ASIAKASALOITTEINEN KÄYTÖNVALVONTA TERVEYDENHUOLLOSSA

Ylitarkastaja Arto Ylipartanen
Tietosuojavaltuutetun toimisto

Terveydenhuollon ATK-päivät 2013
28.5.2013, Turku

LUENNON AIHEET

1. Tietosuojan kehitys terveydenhuollossa

2. ”Asiakasaloitteinen käytönvalvontatapahtuma”
   – TSV:n ohjeiden esittely ja tavoitteet

1. TIETOSUOJAN KEHITYS TERVEYDENHUOLLOSSA

a) Kohti lailla säätelemistä (ennen 2000-lukua)
b) Tietosuojariskien lisääntyminen (2000-luvulla)
c) Tietosuojariskejä tasapainottavia tekijöitä

1. a) Kohti lailla sääntelemistä ennen 2000 -lukua:

- Hippokrateen vala lääkäreille (n. 2500 vuotta sitten)
- Suuret vallankumoukset (1700 –luvulla)
- Joukkotiedotusvälineiden kehittyminen (1890 –luku)
- II-maailmansota (1940 –luku)
- IT-teknologia (1960-luvulta alkaen)
- Henkilörekisterilaki (1.1.1988)
- Rikoslaki (tieto- ja viestintärikokset, 1995)
- Perusoikeusuudistus (1.8.1995)
- EU:n henkilötietodirektiivi (24.10.1995)
- Henkilötietolaki (523/99, 1.6.1999)

1. b) Tietosuojariskien lisääntyminen 2000-luvulla

Kohti sähköisiä valtakunnallisia keskitettyjä rekistereitä/arkistoja:

- eReseptilaki (61/2007, voimaan 1.4.2007);
  - Kelan Reseptikeskus/eResepti (Turku 20.5.2010)
- Terveydenhuoltolaki 9 § (1326/2010, voimaan 1.5.2011);
  - SHPn alueen yhteiskäytössä oleva potilastietorekisteri
  - Kunkin SHP:n alueen sisällä sijaitsevat julkisen terveydenhuollon toimintayksiköt
- eArkistolaki (159/2007, voimaan 1.7.2007);
  - Valtakunnallinen Kelan ylläpitämä potilastiedon sähköinen eArkisto otetaan käyttöön 1.9.2014 (Kuopiossa jo pilotointi suoritettu, 2012)
- Potilastietojen käsittelyn keskittymisen seurauksena tietosuojariskit kasvavat:
  - paljon tietoja
  - paljon potilaita
  - paljon käyttäjiä

1. c) Tarvitaan tietosuojariskejä tasapainottavia tekijöitä

- Vaakakupin toinen puoli / tasapaino ;
- eReseptiL 61/2007, 24 §, voimaan 1.4.2007 ja
- eArkistoL 159/2007, 20 §, voimaan 1.7.2007:

1) Tietosuojavastaava nimettävä organisaatioon
   - tehtävät ja toimenkuva määriteltävä
2) Vastaavan johtajan velvollisuus
   - annettava kirjalliset ohjeet työntekijöille potilastietojen käsittelystä + varmistuttava henkilöstön tietosuoja-osaamisesta
3) Rekisterinpitäjän velvollisuus käytönvalvontaan
   - lokitietojen kerääminen ja pitkäaikaissäilytys sekä potilastietojen käytön seuranta ja valvonta
4) Kansalaisen omien potilastietojen lokimerkintöjen eKatselu
   - nyt jo Kelan Reseptikeskus ja myöhemmin eArkisto

Tietosuojavastaavan nimeäminen

- Laki sähköisestä lääkemääräyksestä (61/2007, voimaan 1.4.2007, eReseptiL 24 §) ja
- Laki sosiaali- ja terveydenhuollon asiakastiedon sähköisestä käsittelystä (159/2007, voimaan 1.7.2007, eArkistoL 20 §)
  - em. lait ja lakien esityöt eivät juurikaan avaa tietosuojavastaavan tehtäviä
  - Tietosuojavaltuutetun toimiston ja STM:n ohjeistus oppaassa: ”Tietosuojavastaavan toimenkuva, tehtävät ja asema”; (http://www.tietosuoja.fi/27212.htm)

Tietosuojavastaavan tehtävät ja asema

- Osallistuu lisäresurssina rekisterinpitäjälle kuuluviin tehtäviin
  - hallinnollisen johdon apuna
  - henkilöstön tukena
- Tehtävien laajuus sovitaan erikseen työsopimuksessa ja tehtäväkuvassa
  - lähinnä potilastietojen käytön seuranta ja valvonta + raportit sekä suunnittelu- ja toimeenpanotehtäviä
    - Luvattoman käsittelyn epäilyä koskevassa selvittämisessä usein koordinoiva rooli
  - päätökset tekee hallinnollinen johto
  - hallinnollinen johto ei voi ulkoistaa rekisteripidon vastuita tietosuojavastaavalle
  - normaali työntekijän vastuu mm. työtehtävien laiminlyömisessä

2. ASIAKASLOITTEINEN KÄYTÖNVALVONTATAPAHTUMA

- TSV:n ohjeiden esittely ja tavoitteet

TSV:n ohjeiden esittely

TSV:n kotisivulla internetissä ”käytönvalvonnan ohjeet” http://www.tietosuoja.fi/60282.htm :

1) Yleisohje lokitiedoista (12.11.2012):
   – Lokitiedot henkilötietojen suojaamisen välineinä
2) Lokitietojen käsittelystä käytönvalvonnassa on laadittu ohje (12.11.2012):
   – Ohje asiakasaloitteisesta käytönvalvonnasta
3) Ohjeen yksityiskohtia on käsitelty erikseen muistiossa (12.11.2012):
   – Muistio käytönvalvontaohjeesta

Keskeisiä käsitteitä

- **Käyttöoikeusjärjestelmä =** tiedot luvallisista käyttäjistä, heidän käyttöoikeuksistaan ja tunnisteistaan
- **Lokitus =** suojattavan tietojärjestelmän käsittelytapahtumien kirjaaminen
- **Lokitiedot =** suojattavan tietojärjestelmän käsittelystä kerättävät käyttäjäkohtaiset merkinnät
- **Lokituloste =** lokitiedoista muodostettuja erilaisia tulosteita
- **Asiakaskohtainen lokituloste =** asiakkaan tietoihin kohdistuneet käsittelytapahtumat
- **Käyttäjäkohtainen lokituloste =** tietylle käyttäjätunnukselle kirjatut käsittelytapahtumat
- **Asiakas =** Suojattavan tietojärjestelmän rekisteröity
- **Käyttäjä =** Käytönvalvontajärjestelmