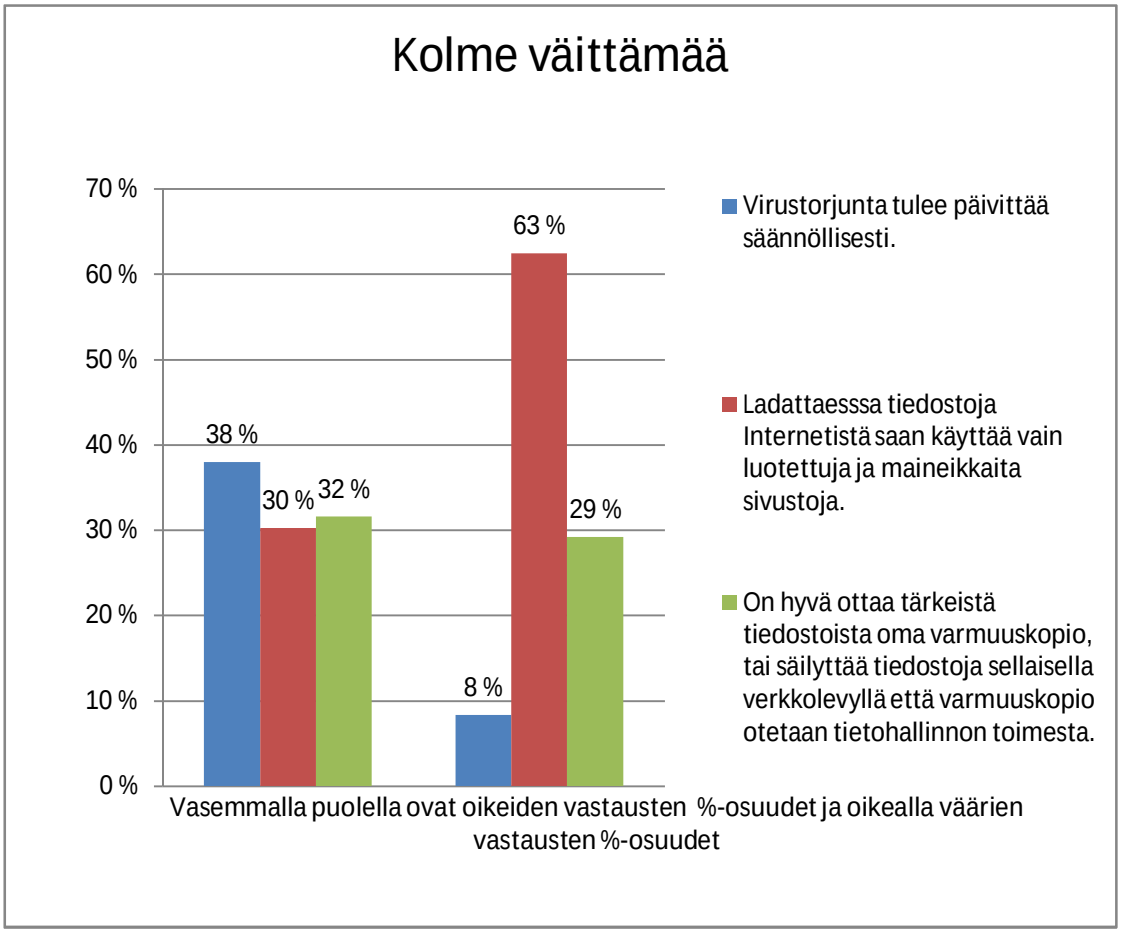
Esitetyistä vaihtoehdoista toinen väittämä on oikein. Voidaan käyttää esimerkiksi piilokopiokenttää sähköpostiositteiden salaamiseen lähetettäessä usealle henkilölle viestiä. Ensimmäinen kohta on väärin, koska henkilön pitää kiinnittää huomiota lähettämiinsä liitetiedostoihin, sillä ne voivat olla korkeintaan muutaman megatavun mittaisia. Viimeinen väittämä on myös väärin, koska viestit pitää tallentaa verkkolevylle, josta otetaan säännölliset varmuuskopiot.

Tämä kysymys oli ehkä hieman vaikea, koska vastaajia oli vain 81. Kuitenkin positiivinen asia on, että moni tiesi oikean vaihtoehdon.

6.1.3 Yleisiä tietoturvakysymyksiä

1 Mitkä seuraavista väittämistä ovat oikein tai väärin?

Seuraavassa kuviossa kuvataan kolmea erilaista väittämää.



KUVIO 3. Kolme väittämää (N=96)

Edellä olevan kuvion kaikki annetut väittämät ovat oikein. Tosin joissakin organisaatioissa voi olla kokonaan kielletty tietojen lataaminen Internetistä. Väärät vastaukset tässä kyselyssä johtuvat todennäköisesti siitä, että virustorjunta päivitetään tietohallinnon toimesta ja näin työntekijöiden ei siitä tarvitse huolehtia. Samoin varmuuskopioiden ottaminen tuntuu osasta turhalta sen takia, että varmuuskopiot verkkolevylle tallennettaessa otetaan samoin tietohallinnon toimesta. Vastaajia tähän kysymykseen tai sen osaan oli 96.

Tässä osiossa käsitellään vielä kahdessa seuraavassa kysymyksessä jokapäiväistä tietojenkäsittelyyn kuuluvaa tietoutta. Kysymykset on laadittu oikein väärin -vaihtoehdoilla. Tarkoitus oli, että jokaiseen vaihtoehtoon tulisi jompikumpi vaihtoehdoista. Ilmeisesti näiden kysymysten osalta on kaikkein eniten tietämättömyyttä henkilökunnan keskuudessa.

2 Kuka on vastuussa tietoturvan toteutumisesta toimintayksikössäni?

Kaikki seuraavat vaihtoehdot ovat oikeita.

- Toimintayksikön johtaja, (oikein 56 kpl eli väärin 5 kpl),
- Kaikki esimiesasemassa olevat, (oikein 49 kpl väärin 9 kpl),
- Tietohallintoyksikkö, (oikein 54 kpl väärin 3 kpl),
- Tietosuojavastaava, (oikein 61 kpl väärin 2 kpl),
- Jokainen työntekijä, (oikein 86 kpl väärin 4 kpl).

Tähän kysymykseen vastasi 93 henkilöä. Monessa lomakkeessa oli vastattu vain viimeiseen vaihtoehtoon ja se riittää oikeaksi vastaukseksi. Kaikki edellä mainitut tahot ovat myös työntekijöitä, niin tietohallintoyksikössä työskentelevät kuin esimiehetkin.

Vastauksista noinkin runsas väärien vaihtoehtojen määrä antaa jälleen aiheen tietoturvan tason nostoon. Varsinkin käsitys siitä, että jokainen työntekijä ei olisi vastuussa tietoturvan toteutumisesta.

3 Valitse seuraavista tietoturvapolitiikkaa koskevista ohjeista oikea/oikeat ja väärä/väärät

Suurin osa vastaajista löysi oikean vaihtoehdon eli kohdan kolme.

- Tietoturvapolitiikka on tietohallinnon käyttöön tarkoitettu ohje, (oikein 49 kpl väärin 26 kpl).
- Tietoturvapolitiikka sisältää päivittäisiä tietoturvaohjeita järjestelmien vastuuhenkilöille, (oikein 58 kpl väärin 16 kpl).
- Tietoturvapolitiikka on toimintayksikön johdon hyväksymä ja koko toimintayksikön laajuisesti käyttöön määräämä (oikein 75 kpl väärin 4 kpl).
- Voit jättää tietoturvapolitiikan huomiotta, kun on hätätilanne, (oikein 7 kpl väärin 70 kpl).

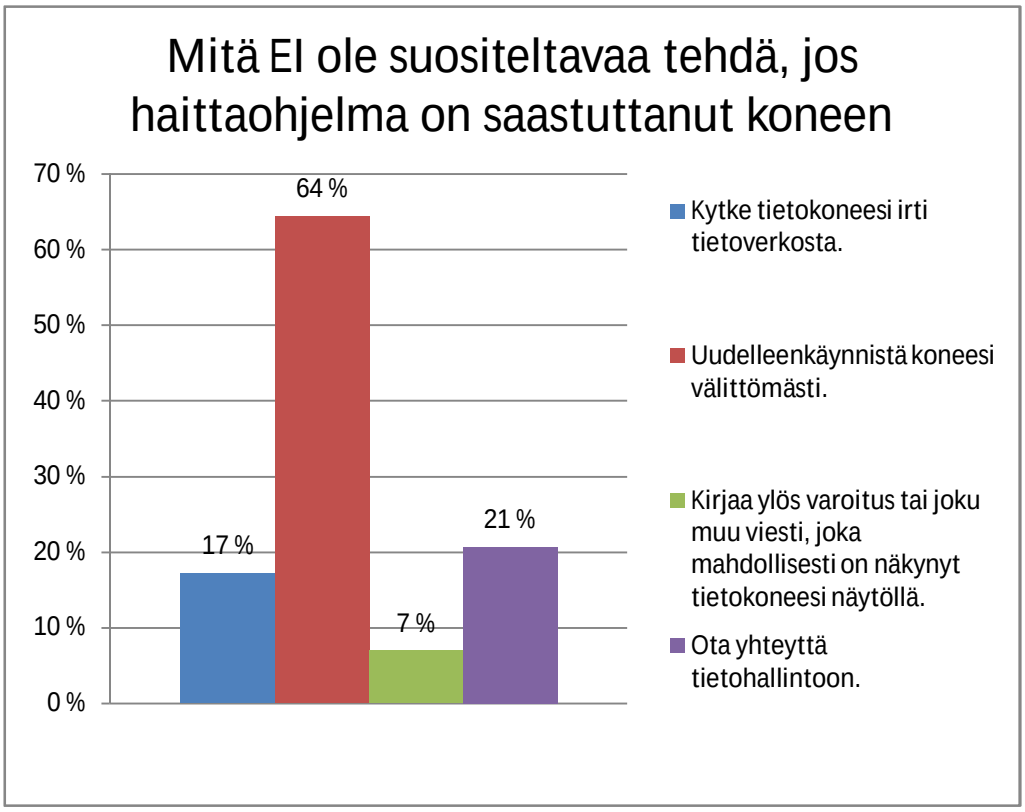
Tämä kysymys oli selvästi yksi vaikeimmista. Siihen vastasi vain 78 työntekijää. Tietoturvapolitiikka on koko organisaation käyttöön tarkoitettu ohje, joten kohta yksi on väärin. Samoin kohta kaksi on väärin, koska tietoturvapolitiikka ei sisällä päivittäisiä ohjeita. Viimeinen kohta on tulkinnanvarainen. Jos on todella iso katastrofi, kuten evakuointi tai potilaan hengen tai terveyden vaarantuminen, ei tietoturvaohjeita tarvitse noudattaa. Tämä ei voi kuitenkaan olla itseisarvo, vaan tietoturvapolitiikan noudattamisen tulee olla pääsääntö. Kaikki nämä kohdat voivat aiheuttaa saivartelua. Varsinkin kohdassa neljä on käytettävä tervettä järkeä ja harkintaa. Tietoturvapolitiikan noudattamatta jättäminen vaatii todellisen hätätapauksen, joka arvioidaan joka kerta erikseen.

6.1.4 Virustorjuntaan liittyvät kysymykset

1 Jos epäilet, että haittaohjelma on saastuttanut tietokoneesi, mitä seuraavista vaihtoehdoista EI ole suositeltavaa tehdä?

Vastauksia tähän kyselyyn tuli 93:lta eri henkilöltä. Neljä vastaajaa ei ollut tähän osannut vastata mitään.

Tätä kysymystä eivät kaikki varmaan lukeneet tarpeeksi tarkasti, koska valittiin vaihtoehdot, että ei saa kytkeä tietokonetta irti verkosta tai ottaa yhteyttä tietohallintoon. Nämä kohdat olisivat voineet olla tyhjät. Oikea vaihtoehto on tietysti, että konetta ei missään tapauksessa saa uudelleen käynnistää, jonka vaihtoehdon 61 vastaajaa oli valinnutkin. Jos tietokone on saastunut, uudelleenkäynnistys ei auta mitään. Päinvastoin jotkut haittaohjelmat saattava käynnistyessään saada uutta puhtia ja saada aikaan lisää haittoja. Jos tietokone on saastunut, tulee siis ensiksi irrottaa kone tietoverkosta mahdollisen haittaohjelman leviämisen estämiseksi. Sitten on otettava mahdolliset viestit ylös ja otettava yhteyttä tietohallintoon. Seuraavassa kuviossa hahmotetaan vielä tätä kysymystä.

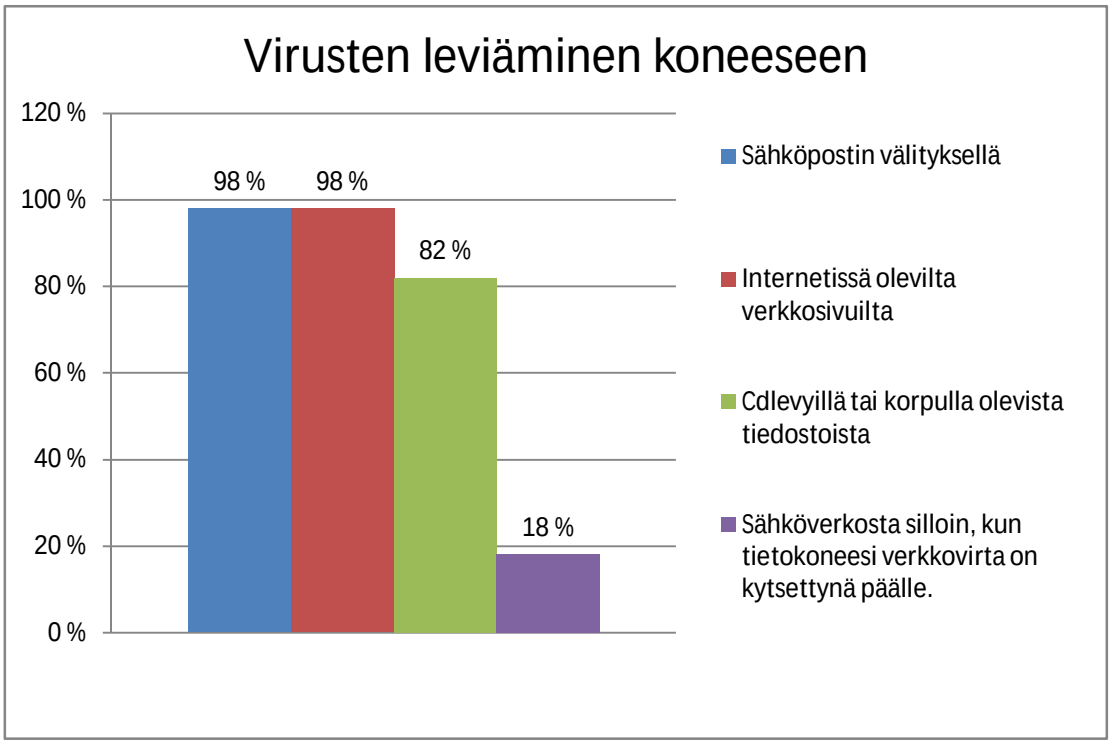


KUVIO 4. Haittaohjelman saastuttama kone (N=93)

2 Valitse seuraavista vaihtoehdoista kaikki oikeat.

Tämän kysymyksen kohdalla kolme ensimmäistä vaihtoehtoa ovat oikein. Kysymykseen oli vastannut 94 työntekijää, joten lähes kaikki ovat tienneet oikeat vaihtoehdot. Myöskään vaihtoehto neljä ei ole väärin, koska nykyteknologia mahdollistaa tie-

donsiirron sähköverkossa ja tällaisen tiedonsiirron ollessa käytössä tietysti myös haittaohjelmat voivat levitä tätä kautta.



KUVIO 5. Neljä tapaa virusten leviämiseen (N=94)

3 Tietokoneesi on virusten saastuttama, jos

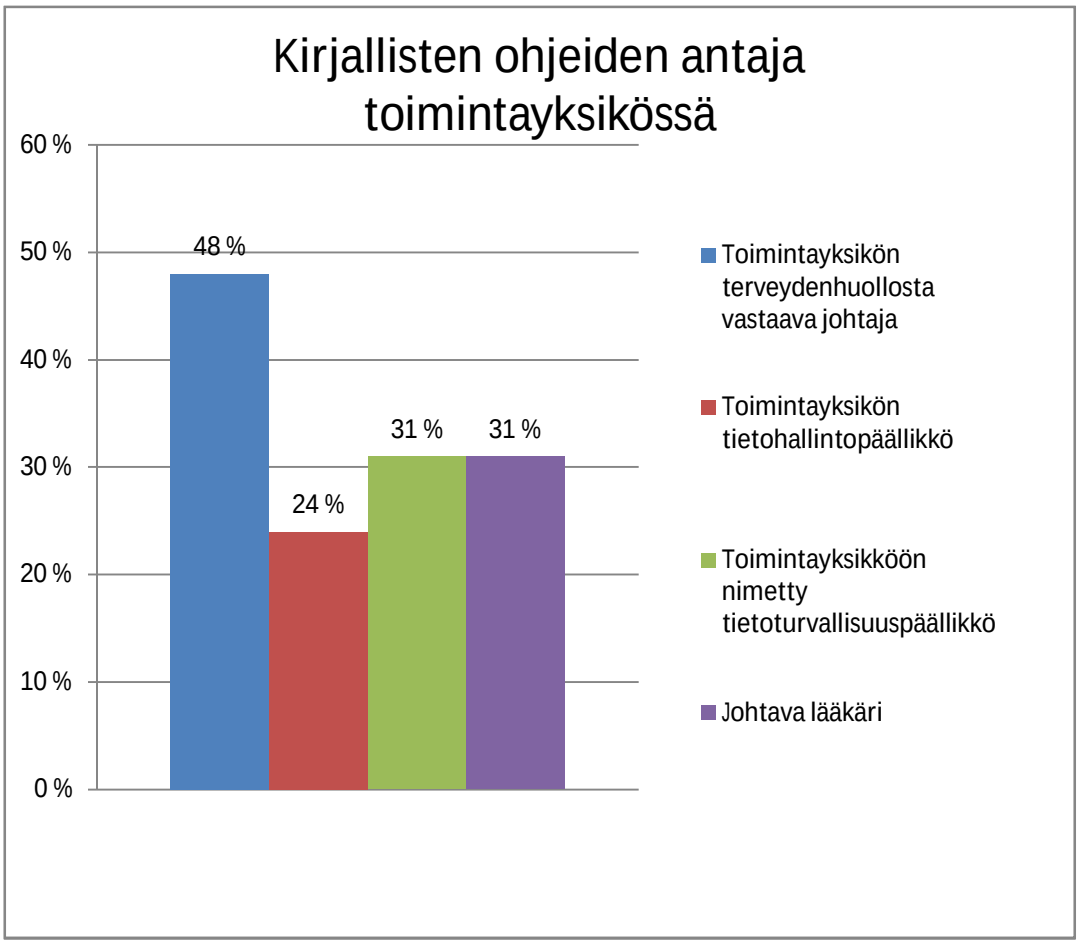
- tiedostojesi sisältö on odottamatta muuttunut, (72 kpl eli 77 %)
- virustorjuntaohjelmisto näyttää hälytysviestin, (88 kpl eli 94 %)
- tietokoneesi toimii normaalia hitaammin, (68 kpl eli 72 %)
- tietokoneesi uudelleen käynnistyy itsekseen ilmoittamatta siitä millään varoitusviestillä, (47 kpl eli 50 %).

Kaikki vaihtoehdot olivat oikein tämän kysymyksen kohdalla.

6.2 Effica-tietojärjestelmään liittyvät kysymykset

Tämän osion kysymyksiin vastasi enimmillään 75 henkilöä. Vastauksittain määrät vaihtelivat jonkin verran. Kysymyksiä on kaikkiaan 25 kpl. Joidenkin kysymysten osalta Hankasalmen tulosta verrataan Etelä-Pohjanmaan sairaanhoitopiiriin vastaavaan tutkimustulokseen. Kuvioissa tästä organisaatiosta käytetään lyhennettä E-P SHP ja tekstissä myös termiä vertailukunta. Kuvioteksteissä ilmoitetaan kappalemäärissä aina ensin Hankasalmen vastausten määrä ja sitten Etelä-Pohjanmaan sairaanhoitopiirin vastausten määrä.

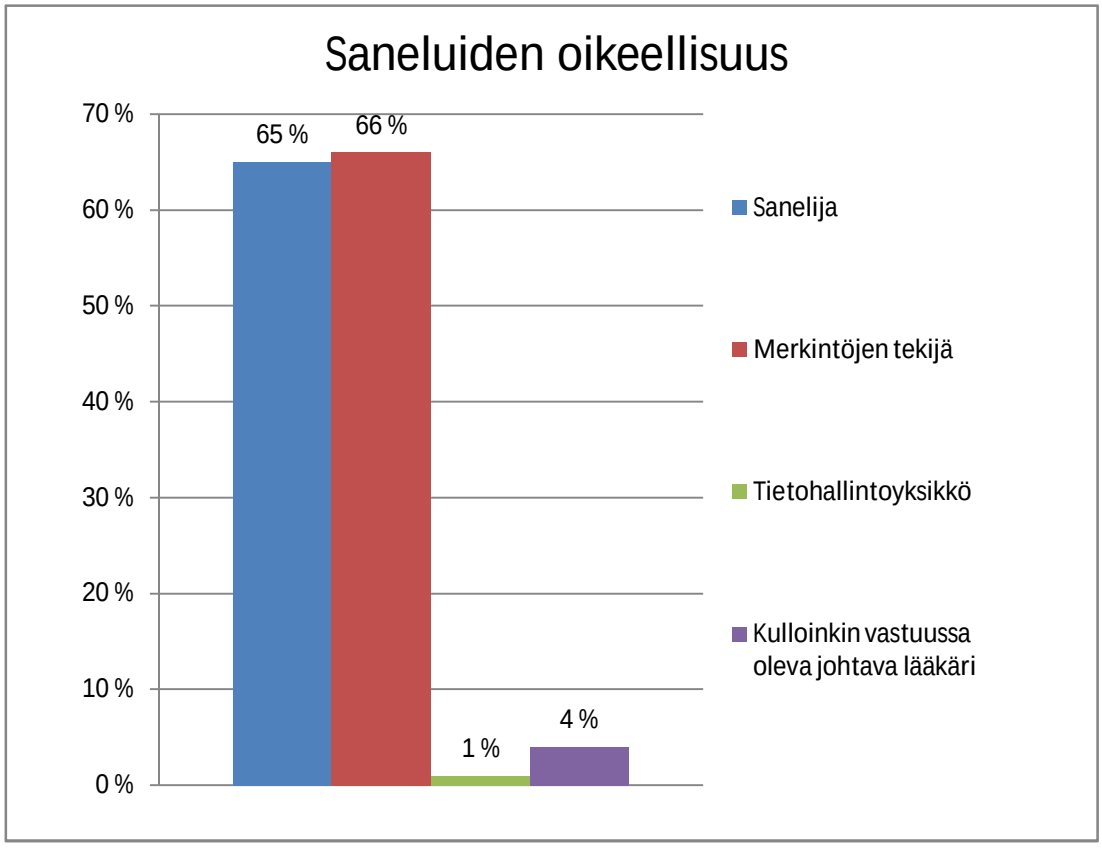
Kysymys 1. Kuka vastaa siitä, että toimintayksikössä on saatavilla kirjalliset ohjeet potilasasiakirjoihin sisältyvien tietojen käsittelystä ja menettelytavoista?



KUVIO 6. Kirjallisten ohjeiden antaja toimintayksikössä (N=62)

Sosiaali- ja terveysministeriön asetuksessa potilasasiakirjojen laatimisesta ja säilyttämisestä todetaan toimintayksikön johtajan toimivan rekisterinpitäjän edustajana. Vaihtoehdot kaksi ja kolme ovat väärin. Viimeinen vaihtoehto on myös oikein tässä kyselyssä, koska jos terveydenhuollosta vastaavana johtajana toimii johtava lääkäri, hän tietysti vastaa myös potilasasiakirjoista. Tämä kysymys oli vaikea ja hajonta oli melkoinen. Vain 62 työntekijää vastasi kysymykseen. Tämä asia on harvoin arjessa esillä.

Kysymys 2: Terveydenhuollon ammattihenkilön sanelun perusteella tehtyjen merkintöjen oikeellisuudesta vastaa:



KUVIO 7. Sanelujen oikeellisuudesta vastaaminen (N=71)

Tämä kysymys oli sellainen, jossa kaksi mielipidettä oli lähes tasoissa. Lukumäärinä ilmaistuna vastaukset olivat: sanelija vastaa oikeellisuudesta 46 ja merkintöjen tekijä vastaa oikeellisuudesta 47 kpl. Käytännössä tämä jää merkintöjen tekijän vastuulle

monta kertaa, mutta oikea vastaus kuitenkin on yksiselitteinen. Sanelija vastaa aina tehtyjen merkintöjen oikeellisuudesta.

Vastauksia tähän kysymykseen tuli 71 kpl.

Kysymys 3. Terveydenhuollon ammattihenkilö ei saa kertoa sivullisille:

- yksikössään hoidossa olevan potilaan nimeä, (73 kpl eli 97 %)
- yksikössään hoidossa olevan potilaan henkilötunnusta, (75 kpl eli 100 %)
- yksikössään hoidossa olevan potilaanterveydentilaan liittyviä seikkoja, (73 kpl eli 97 %)
- yksikössään hoidossa olevan potilaan perheestä ilmi tulleita seikkoja, (74 kpl eli 99 %).

Oikeita vastauksia ovat nämä kaikki ja lähes kaikki vastaajat ovat myös tämän tienneet. Terveyskeskussairaalan vastauksissa oli muutama vastaus, joissa joko nimi voitiin kertoa sivulliselle tai terveydentilasta asioita. Tämä on ymmärrettävää, jos sivulliseksi on ajateltu esimerkiksi puolisoa. Kyllähän omaiselle kerrotaan sairaalasta omaisen hoidossa olosta, ellei potilas sitä erikseen kiellä.

Kysymys 4. Jos henkilö tehtäviä hoitaessaan tai muutoin rikkoo henkilötietojen käsittelystä säädettyjä lakeja tai salassapitovelvoitteita, seuraamukset voivat olla:

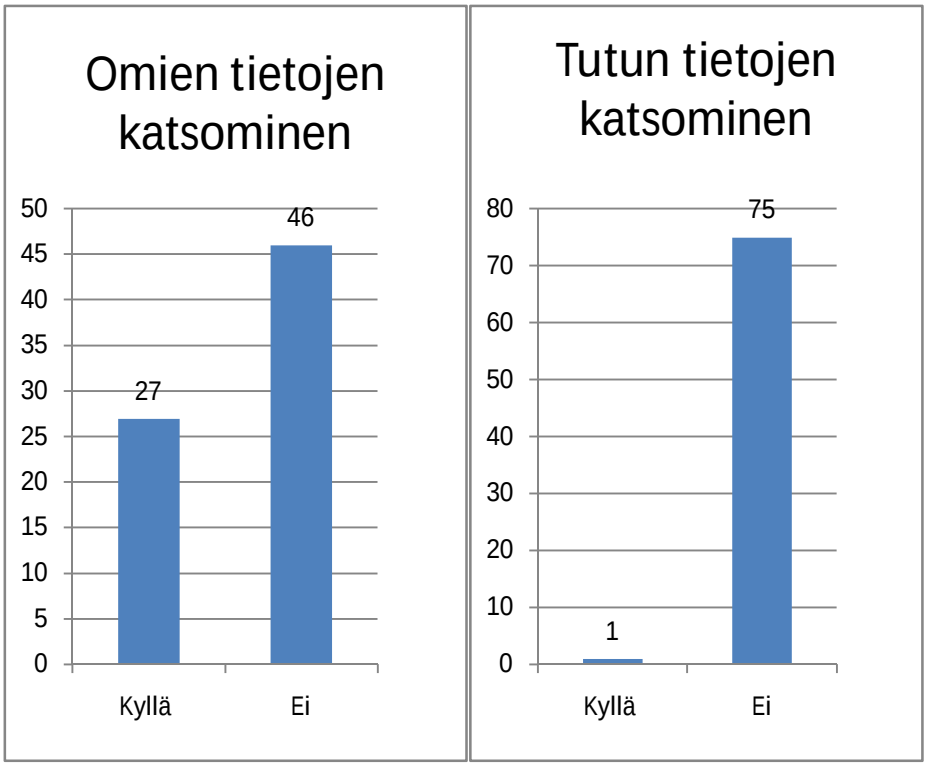
- sakkorangaistus, (44 kpl eli 57 %)
- vankeusrangaistus, (28 kpl eli 36 %)
- ammatinharjoittamisoikeuden rajoittaminen tai poistaminen, (56 kpl eli 76 %)
- kirjallinen varoitus, (49 kpl eli 64 %).

Rikoslain ja useiden erityislakien mukaan kaikki tämän kysymyksen vastausvaihtoehdot ovat oikeita. Saattaa olla, että oikeustapauksia ei näistä kaikista rikkomuksista ole, mutta kaikki vaihtoehdot ovat lain mukaan mahdollisia rangaistuksia.

On myös huomattava, että työnantaja voi määrätä näistä poiketen tai näihin lisäten muita seuraamuksia erilaisten työtehtävien suorittamisesta annettujen ohjeiden noudattamatta jättämisestä, luonnollisesti myös muista kuin salassapitovelvoitteiden rikkomisesta. Esimerkiksi Etelä-Pohjanmaan sairaanhoitopiirissä on käytäntö, että ensimmäisestä tietosuojarikkeestä seuraa kirjallinen huomautus ja saman henkilön tätä seuraavasta toisesta tietosuojarikkeestä irtisanominen. Samantyylinen käytäntö tultaneen ottamaan myös Hankasalmen sosiaali- ja terveystoimessa.

Kysymys 5. Saanko katsoa Effica järjestelmästä omia potilastietojani?

Kysymys 6. Saanko katsoa tuttuni potilastietoja, vaikka en tietoja hänelle tai muulle kertoisikaan?



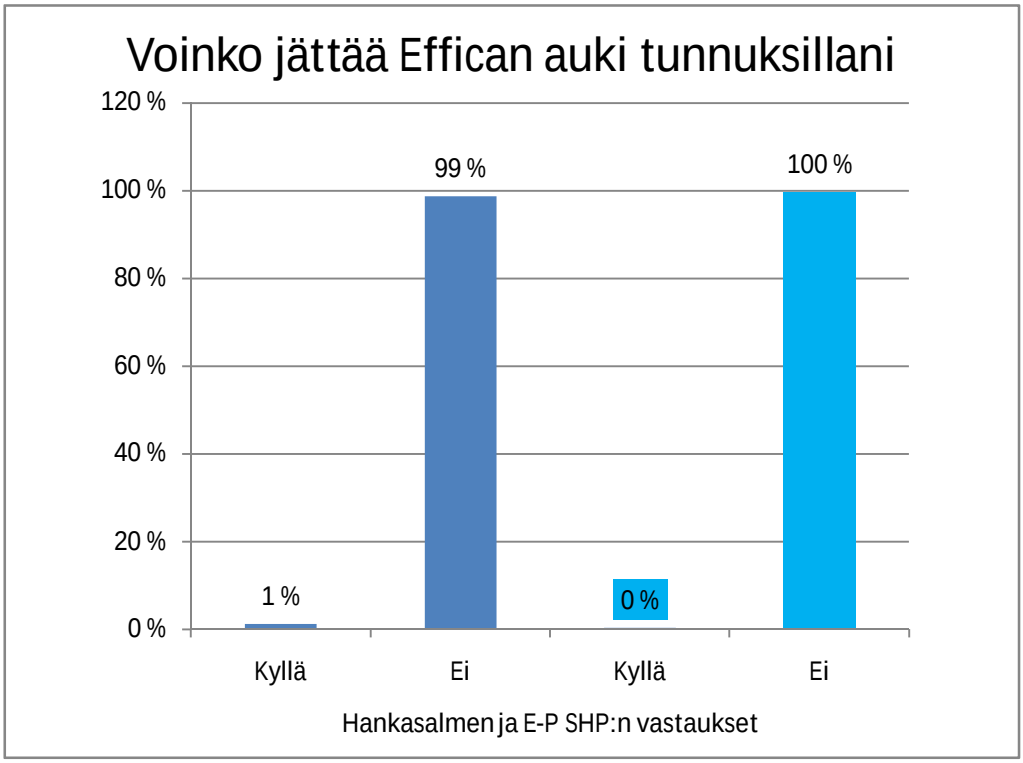
KUVIO 8. Potilastietojen katselu (N=I 73 ja II 76)

Näitä vaihtoehtoja rikotaan varmasti työyksiköissä eniten. Laissa lähdetään siis siitä, että potilastietoja ei saa katsella, jos se ei liity työtehtävien hoitoon. Aina pitää olla selkeä selitys sille, miksi työntekijä on katsellut jonkun henkilön tietoja. Tähän tämänhetkisen lain mukaan kuuluu myös omien tietojen katselu, sillä niitä ei laissa ole

rajattu erikoisasemaan. Lisäksi tämä on tällä hetkellä oikeudenmukaisuuskysymys. Terveydenhuollon ammattilaiset näkevät helposti omat tietonsa, mutta muille ihmisille tämä on vaikeampaa.

Edellä olevien kysymysten osalta Etelä-Pohjanmaan sairaanhoitopiriin vastaukset noudattelivat tämän tutkimuksen lukuja. Omien tietojen katselun luvut olivat (Kyllä 125 kpl ja Ei 906 kpl) ja tutun tietojen katselun määrät olivat (Kyllä 3 kpl Ei 1028 kpl).

Kysymys 7. Kun poistun ruokalaan/kokoukseen työhuoneestani, voinko jättää Effican auki tunnuksillani?

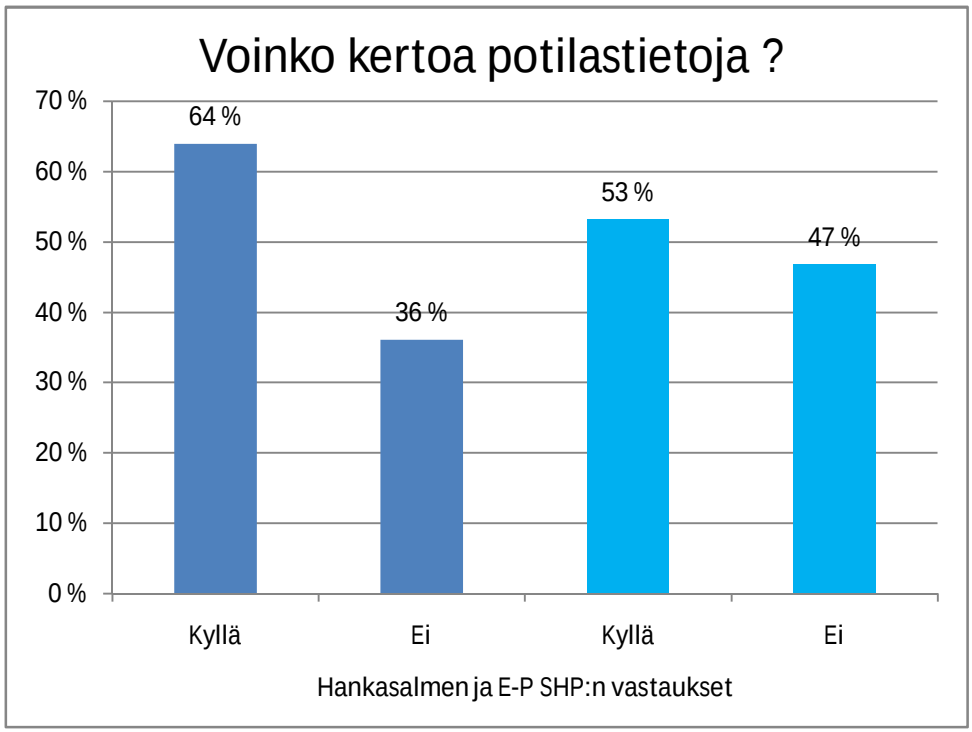


KUVIO 9. Ruokalaan/kokoukseen poistuminen (N=76 ja 1031)

Asiaton pääsy tietojärjestelmiin on estettävä lukitsemalla työasema, kun työhuoneesta poistutaan. Koneen auki jättäminen vaarantaa oleellisesti tietoturvallisuutta. Vaikka työhuoneeseen ei ulkopuolisia pääsisikään, eri henkilöillä työyhteisössä voi olla erilaiset oikeudet ohjelmien käyttöön. Jos ulkopuolinen pääsee vaikkapa potilastietojärjestelmään toisen tunnuksilla, hänen tekemänsä mahdollinen väärinkäytös tulee salasanojen haltijan kontolle.

Kysymyksen vastaukset muistuttavat jälleen yksiköiden välillä toisiaan. Tosin vastausten määrä on vaikea esittää kaaviona henkilöstömäärän suuren eroavaisuuden vuoksi, joten ne avataan vielä tässä: Hankasalmi (Kyllä-vaihtoehto 1 kpl, Ei-vaihtoehto 75 kpl) ja E-P SHP (Kyllä 4 kpl ja Ei 1027 kpl).

Kysymys 8. Voinko kertoa hoidossa olevan täysi-ikäisen potilaan yleistilan puhelimessa lähiomaiseksi merkitylle henkilölle, jonka henkilöllisyyden olen varmistanut?



KUVIO 10. Yleisten potilastietojen kertominen lähiomaiselle (N=72 ja 1031)

Laissa potilaan asemasta ja oikeuksista 17.8.1992/785 1. luvussa 6 §:ssä todetaan, että jos potilas jonkin syyn perusteella, kuten mielenterveyshäiriön tai kehitysvammaisuuden vuoksi, ei pysty päättämään hoidostaan, potilaan lähiomaista on kuultava ennen tärkeän hoitopäätöksen tekemistä. Kuten vastausten hajonnastakin näkyy, tämä asia ei ole selkeä. Kuitenkin monissa laitoksissa on käytäntönä, että nimenomaan yleisvoinnista voidaan omaiselle kertoa. Voidaan kertoa, onko vointi ennallaan, millaisia muutoksia siinä on ollut parempaan tai huonompaan. Vaikka laissa ei ole selvää lupaa asialle, on kertominen inhimillistä. Vastaukset kummassakin työyh-

teisössä noudattivat jälleen toisiaan. Samanlaista epätietoisuutta käytännöistä oli molemmissa. Vastausten määrät olivat seuraavat: Hankasalmi (Kyllä-vaihtoehto 46 kpl Ei-vaihtoehto 26 kpl) ja (E-P SHP Kyllä 549 kpl Ei 482 kpl).

Kysymys 9. Saanko pyytää potilaalta etukäteen tietojen luovutukseen toistaiseksi voimassa olevaa lupaa?

Hankasalmella Kyllä-vastaukset olivat (Kyllä 48 kpl eli 70 %) ja (Ei-vastaukset 20 kpl eli 30 %). Etelä-Pohjanmaan sairaanhoitopiirissä vastausten määrät eri vaihtoehdoissa olivat (Kyllä 458 kpl eli 44 % ja Ei 573 kpl eli 56 %). Tässä vastaukset erosivat toisistaan. Enemmistö Hankasalmen työntekijöistä luovuttaisi tietoja toistaiseksi voimassa olevalla luvalla. Vertailuyksikössä tulos oli juuri päinvastainen. Laissa lähdetään siitä, että potilaan suullinen tai muuten asiayhteydestä ilmenevä suostumus tarvitaan, kun kysymys on hänen tutkimuksensa ja hoitonsa järjestämiseksi tarpeellisten tietojen luovuttamisesta toiselle terveydenhuollon yksikölle tai ammattihenkilölle. Tässä kohdassa ei puhuta lainkaan toistaiseksi voimassa olevasta luvasta. Lupa tai suostumus täytyy kysyä joka kerran. Tällaisesta luvasta on aina tehtävä merkintä potilasasiakirjoihin. (Eriksson 2003.) Hankasalmen työntekijöiden piirissä on näin ollen enemmän tämän tiedon suhteen korjattavaa. Tosin Etelä-Pohjanmaan sairaanhoitopiirissäkin on paljon vääriä vastauksia.

Kysymys 10. Voinko muuttaa antamani kirjallisen hoitosuhteeseeni liittyvän suostumuksen lääkärivastaanotolla suullisesti?

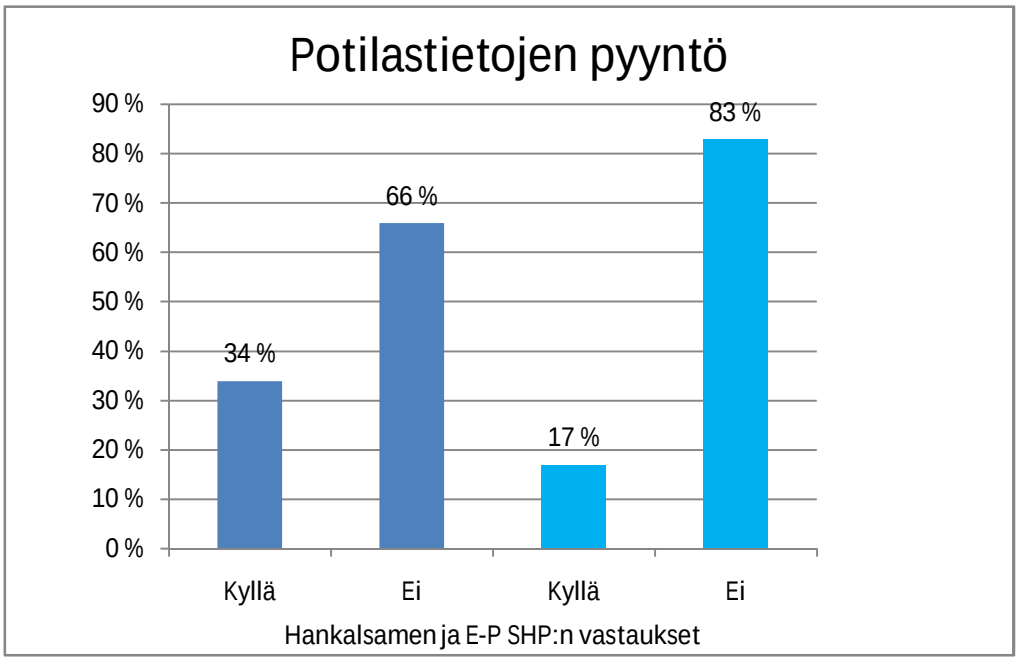
Vastaus on jo edellisenkin kohdan perusteella kyllä. Kirjallinen lupa on lain mukaan pääsääntö. Kirjallisia suostumuksia annetaan esimerkiksi tilattaessa potilaspapereita toisesta terveydenhuollon yksiköstä. Siihen tarvitaan kirjallinen suostumus, joka lähetetään yksikköön ja josta potilaspaperit sitten aikanaan tulevat. Tällaisen luvan voi potilas peruuttaa suullisesti vastaanotolla.

Vastaukset tähän kysymykseen menivät mahdollisimman tasan, eli Hankasalmella 71 vastaajasta 36 kpl (51 %) oli sitä mieltä, että kirjallisen luvan voi perua suullisesti ja 35 kpl (49 %), että ei voi. Etelä-Pohjanmaan sairaanhoitopiirin vastaavat luvut olivat Kyllä voi perua, 314 kpl (31 %) ja Ei voi perua, 717 kpl (69 %).

Kysymys 11. Voinko antaa poliisille tiedon, onko henkilö tk-sairaalaan sisäänkirjoitettu potilas?

Nimi ei ole terveydenhuoltolaissa luokiteltu salassa pidettäväksi tiedoksi. Näin ollen poliisi voi saada tiedon hoidossa olevasta potilaasta. Enemmistä Hankasalmen sosiaali- ja terveystoimen henkilöstöstä vastasi tähän kysymykseen (Kyllä 41 kpl eli 58 % ja Ei 30 kpl eli 42 %). Etelä-Pohjanmaan sairaanhoitopiirin vastaavat luvut olivat (Kyllä, 328 kpl eli 32 % ja Ei, 703 kpl eli 68 %).

Kysymys 12. Poliisin soittaessa virka-asioissa potilaasta, voinko antaa puhelimessa hänen pyytämänsä potilastiedot?



KUVIO 11. Poliisille annettavat tiedot (N=71 ja 1031)

Poliisilla on rikoslain mukaan oikeus tietää viranomaisten rekistereihin sisältyviä tietoja, jos poliisi pystyy yksilöimään tarvitsemansa tiedon. Tämä kohta poliisin mahdollisuudesta saada tietoja on hieman ongelmallinen, koska terveydenhuollon viranomaisilla ei ole ilmoitusvelvoitetta antaa tietoja edes silloin, kun esiin tulleet asiat viittaavat vakavaan rikokseen (Castren 2008). Lisäksi potilaan oikeuksista annetussa laissa ei ole suoranaista velvoitetta antaa poliisille potilastietoja.

Kuten edellä olevasta kuviosta ilmenee, vastaukset olivat molemmissa työyksiköissä oikeansuuntaiset. Tosin Hankasalmella tilanne on hieman ongelmallisempi, eli 24 henkilöä antaisi poliisille potilastietoja. Etelä-Pohjanmaan sairaanhoitopiirissä tietoja antaisi 174 henkilöä. Kielteisiä vastauksia Hankasalmella oli 47 kpl ja vertailuyksilössä 857 kpl.

Kysymys 13. On tavallista, että iäkkään potilaan vaivoista soittaa puoliso. Mies on ollut esimerkiksi tutkimuksissa ja hänellä on todettu syöpä.

TAULUKKO 2. Potilastietojen ilmaiseminen läheiselle

	Kyllä	Ei
1 Käy ilmi, että vaimolla ei tietoa syövästä. Voinko kertoa sen?	Hankasalmi 11 %, 8 kpl E-P SHP 0,8 %, 8 kpl	Hankasalmi 89 %, 65 kpl E-P SHP 99,2 %, 1023 kpl
2 Voinko kertoa vaimolle seuraavan vastaanotto-ajan, kun mies on vaimon vieressä kotona?	Hankasalmi 54 %, 39 kpl E-P SHP 46 %, 466 kpl	Hankasalmi 46 %, 33 kpl E-P SHP 54 %, 565 kpl

Tähän kysymykseen oli vastannut Hankasalmella yhteensä 73 työntekijää ja Etelä-Pohjanmaan sairaanhoitopiirissä 1031 työntekijää.

Ensimmäisessä kysymyksessä vastaukset noudattelivat samaa linjaa Kyllä- ja Ei-vaihtoehtojen välillä. Tosin Hankasalmella prosentuaalisesti isompi ryhmä tekisi lainvastaisesti, jos kertoisi vaimolle puhelimessa miehen syöpädiagnoosista. Henkilöstöllä ei vielä voi olla mieheltä saatua lupaa tietojen antamiseen. Laki potilaan asemasta ja oikeuksista antaa tähän ehdottoman kiellon. Potilastietoja ei saa luovuttaa sivullisille ja tässä tapauksessa voidaan ajatella myös todennäköisesti iäkkään vaimon suojaamista tiedolta. Vastaanottoaikoja soittavat usein puolisot, varsinkin iäkkäiden ihmisten kohdalla. Tästä on Hankasalmella hammashuollossa ollut ennakkotapauskin jokunen vuosi sitten. Vanhemmille annettiin aikuisen pojan vastaanottoaika vietäväksi hänelle. Poikaa ei ollut saatu puhelimella tavoitettua. Tästä vanhemmille vas-

taanottoajan antamisesta poika valitti hallinto-oikeuteen. Vastaanottoaika ei ole salassa pidettävä asia, oli vastaus lyhykäisyydessään. Näin valitus hylättiin.

Kysymys 14. Voiko hoitotilanteessa oleva potilas tutustua sairaskertomukseensa, kun huoneessa on terveydenhuollon ammattihenkilö läsnä?

Henkilötietolain 6. luvun 26–28 pykälissä selitetään potilasta koskevien tietojen tarkastusoikeutta. Terveydenhuollon ammattilaisen on pyydettäessä annettava rekisterissään olevat potilasta koskevat tiedot ymmärrettävässä muodossa potilaalle nähtäväksi. Tietojen ymmärrettävyysvaatimuksen vuoksi on tärkeää, että terveydenhuollon ammattilainen on läsnä tietoihin tutustuttaessa. Usein lääkärien käyttämä latina on vaikeaselkoista maallikolle ja voi aiheuttaa väärinymmärrystä.

Kysymykseen vastasi Hakasalmella 75 työntekijää (Kyllä-vastauksia oli 65 kpl eli 87 % ja Ei-vastauksia 10 kpl eli 13 %). Etelä-Pohjanmaan sairaanhoitopiirissä kysymykseen vastasi 1031 työntekijää, (Kyllä-vastauksia siellä oli 764 kpl eli 74 % ja Ei-vastauksia 267 kpl eli 26 %).

Kysymys 15. Saanko puhua potilasasioista ruokalassa muun osaston henkilökunnan jäsenten kesken?

Laki potilaan asemasta ja oikeuksista lähtee siitä, että työntekijä voi käsitellä potilaan tietoja työtehtävää suorittaessaan. Siis hänellä täytyy olla aina syy, kun henkilöstö käsittelee potilastietoja. Ruokala ei ole sellainen paikka. Ymmärrän Hankasalmen työntekijöiden vastauksen tk-sairaalan osalta. Sairaalassa on oma ruokala, jossa ruokailee vain sairaalan henkilökunta. On inhimillistä, jos siellä vaihdetaan myös potilastietoja, koska potilaita hoidetaan yhdessä. Kuitenkin laki lähtee yksiselitteisesti edellä mainitusta vaatimuksesta.

Molemmista yksiköistä henkilöitä, jotka vastasivat tähän kyllä ehkä edellä mainitusta syystä. Hankasalmella noin kolmannes vastaajista ja Etelä-Pohjanmaan sairaanhoitopiirissä koko henkilöstö työskentelevät sairaalassa. Hankasalmi, (Kyllä-vastaukset 11 kpl eli 15 % ja Ei-vastaukset 64 kpl eli 85 %). Etelä-Pohjanmaan sairaanhoitopiirin vastaavat luvut olivat (Kyllä 28 kpl eli 3 % ja Ei 1003 kpl eli 97 %).

Kysymys 16. Voinko antaa hoito-ohjeita potilaalle toisten potilaiden kuullen?

Tämä kysymys kysyttiin vain Hankasalmen työntekijöiltä. Käytäntö on näyttänyt, että tässä kohdin on puutteita tietoturvassa. Kaikki potilasta käsittelevät lait lähtevät siitä, että potilaan tietoja ei luvatta saa antaa sivulliselle. Tässä ei eritellä, mitä tiedot ovat.

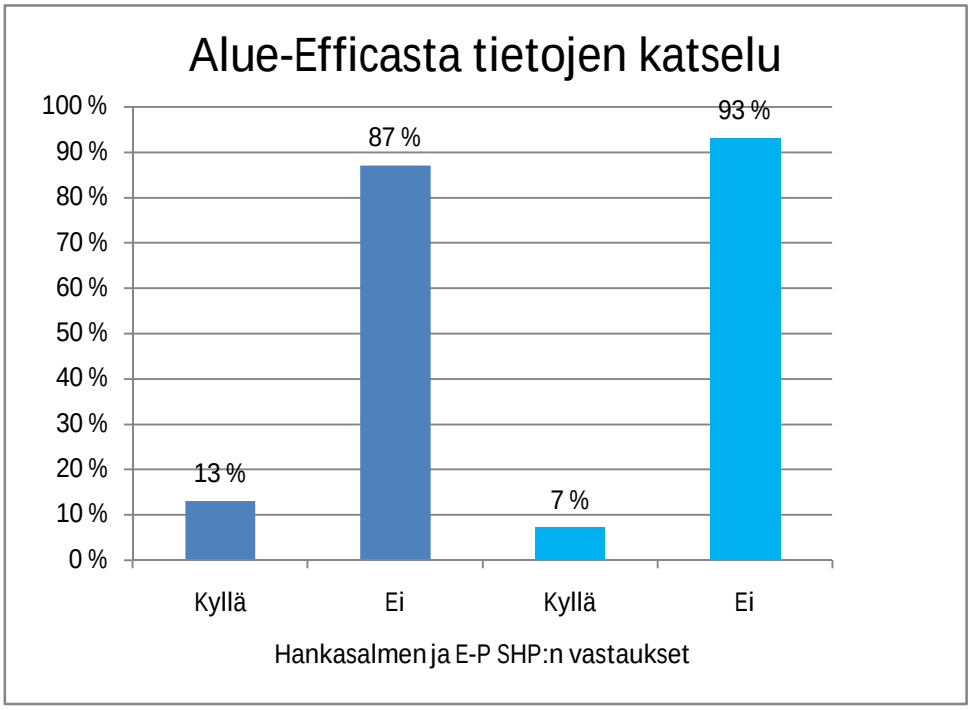
Vastaukset olivat odotettuja, (Kyllä-vaihtoehto 9 kpl eli 12 %, Ei-vaihtoehto 64 kpl eli 88 %). Yhteensä tähän kysymykseen vastasi 73 työntekijää.

Kysymys 17. Sähköisessä järjestelmässä tietojen luovutus on merkitty seuraavasti: palautteen lähettäminen lähettävään yksikköön, rasti kohdassa EI. Lääkäri ohjelmoi lähetteen perusteella jatkotutkimuksia terveyskeskuksessa. Voinko palauttaa lähetteen lähettäneelle taholle?

Hankasalmen työntekijät olivat tähän vastanneet varovaisesti, sillä vain 59 oli vastannut. Vastaukset jakautuivat jälleen aika samankaltaisesti molemmissa yksiköissä. Hankasalmella (Kyllä-vastauksia oli 15 kpl eli 25 % ja Ei-vastauksia 44 kpl eli 75 %). Etelä-Pohjanmaan sairaanhoitopiirissä vastaavat luvut olivat (Kyllä 216 kpl eli 21 % ja Ei 815 kpl eli 79 %). Enemmistö oli jälleen oikeassa, vastaus on Ei.

Tähän vastaus on jälleen yksiselitteinen. Lain mukaan potilasta koskeva hoitopalaute, joka sisältää yhteenvedon annetusta hoidosta, voidaan potilaan suullisen tai muuten asiayhteydestä ilmenevän suostumuksen perusteella toimittaa hänet hoitoon lähettäneelle terveydenhuollon yksikölle. Potilas oli tässä tapauksessa jo kieltänyt lähetteen lähettämisvaiheessa tiedon palauttamisen. Näissä kysymyksissä on aina mietittävä, onko potilas kykenevä arvioimaan omaa tilaansa. Vastauksissa on lähdetty siitä olettamuksesta, että ei ole kysymys laissa mainituista erityistapauksista, jolloin tiedot voidaan antaa ilman potilaan lupaa.

Kysymys 18. Kysymys on kokonaisuudessaan seuraava: saako terveydenhuollon ammattihenkilö katsoa Alue-Efficasta potilaan tietoja tarkistamatta potilaan mahdollisesti antamaa suostumusta katseluun?



KUVIO 12. Alue-Efficasta potilastietojen katselu (N=67 ja 1031)

Alue-Effica tarkoittaa järjestelmää, jossa terveydenhuollon ammattilaisilla on mahdollisuus katsella potilaan tietoja myös toisen rekisterinpitäjän järjestelmästä. Tällainen järjestelmä on tulossa mm. Keski-Suomen alueelle mahdollisesti vielä tämän vuoden kuluessa.

Lain mukaan ilman potilaan lupaa ei voida katsoa Alue-Efficasta mitään, sillä alueellisessa tietojärjestelmässä mennään toisen rekisterinpitäjän potilastietoihin. Kuten paperisiinkin, myös sähköisiin pyyntöihin toisesta organisaatiosta tarvitaan potilaan kirjallinen suostumus. Yhä laajemman henkilöstön pääsy yhä laajempiin potilastietoihin asettaa tietoturvalle kovat haasteet. Molemmissa yksiköissä on edelleen niitä, joille tämä asia ei ole selvä. Ohjeistusta ja koulutusta tarvitaan kummassakin työyhteisöissä.

Kuviossa esitetyt prosentteina esitetyt vastaukset lukuina ilmaistuna ovat seuraavat: Kyllä-vaihtoehto Hankasalmi 9 kpl ja Etelä-Pohjanmaan sairaanhoitopiiri 71 kpl ja oikeat Ei-vaihtoehdot vastaavasti 58 kpl ja 960 kpl.

Kysymys 19. Saanko katsella kaikkea tietoa ja rekistereitä, joihin käyttäjätunnuksellani pääsen?

Vastaus tähän kysymykseen on yksiselitteisesti Ei. Aina täytyy olla jokin syy, minkä takia potilastietoihin rekisterissä mennään. Syyn täytyy liittyä potilaan asioiden hoitoon. Se voi olla katseluakin, mutta on tärkeä pitää mielessä, että jos työntekijä ei voi selittää käyntiään jonkun potilaan tiedoissa, hän on karkeasti sanoen lainrikkoja. On myös tärkeää dokumentoida jokainen katselu. Se auttaa myöhemmin asioiden muistamisessa ja myös potilas näkee, jos haluaa rekisterissä olevat tietonsa tarkistaa, kuka ja minkä takia on tietoja käyttänyt.

Kyllä-vastauksia oli molemmissa yksiköissä, (Hankasalmella 8 kpl eli 11 % ja Etelä-Pohjanmaan sairaanhoitopiirissä 48 kpl eli 5 %) ja oikeita Ei-vastauksia vastaavasti (63 kpl eli 89 % ja 983 kpl eli 95 %).

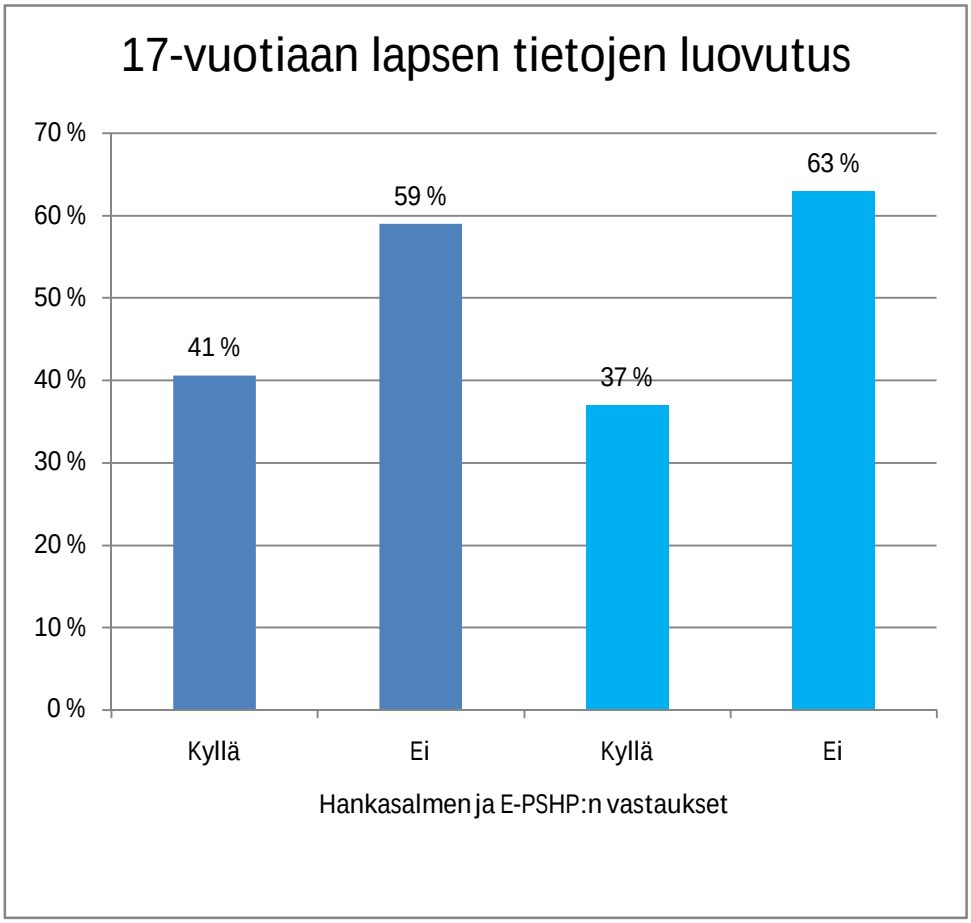
Kysymys 20. Henkilökohtainen käyttäjätunnuksen salasana minun tulee vaihtaa

- 3 kuukauden välein
- 6 kuukauden välein
- vuoden välein
- harvemmin.

Suosituksen mukainen salasanan vaihtoväli on 3 kuukautta. Tosin monet tietojärjestelmät, kuten Effica-järjestelmä, vaativat jopa kuukauden välein vaihdettavan salasanan.

Työntekijöistä enemmistö tiesi tämän suosituksen, sillä Hankasalmella 92 henkilöä (95 %) ja vertailukunnassa 854 (83 %) työntekijää valitsi tämän vaihtoehdon. Seuraavat vaihtoehdot järjestyksessä lukumäärinä ja prosentteina: Hankasalmi (2 kpl eli 2 %, 2 kpl eli 2 % ja 1 kpl eli 1 %). Etelä-Pohjanmaan sairaanhoitopiirin vastaavat luvut: (87 kpl eli 8 %, 19 kpl eli 2 % ja 71 kpl eli 7 %).

Kysymys 21. Voinko huoltajan pyynnöstä lähettää sairauskertomustiedot toiseen terveydenhuollon yksikköön 17-vuotiaata lapsesta ilman lapsen kirjallista suostumusta?



KUVIO 13. Voiko 17-vuotiaan lapsen tietoja luovuttaa ilman lupaa vain huoltajan pyynnöstä? (N=69 ja 1031)

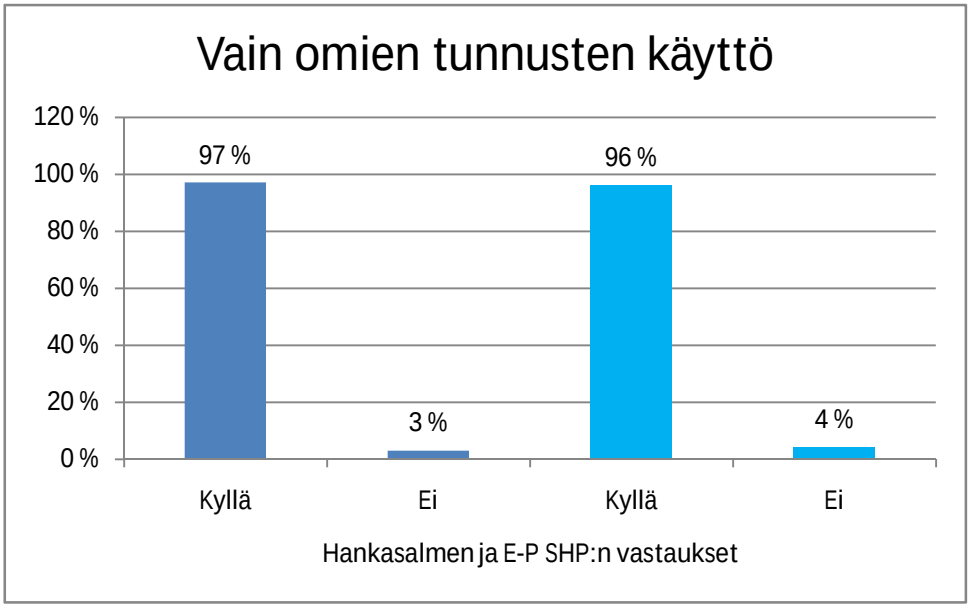
Vastauksista molemmissa työyhteisöissä näkee, että kysymys ei ole helppo. Laissa potilaan asemasta ja oikeuksista käsitellään alaikäisen asemaa. Laissa määrätään, että alaikäisen potilaan mielipide hoitotoimenpiteeseen on otettava huomioon, kun se on hänen ikäänsä ja kehitystasoonsa nähden mahdollista. Jos alaikäinen kykenee ikänsä ja kehitystasonsa perusteella päättämään hoidostaan, on se hoidettava yhteisymmärryksessä hänen kanssaan. 17-vuotias on varmasti jo kyllin kykenevä hoitamaan asioitaan aivan itse, joten vastaus kysymykseen on Ei. Vastaukset lukumäärinä olivat: Hankasalmi (Kyllä, 28kpl ja Ei, 41 kpl) ja vertailukunta (Kyllä, 381 kpl ja Ei, 650

kpl). Hajontaa on paljon tämän kysymyksen kohdalla juuri lain tulkinnanvaraisuuden vuoksi.

Kysymys 22. Saanko lähettää sähköpostilla potilaalle hänen hoitoonsa liittyviä yksityiskohtaisia tietoja?

Stakes ja tietosuojavaltuutettu ovat antaneet ohjeistusta sähköpostin käytöstä potilastietoja käsiteltäessä. Siinä tulkinnassa ehdoton edellytys on, että sähköposti lähetetään salaisena. Kuitenkin on myös huolehdittava siitä, että tällainen posti ei jää palvelimelle muistiin, vaan se täytyy heti tuhota. Samoin tähän potilastietojen lähetystapaan pitäisi aina olla potilaan lupa. On paljon helpompi lähettää kirjeitse potilastietoja jo siitäkin syystä, että potilastietojärjestelmissä on osoitteet ja sähköpostiosoitteille ei ainakaan Effica-järjestelmässä ole omaa kenttää. Monissa yksiköissä, kuten myös Etelä-Pohjanmaan sairaanhoitopiirissä, on kokonaan kielletty sähköpostin käyttö potilastietojen lähettämiseen. Hankasalmella kaikki vastasivat tähän Ei. Vertailukunnassa 25 henkilöä (2 %) oli sitä mieltä, että sähköpostin avulla voidaan potilastietoja lähettää. Ei-vaihtoehtoja oli kuitenkin 1005 kpl (98 %).

Kysymys 23. Saanko käyttää Effica-potilastietojärjestelmää ainoastaan omilla tunnuksillani?



KUVIO 14. Effica-tietojärjestelmän käyttö (N=75 ja 1031)

Lähes kaikki ovat tienneet, että potilastietojärjestelmää tulee käyttää vain omilla tunnuksilla. Jo aiemmin tässä työssä on kerrottu, mitä ongelmia aiheutuu toisten tunnusten käytöstä. Esimerkiksi mahdolliset tietoturvan väärinkäytökset tulevat sen henkilön kontolle, jonka tunnuksilla ollaan järjestelmässä.

Kysymys 24. Saanko käyttää henkilökohtaiseen viestintään sähköisiä keskustelupalstoja, kuten Facebookia, Messengeriä tai muita vastaavia työaikana?

Laki ei kiellä näiden käyttöä, mutta useimmat työyksiköt omissa tietoturvaohjeissaan ovat nämä kieltäneet. Niin on myös tehty Hankasalmella ja samoin vertailukunnassa.

Hankasalmella tulos oli niiden osalta, jotka olivat vastanneet, 100-prosenttisesti Ei, 71 kpl. Etelä-Pohjanmaan sairaanhoitopiirissä 12 henkilöä (1 %) oli vastannut tähän kysymykseen Kyllä. Valtaosa heistäkin vastasi Ei, eli 1025 kpl (99 %).

Kysymys 25. Voinko kertoa työkaverini sairausloman syytä ulkopuoliselle?

Ilman työkaverini lupaa en voi asiasta mainita kenellekään. Laki potilaan asemasta ja oikeuksista on tämän asian suhteen ehdoton.

Hankasalmen tulos oli 100-prosenttisesti tämänkin kysymyksen kohdalla oikein, Ei-vastauksia oli 77 kpl. Vertailukunnassa 1 % eli 10 henkilöä voisi kyselyn mukaan kertoa työkaverin sairausloma syyn ulkopuoliselle. Tosin valtaosa sielläkin asian tiesi: 1021 henkilöä eli 99 %.

Kysymys 26. Kommentteja kyselystä. Oliko tarpeellinen? Ymmärsitkö kysymykset?

Kyselyyn tuli kommentteja 46 kappaletta eli 47 prosentilta vastaajista. Useimmissa kommenteissa oli maininta, että kysely oli vaikea tai että kysymyksissä olisi voinut olla vaihtoehto En tiedä. Yli puolessa kommenteista kyselyä kuitenkin pidettiin tarpeellisena ja monessa vastauksessa toivottiin myös koulutusta asiasta. Muutamia erilaisia kommentteja poimitaan tähän mukaan:

- En ymmärtänyt kaikkia kysymyksiä. Varmasti tarpeellinen kysely, olisi mukava tietää kysymysten oikeat vastaukset.
- Liian pitkä!

- Jotkin oli kimurantteja kysymyksiä, joihinkin olisi voinut vastata sekä että…
- Hyvä muistuttaa mieliin esim. vaitiolovelvollisuuteen liittyviä kysymyksiä. Ok.
- Kaikki kysymykset eivät olleet selkeitä, olisi voinut olla En tiedä -vaihtoehto, sillä joitakin asioita en tiennyt ja veikkaamiseksi meni.
- Kysymysten muotoilussa puutteita, kaikista kysymyksistä en päässyt perille, mitä halutaan kysyä. Haluaisin vielä kertoa toiveeni, että tk:sta suljettaisiin mahdollisuus olla yhteydessä Facebookiin. Yövuorolaisilla menee joskus paljon aikaa täällä oloon.
- Tarpeellinen kysely. Olen jättänyt vastaamatta kysymyksiin, mitä en tiennyt tai ymmärtänyt kysymystä.
- Perehdytystä en näihin asioihin ole saanut lainkaan, tarpeellinen yleinen tiedotustilaisuus asian tiimoilta.
- Kysely oli tarpeellinen. Pisti miettimään asioita ja huomasin, että oli aukkoja tiedoissa. Kysymykset olivat hyvin laadittuja. Tosin pari kinkkisempää oli joukossa, Kiitos, koulutusta asian tiimoilta.

7 PÄÄTELMIÄ JA EHDOTUKSIA

Tässä luvussa käydään läpi tutkimuksen esiin tuomia asioita. Lisäksi pyritään antamaan kuva niistä toimista, joihin on tietoturvan parantamiseksi ryhdyttävä. Ensin käydään läpi tutkimus pääpiirteittäin ja siitä etsitään myös vaikeimmat kohdat tietoturvan parantamisen kannalta. Lopuksi kirjataan ehdotukset, joita voidaan tehdä ongelmallisten kohtien ratkaisemiseksi.

7.1 Tietoturvan ymmärrys ja taso sosiaali- ja terveystoimessa

Tietoturvan taso on kohtalainen yleisten tietoturvakysymysten osalta. Tosin joissakin kysymyksissä oli selvästi havaittavissa tietämättömyyttä. Tämä johtuu siitä, että Hankasalmella ei yleisiin tietoturvaa koskeviin asioihin ole koskaan kiinnitetty tarpeeksi huomiota. Asiat, joihin oli vastattu vähemmän, liittyivät joihinkin salasanaa ja sähköpostia koskeviin kysymyksiin. Samoin monivalintatehtävien Kyllä- ja Ei-osuudet olivat hieman hankalia monelle vastaajalle. Tarkoitus oli, että ruksataan jompikumpi, mutta usein oli vastattu vain Kyllä-vaihtoehtoon. Tältä osin kysely jäi puutteelliseksi. Yleisissä tietoturvakysymyksissä ehkä tärkeimpiä olivat virustorjuntaan liittyvät kysymykset. Vastausten perusteella koulutusta tarvitaan näissä asioissa. Sataan prosenttiin ei mikään vaihtoehto näissä kysymyksissä yltänyt.

Effica-osiossa saatua tulosta vertailtiin myös Etelä-Pohjanmaan sairaanhoitopiirin vastaavan kyselyn tulokseen. Vastaukset kysymyksiin noudattivat hämmästyttävällä tavalla toisiaan. Vain parissa kysymyksessä oli jonkin verran eroavaisuutta. Tämän osion kysymykset olivat henkilöstön enemmistöllä kohtuullisesti hallussa. Tärkeimpiin kysymyksiin, jotka koskivat potilastietojen luovutusta ja tarkastelua, vastattiin vaihtelevasti. Joidenkin kysymysten kohdalla huomattava osa työntekijöistä oli valmis kertomaan hoito-ohjeita toisten potilaiden kuullen tai luovuttamaan niitä toiselle viranomaiselle ilman lupaa. Näissä kohdin tarvitaan tarkennusta käytänteissä.

Kyselyssä oli mukana pari kysymystä, jotka olivat tulkinnanvaraisia joko lain tai ennakkotapausten kannalta. Näitä kysymyksiä on tulkittava tapauskohtaisesti ja oikeaa

yleispätevää vastausta tuskin onkaan, ja niinpä näissä kysymyksissä kaikki vastausvaihtoehdot saivat tasaisesti kannatusta.

Kysymys kolme otetaan aivan erikseen esille, koska siinä kulminoituu koko salassapidon ydin: terveydenhuollon ammattihenkilö ei saa kertoa sivulliselle potilaan nimeä, henkilötunnusta, terveydentilaan liittyviä seikkoja eikä potilaan perheestä ilmi tulleita seikkoja. Tämän kysymyksen osalta päästiin lähes sataan prosenttiin kaikilta osin. Kolmen kysymyksen kohdalla päästiin täyteen nollaan väärän vaihtoehdon ja 100 prosenttiin oikean vaihtoehdon kohdalla. Nämä olivat lisäksi tärkeitä kysymyksiä, joten tämä antaa uskoa tietoturvan toteutumiseen lähes lain edellyttämällä tasolla.

Yleisenä huomiona koko tutkimuksesta voidaan sanoa, että vastausten taso vaihteli suhteellisen paljon. Tietoturvan kannalta tärkeiden asioiden tietämys oli hyvällä tasolla, joskin yksikin heikko lenkki on liikaa. Joistakin kysymyksistä voidaan sanoa, että ne kuuluivat yleissivistyksen piiriin, kuten vaikkapa lain tulkintaa koskevat kysymykset. Niissä oli eniten hajontaa.

7.2 Toimet tietoturvan parantamiseksi

Ensimmäinen asia, joka jo kyselyyn perustuen on luvattu tehdä, on työyksikkökokouksissa henkilöstön koulutus tietoturvatutkimuksen vastauksista ja niihin liittyvistä vaikeista kohdista jo tämän kevään aikana. Kysely voidaan sopivan ajan kuluttua uusia, vaikkapa loppusyksystä, jolloin voidaan varmistaa ensimmäisestä kyselystä saadun palautteen ymmärtäminen.

Toinen lähes yhtä tärkeä asia on tietoturvaoppaan tekeminen. Siinä avataan nimenomaan yleistä tietoturvatietämystä. Ensiksi avataan yleisellä tasolla lainkohtia: mitä laissa todetaan ja mitä se tarkoittaa. Käytännön tasolla annetaan ohjeita sähköpostin käyttöön, virustorjuntaan ja yleisiin työrutiineihin. Tämä opas on tarkoitettu jokapäiväiseen käyttöön ja sitä päivitetään tarvittaessa.

Kolmanneksi tietoturvavastaavan toimenkuvasta tiedottaminen ja myös tietoturvaseurannan säännöllinen aloittaminen ja siitä tiedottaminen ovat tärkeitä tietoturvatekijöitä. Selvien käytänteiden luominen tietoturvan väärinkäytöksissä on myös vält-

tämätöntä. Lokitiedostojen säännöllinen tarkkailu lisää huomattavasti tietoturvallisuutta.

8 POHDINTA

Tietotuvallisuus nykyisenä voimakkaasti verkottuvana ja sähköistyvänä aikana on avainasemassa. Arkaluonteiset ja salassa pidettävät tiedot tulee erityisesti suojata. On huolehdittava myös organisaatioissa olevien työntekijöiden tietämyksestä tietoturvan suhteen, sillä onhan tutkittu, että 25 % tietoturvauhista aiheutuu yrityksen ulkopuolelta ja peräti 75 % yrityksen sisältä. Henkilökunta on siis avainasemassa puhuttaessa asiakirjojen salassapidosta ja yleisestä tietoturvallisuudesta.

Keski-Suomen sairaanhoitopiirin hallinnoima Alue-Effica on ollut suunnitteilla jo pari vuotta ja nyt sitä testataan käyttöönottoa varten. Tässä järjestelmässä lääkärit ja hoitohenkilökunta voivat katsella toisen rekisterinpitäjän tietokannassa olevia potilastietoja potilaan luvalla. Hankasalmen terveyskeskus liittynee Jyväskylän isäntäkuntaan, ja rekisterinpitäjä vuoden 2011 alussa on alueellinen terveyskeskus. Lääkäreitä ja hoitohenkilökuntaa on monikymmenkertainen määrä tässä uudessa organisaatiossa, ja he kaikki pääsevät hankasalmelaistenkin potilastietotoihin. Näiden vuoksi terveystoimessa asioivien potilastiedot leviävät laajalle aiempiin käytäntöihin verrattuna.

Henkilökunnalle osoitetussa tietototurvaan liittyvässä tutkimuksessa havaittiin aukkoja yleisessä tietoturvatietämyksessä, ja myös potilastietojen käsittelyssä oli puutteita. Tutkimuksessa ei selkeästi saatu selville, missä yksiköissä tietoturva on puutteellisempaa. Kaikissa yksiköissä sekä sosiaali- että terveystoimessa vastaukset noudattivat toisiaan. Opastusta ja koulutusta tarvitaan koko sosiaali- ja terveystoimessa.

Mielenkiintoista oli myös tutkimuksen Effica-osion vertaaminen Etelä-Pohjanmaan sairaanhoitopiiriin vastaavaan tutkimukseen. Tämä on yli tuhannen työntekijän yhteisö, mutta tulokset noudattelivat prosentuaalisesti toisiaan. Vertailuyksikössä olisi tilanne voinut olla parempikin, koska tämä oli jo toinen kysely. Väliin on sisältynyt tietoiskuja tietoturvasta.

Tutkimuskysymyksiin tuli muutamia kommentteja siitä, että kysely oli vaikeaselkoinen tai että se oli liian pitkä. Kun tutkimus uusitaan tietoturvakoulutuksen jälkeen, tulee tutkimuskysymyksiin kiinnittää huomiota. Kyselyä voidaan tiivistää ja karsia

sellaisia kysymyksiä pois, jotka eivät ole olennaisia tietoturvan kannalta. Samoin voidaan yksilöidä vielä tarkemmin eri yksiköt, jotta saadaan selkeämmin selville tietoturvan ymmärtämistä ja selvennystä kaipaavat tahot.

Valtionhallinnon taholta on esitetty jopa edellä kuvattuja yhdistymisiä suurempiakin kokoonpanoja terveydenhuollossa. Viiden terveyspiirin muodostaminen koko Suomeen oli jo jonkin aikaa sitten esillä. Tämä hanke pantiin kuitenkin lepäämään, kunnes 20 000 väestöpohjan vaatima hanke on viety loppuun. Tietoturvan lain edellyttämästä tasosta huolehtiminen on ensiarvoisen tärkeää näissä laajoissa hankkeissa niin teknisten suojautumiskeinojen, ohjelmistojen kuin työntekijöidenkin osalta.

LÄHTEET

Castren, K. Tietosuoja tulilinjalla. Tietosuoja, tietoturvan ja tietosuojan erikoislehti 4/2008, 1. Viitattu9.4.2010.
http://www.tietosuojalehti.fi/Digipaper/OldNews.aspx?id=608

Eriksson, N. 2003. Muutoksia potilastietojen luovuttamisessa. Viitattu 9.4.2010. Sosiaaliturva 15/2000.
http://www.kunnat.net/k_perussivu.asp?path=1;29;349;22080;29601;5276. Kuntaliitto.

Hankasalmen kunta: Vuosikertomus 2008.

Heikkilä M., Rousku K. & Ruotsalainen P. 2006. STAKES lausunto. A Strategy for A Secure Information Society – Dialoque, partnership and empowerment COM (2006) 251. Viitattu 22.3.2010.
http://www.stakes.fi/FI/ajankohtaista/lausunnot/060628.htm?NRMODE=Publis..

Heiliö, P., Kattelus, M., Kaukonen, O., Kumpula, A., Narikka, J., Sintonen, H. & Ylipartanen, A. 2006. Sosiaali- ja terveyspalvelujen lainsäädäntö käytännössä. 2. uud. l. Kokoomateos. Tallinna: AS Paket.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uud. p. Helsinki: Tammi.

Kinnunen, M. Joko teillä on tietosuojavastaava. Tietosuojalehti 4 2008, 1. Viitattu 31.1.2010. http://www.tietosuojalehti.fi/Digipaper/OldNews.aspx?id=781.

L 17.8.1998/785. Laki potilaan asemasta ja oikeuksista. Viitattu 7.2.2010 ja 9.3.2010. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 22.4.1999/523. Henkilötietolaki. Viitattu 10.4.2010. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 22.9.2000/812. Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista. Viitattu 7.2.2010. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 28.6.1994/559. Laki terveydenhuollon ammattihenkilöistä. Viitattu 7.2.2010. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

Nikkilä, A-R. 2009. Tietojen tirkistelystä tuomitaan harvoin. Vantaan Sanomat 1.4.2009, 2.

Pääasia jäi sivurooliin PARAS—hankkeessa 10.3.2009. Artikkeli Elinkeinoelämän keskusliiton sivustolla. Viitattu 23.3.2010.
http://www.ek.fi/www/fi/2010Tapahtumat/PK_Valtuuskunta_27012010/index.php?

we_objectID=9187&pid=39022 , Elinkeinoelämän keskusliitto.

Salo, I., Kallio, A. 2010. Sähköinen resepti vihdoin käyttöön. Terveydeksi !, apteekkien asiakaslehti 1 / 2010, 8.

Solin, H. 2005. Lääkärin etiikka. Asiakirjajulkisuus ja tietosuoja sosiaali- ja terveydenhuollossa. Toim. I. Palman. Helsinki: Edita Prima.

Sorvari, H. 2001. Asiakastietojen suoja sosiaalihuollossa. Helsinki: Tammi.

Sorvettula, J., Tietoturvakysely 2009. Etelä-Pohjanmaan sairaanhoitopiiri. Sähköpostin liitetiedosto. Saatu 15.2.2010.

STM, Tietotekniikan hyödyntämisstrategia 1999. Viitattu 4.3.2010. Sosiaali- ja terveysministeriö.
http://pre20031103.stm.fi/suomi/tao/julkaisut/hyodstra/ttekнteksti.htm#31

Tammisalo, T. 2005. STAKES, Raportteja 5/2005. Sosiaali- ja terveydenhuollon tietojärjestelmien tietoturvan ja tietosuojan hallinnan periaatteet ja hyvät käytännöt. Viitattu 22.3.2010. http://www.stakes.fi/FI/Julkaisut/verkkojulkaisut/raportteja05/Ra5-2005.htm

Tammisalo, T. 2007. STAKES Työpapereita 11 / 2007. Tietoturvakoulutuksen esitysmateriaali.

Tietosuojavaltuutetun toimisto, Hyvä tietää julkaisu 7/2008. Viitattu 31.1.2010. http://www.tietosuoja.fi/42725.htm.

Witick, T., Meriläinen, M. 2009. Kokkolan kaupungin tietoturvaohje. Viitattu 4.2.2010.http://kokwww.kokkola.fi/dynastia/kokous/KOKOUS-2865-7-Liite-1.PDF

Ylipartanen, A. 2004. Tietosuoja terveydenhuollossa, potilaan asema ja oikeudet henkilötietojen käsittelyssä. 2. uud. p. Pieksämäki: RT-Print .

LIITTEET

Liite 1. Tietoturvaohje

HANKASALMEN SOSIAALI- JA TERVEYSTOIMEN TIETOTURVAOHJE

Tämä tietoturvaohje on tarkoitettu Hankasalmen kunnan sosiaali- ja terveyspalvelujen henkilöstölle, sen toimeksiannosta työskenteleville (esimerkiksi ostopalvelulääkärit ja ambulanssihenkilökunta) ja tietojärjestelmiä säännönmukaisesti käyttäville henkilöille, kuten opiskelijoille.

Tämä ohje antaa neuvoja tietoturvallisuuden toteuttamiseen omassa työssä ja muissa käytännön tuomissa tilanteissa.

Tietoturvallisuuden tavoitteet

Tietoturvallisuus on osa sosiaali- ja terveystoimen kokonaisturvallisuutta ja laatujärjestelmää. Tietoturvatoimenpiteillä turvataan yksilön, yhteisön ja ennen kaikkea asiakkaan ja yhteiskunnan etuja. Yhteiskunnan toiminnot ovat suurelta osin riippuvaisia tietojen käsittelystä ja sen erityyppisistä siirroista. Verkottuneessa tietoyhteiskunnassa on harva organisaatio enää vastuussa vain omasta tietoturvallisuudestaan.

Lainsäädäntö tietoturvallisuuden perustana

Julkishallinnossa käsitellään sekä julkista että salassa pidettävää tietoa. Suomen lainsäädännössä on laajasti tietoturvamääräyksiä ja tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain lisäksi useisiin muihinkin lakeihin ja asetuksiin. Yksityiselämän suoja ja toisaalta tiedon julkisuusperiaate ovat jo perustuslaissa säädettyjä perusoikeuksia.

Julkisuuslainsäädännön mukaan tieto on aina julkista, ellei se julkisuuslain tai muiden säännösten perusteella ole salassa pidettävää tietoa. Tietojen lainmukaisesta käsittelystä on aina huolehdittava.

Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä tai muulta laittomalta käsittelyltä. (Henkilötietolaki 32 §, Tietojen suojaaminen).

Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niissä olevien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laa-

tuun vaikuttavista tekijöistä. (Laki viranomaisen toiminnan julkisuudesta 18 §, Hyvä tiedonhallintapa).

Tietoturvallisuus käytännössä

Tietoturva kattaa kaikki sosiaali- ja terveyspalvelujen tietojenkäsittelytehtävät sisältäen myös toimistotyön ja siihen sisältyvän arkistoinnin. Tietoturvatoimet koskevat sähköisessä, puhutussa ja kirjallisessa muodossa olevan tiedon käsittelyä, luovutusta, siirtoa ja säilytystä.

Käytännössä tämä merkitsee mm. sitä, että osa tiedoista ja tietojärjestelmistä pidetään vain niiden käyttöön oikeutettujen saatavilla. Tällöin sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja. Tietojen käsittelyyn oikeutetutkin saavat käyttää tietoja ja järjestelmiä vain asianmukaisissa työtehtävissään.

Tietojen, palveluiden ja järjestelmien on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa muuttua, tuhoutua tai paljastua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- ja ohjelmistovikojen tai muidenkaan vahinkojen tai tapahtumien seurauksena. Tietojen ja järjestelmien on myös pysyttävä toiminnassa ja oltava saatavilla silloin, kun niitä tarvitaan sekä normaalioloissa että uhka- ja poikkeustilanteissa. Sähköisen asioinnin yleistyttyä on korostunut vaatimus, että asioinnin osapuolet tunnistetaan luotettavasti ja että asiointitapahtuman olemassaolo ja sisältö voidaan jälkikäteenkin todeta.

Työntekijän velvollisuus huolehtia tietoturvasta

Tietoturvallisuus perustuu siis lainsäädäntöön, ja siitä huolehtiminen ja siihen liittyvä osaaminen on jokaisen organisaatiossa työskentelevän velvollisuus. Suurimmat tietoturvallisuuden uhat liittyvät yleiseen kiireeseen, huolimattomuuteen, osaamattomuuteen tai muihin tietojärjestelmän käytön ja toteutuksen laadullisiin tekijöihin. Tietoturvallisuus on juuri niin hyvä kuin sen heikoin lenkki. Puutteellinen tietoturvallisuus vaarantaa kansalaisten, yhteisöjen ja asiakkaiden etuja ja aiheuttaa lisätyötä ja -kustannuksia. Tietoturvallisuutta kehittämällä parannetaan toimintojen luotettavuutta ja jatkuvuutta.

Tietojen käsittely

Asiakirjahallinto tarkoittaa organisaation toimintaan sisältyvien asioiden ja asiakirjojen käsittelyn ohjaamista niiden koko elinkaaren ajan. Asiakirjalliset tiedot ovat osa organisaation pääomaa, jolloin niiden laatuvaatimukset on turvattava, käsittelykäytännöt suunniteltava ja suojaaminen varmistettava. Asiakirjallisten tietojen laatuun liittyviä vaatimuksia ovat alkuperäisyyden, eheyden, luotettavuuden ja käytettävyyden takaaminen.

Tiedolla tarkoitetaan eri muodoissa tallennettavaa, käsiteltävää tai siirrettävää tietoa. Tieto voi olla yksittäisessä asiakirjassa, puheessa, sähköposti- tai tekstiviestissä, tietokannassa, tietokoneen tai matkapuhelimen muistissa tai vaikkapa yksittäisen työntekijän muistissa. Tietoa on tarkasteltava koko sen elinkaaren ajan, jolloin tietoturvan näkökulmasta merkittäviä käsittelyvaiheita ovat tiedon luominen, käyttäminen, muuttaminen, tallentaminen, siirtäminen, jakelu, kopioiminen, arkistoiminen ja lopulta tiedon hävittäminen.

Tietojen käyttöoikeus ja huolellisuusvelvollisuus

- Jokainen vastaa käsiteltävinä olevista asiakirjoista.
- Käsittele tietoja huolellisesti välineestä riippumatta, olipa tiedon välittäjänä henkilö, tietokone, paperi, puhelin tai telekopio.
- Muista, että voit käyttää ja käsitellä käyttöön saamiasi salassa pidettäviä ja arkaluonteisia tietoja vain työtehtävien hoitamisessa. Esimerkiksi henkilörekisterin tietojen käyttötarkoituksen vastainen käyttö on lainvastaista.
- Huomioi, että tietojärjestelmien käyttöä valvotaan ja tietojen käytöstä jää merkintä lokitietoihin ja että organisaation laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkossa aina organisaation edustajana.
- Kaikki ovat vaitiolovelvollisia toisten viesteistä, jotka on työtehtävissään vahingossa saanut tietoonsa.

Lokitiedot

Huomioi, että tietojärjestelmiin ja tietoverkon laitteisiin tallentuu yksityiskohtaista lokitietoa järjestelmien käytöstä. Tietoja käytetään ylläpidossa, vianmäärityksessä ja tietoturvallisuuden valvonnassa. Lokitietoja tarkastetaan väärinkäytösepäilyjen yhteydessä, asiakkaan pyynnöstä sekä säännönmukaisessa seurannassa. Mikäli tarkastuksen yhteydessä ilmenee huomautettavaa lokitiedoissa, vastaa kyseisen työntekijän esimies jatkotoimista. Säännönmukaisen tarkastuksen tavoitteena on tarkistaa henkilötietolain ja lain potilaan asemasta ja oikeuksista noudattaminen. Asiakastietojen ja potilasasiakirjojen lokitiedoista annetaan myös asiakkaalle, hänen sitä pyytäessään, selvitys siitä, kuka on käyttänyt hänen tietojaan tai kenelle on luovutettu häntä koskevia tietoja sekä mikä on ollut käytön tai luovutuksen peruste.

Ilmoitusvelvollisuus ja toiminta ongelmatilanteissa

- Mikäli hallussasi oleva laite, avain tms. katoaa tai varastetaan, ilmoita siitä välittömästi ao. vastuuhenkilölle oman vastuusi rajaamiseksi.
- Ilmoita aina haittaohjelmista (esimerkiksi virukset, madot ja troijalaiset) ja muista tietoturvallisuuteen liittyvistä epäilyistä, ongelmista tai suojauspuutteesta välittömästi tietohallintoon, jonka velvollisuutena on ryhtyä tarvittaviin toimenpiteisiin.
- Voit ilmoittaa myös turvallisuuteen liittyvistä epäilyistä tai ongelmista esimiehelle.

Seuraamukset

- Rikkomuksista tiedotetaan aina esimiehelle, joka ryhtyy jatkotoimiin.
- Vakavissa tapauksissa väärinkäyttö voi johtaa myös vahingonkorvausvaatimuksiin ja rikosoikeudellisiin seuraamuksiin.
- Seurauksena voi olla myös irtisanominen tai palvelussuhteen purku.

Tietoturva tietokoneella

Tietokoneen käyttö sisältää sekä oman työaseman että verkon kautta käytettävien palvelujen käytön. Jokaisen velvollisuus on seurata tietoturvallisuuteen liittyviä tiedotteita, tutustua ohjeisiin ja osallistua tarjottuun koulutukseen sekä pyytää tarvittaessa neuvoa organisaation asiantuntijoilta.

Tietokoneen käyttö

- Vastaat käyttäjänä omasta koneestasi.
- Vain tietohallintoyksikkö saa asentaa tietokonelaitteita verkkoon, siirtää niitä ja asentaa ja päivittää koneisiin ohjelmia tai tehdä niiden asetusmuutoksia.
- Hankasalmen kunnan hankkimia ohjelmia ei saa kopioida.
- Estä asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi (paina CTRL+Alt+Del ja valitse lukitse tietokone) aina, kun poistut pidemmäksi aikaa työpisteestäsi.
- Kirjaudu ulos sekä ohjelmistoista että koneeltasi työpäivän päättyessä ja sammuta kone.
- Työaseman käytössä on otettava huomioon tietoverkon ja palvelinlaitteiden rajoitettu kapasiteetti. Kuvia ja grafiikkaa saa välittää verkossa tai tallentaa palvelimelle vain työtehtävien vaatiessa ja sen jälkeen ne on poistettava välittömästi.

Käyttöoikeudet ja salasanat

- Kirjaudu koneelle aina omilla käyttöoikeuksillasi. Käyttöoikeus on henkilökohtainen ja se on yhdistetty juuri sinun henkilöllisyyteesi ja työtehtävääsi. Käsittele käyttäjätunnusta ja salasanaa samalla tavalla kuin pankkikorttiasi ja tunnuslukuasi. Salasanan tulee olla vähintään 8 merkkiä pitkä (Effica-järjestelmässä 5 merkkiä) ja sen tulee koostua pienistä ja isoista kirjaimista ja siihen tulee sisältyä vähintään 1 numero.

- Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi tai muita tunnuksiasi toisen henkilön käyttöön.
- Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen. Ota yhteys tietohallintoyksikköön, jos epäilet jonkun ulkopuolisen käyttävän konettasi.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen, jokapäiväisten sanojen käyttöä salasanana.
- Hyvä salasana on sinun helppo muistaa, mutta ulkopuolisen vaikea arvata.
- Älä kirjoita salasanoja muistiin ainakaan sellaiseen paikkaan, mistä ne ovat helposti löydettävissä.
- Älä käytä organisaation antamaa käyttäjätunnusta ja salasanaa Internetin palveluihin rekisteröityessäsi.

Tallentaminen ja varmuuskopiointi

- Tallenna tekemäsi työ mahdollisuuksien mukaan palvelimen verkkolevylle, jonka varmuuskopioinnista tietohallintoyksikkö huolehtii. Vältä tilannetta, jossa asiakirja tai muu aineisto olisi ainoastaan sellaisella laitteella tai tietovälineellä, jonka varmuuskopiointi on epäsäännöllistä (esimerkiksi oman tietokoneesi työpöytä tai kiintolevyasema).
- Tallenna työsi käyttäen välitallennuksia. Älä jätä työtä tallentamatta, kun poistut työpisteestä.
- Vältä turhaa tulostamista ja kopiointia, koska ylimääräiset kopiot, väliversiot ja epäkelvot kappaleet lisäävät tiedon vääriin käsiin joutumisen vaaraa ja siten turvaamistehtäviä erityisesti säilyttämisen tai hävittämisen osalta.
- Omia henkilökohtaisia tiedostoja ei pidä tarpeettomasti tallentaa työpaikan työasemaan tai palvelimelle.
- Luo itsellesi selkeä kansiorakenne.

Tiedon siirtäminen, tallennus- ja tiedonsiirtovälineen hävittäminen

- Tarkista organisaatiosi ulkopuolelta tuotu muistitikku, CD-/DVD- levy tai muu tietoväline virustorjuntaohjelmalla ennen käyttöä. Käyttäjä vastaa aina mahdollisista seuraamuksista käyttäessään ulkopuolelta tuotuja aineistoja.

- Mikäli aineisto luovutetaan tietovälineellä sähköisessä muodossa (CD-levy, muistitikku), tulee käytettävän tietovälineen ehdottomasti olla uusi ja aiemmin käyttämätön.

- Varmista, mihin tulostimeen tulostat ja missä tulostin sijaitsee. Hae tulosteesi verkkotulostimesta heti tulostuksen jälkeen.

- Hävitä säännöllisesti sähköisessä muodossa olevat tarpeettomat työkappaleet tiedostoistasi.

- Tuhoa oman tietokoneen roskakorin sisältö säännöllisesti ja varmista, että tietokoneen roskakoriin ei jää hävitettävää tietoa.

- Jos työaseman kiintolevy tai muu tallennusväline, kuten esimerkiksi muistitikku tai CD-/DVD- levy, rikkoutuu tai poistetaan muuten käytöstä, ei sitä saa laittaa roskakoriin. Huolehdi hävittämisestä toimittamalla tallennusväline tietohallintoyksikköön hävitettäväksi.

- Tietokonetta vaihdettaessa kovalevyjen tietojen hävittäminen on tietohallintoyksikön vastuulla, mutta käyttäjän on huolehdittava omien tiedostojensa poistamisesta tai kopioimisesta.

Internet ja sähköposti

Internet ja sähköposti ovat hyviä työvälineitä sekä tiedon hakuun että yhteydenpitoon. On kuitenkin muistettava, että sähköpostissa tai Internetissä ei itsessään ole mitään suojausta, vaan tiedot liikkuvat salaamattomina julkisessa verkossa. Sähköpostin ja Internetin käyttö vaatiikin käyttäjältä huolellisuutta. Hankasalmen kunnan sähköpostipalvelinjärjestelmässä toimii automaattinen viruksentorjunta, jonka avulla tietoturvauhat eliminoidaan. Internet ja sähköposti ovat työpaikalla tarkoitettu pääsääntöisesti työkäyttöön. On käytettävä vain sellaisia palveluita, jotka tiedetään asiallisiksi.

Sähköposti

- Käytä henkilökohtaiseen viestintään yksityistä sähköpostiosoitettasi.
- Ohjaa sähköisesti asioivat asiakkaat lähettämään käsittelyyn tulevat, vireille saatetut asiat organisaation sähköpostiin. Asiakkaan henkilökohtaisia tai arkaluonteisia asioita ei käsitellä sähköpostin välityksellä.
- Älä anna työsähköpostisoitettasi ulkopuoliselle muissa kuin työhön liittyvissä yhteyksissä.
- Työsähköpostia ei saa kääntää organisaation ulkopuoliseen sähköpostijärjestelmään esimerkiksi lomalle lähdettäessä.
- Huolehdi, että lähettämäsi sähköpostiviesti on kohdistettu oikeille henkilöille ja oikeisiin osoitteisiin, etenkin valmiita jakelulistoja käyttäessäsi.
- Mikäli saat toiselle henkilölle kuuluvan sähköpostin, ohjaa viesti oikealle vastaanottajalle ja ilmoita lähettäjälle vastaanottajan oikea sähköpostisoite. Muista, että sinulla on vaitiolovelvollisuus saamastasi viestistä. (Laki yksityisyyden suojasta televiestinnässä ja teletoiminnassa luku 4 § 2.)
- Lähetä sähköpostit tekstimuodossa ja käytä turvallisia liitetiedostomuotoja esimerkiksi rtf, jpg ja gif.

- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä. Tarvittaessa voit ilmoittaa tietohallintoyksikköön asiasta.

- Roskapostia voivat olla esimerkiksi sähköpostiin tilaamatta tulleet mainokset. Roskaposti kannattaa tuhota heti. Jos vastaat viestiin, tietää roskapostittaja sähköpostiosoitteesi toimivaksi ja jatkaa viestien lähettelyä ja voi lisäksi välittää osoitteesi myös muille roskapostittajille.

- Älä välitä ketjukirjeitä eteenpäin.

Internet

- Internetin välityksellä ei ole luvallista välittää salassa pidettävää tietoa.

- Internetistä voi ladata ainoastaan työkäyttöön tarvittavia tietoja.

- Palveluyhteyksiä voi käyttää henkilökohtaiseen asiointiin vapaa-aikana.

- Messengerin ja Skypen käyttö on kielletty.

- Vertaisverkkojen käyttö ja asennus työasemaan on kielletty.

- Laittomien tiedostojen lataaminen on kielletty (elokuvat, musiikki).

Virukset ja virustorjunta

Virus on haittaohjelma, joka voi liittää itsensä muihin ohjelmiin, tiedostoihin ja levykkeisiin. Virukset leviävät Internet-selaimen, sähköpostin liitetiedostojen, levykkeiden ja CD-levyjen välityksellä. Virus voi tuhota kovalevyn sisällön ja hävittää tietoa, varata muistitilaa, hidastaa koneen toimintaa tai näyttää ylimääräisiä viestejä sähköpostissa. Jokaisessa organisaation omistamassa tietokoneessa on konekohtainen viruksen torjuntaohjelma. Epäiltäessä työaseman olevan tietokoneviruksen saastuttama, työasemalla työskentely on lopetettava välittömästi. Tietokonetta ei tarvitse sulkea, mutta irrota lähiverkkokaapeli työasemastasi.

- Kirjoita ylös, mitä mahdollisessa ilmoituksessa tai varoituksessa luki.

- Ilmoita aina haittaohjelmista ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi tietohallintoyksikköön.
- Kerro, mitä olit tekemässä, kun kone alkoi toimia odottamattomasti.
- Toimi saamiesi ohjeiden mukaan.

Tietohallintoyksikön ja työnantajan toimet

- Tietohallintohenkilöstöllä on velvollisuus puuttua havaitsemiinsa epäkohtiin tai väärinkäytöksiin atk-järjestelmän käytössä
- Tietohallintohenkilöstöllä on tehtäviä suorittaessaan oikeus päästä kaikkiin niihin tiloihin, joihin laitteistoja on sijoitettu.
- Tietohallintohenkilöstöllä on oikeus keskeyttää/pysäyttää atk-järjestelmän tai sen osan toiminta.
- Työnantaja voi avata työntekijän sähköpostin tietyissä erityistapauksissa esimerkiksi pitkän sairausloman sattuessa tai kuolemantapauksessa. Sähköpostin avaus tapahtuu vain silloin, jos on vahvaa syytä olettaa, että työntekijälle on tullut tärkeää työhön liittyvää sähköpostia. Tällaisissa tilanteissa esimies ja tietoturvapäällikkö yhdessä tekevät päätöksen ja ottavat yhteyttä sähköpostin lähettäjään. Läsnä on aina kaksi henkilöä. Tapahtuman kulku kirjataan muistiin. Muutoin verkkoliikennettä seurataan tarvittaessa lakien mahdollistamissa puitteissa tästä etukäteen työntekijöitä tiedottaen.

Mistä saat lisätietoa?

Lisää tietoa tietoturvallisuudesta ja laeista on saatavissa mm. seuraavista lähteistä:

- Esimieheltä
- Tietohallintoyksiköstä
- Tietosuojavastaavalta (Sosiaali- ja terveystoimessa Marja Leena Hämäläinen)
- Lainsäädännöstä. Valtion säädöstietopankki (www.finlex.fi)
- Tietoturvallisuutta ohjeistavista ja säätelevistä organisaatioista, esimerkiksi valtiovarainministeriön Vahti-ohjeista

- Arkistolaitoksen ohjeista (www.narc.fi)
- Tietosuojavaltuutetuntoimiston ohjeista (www.tietosuoja.fi)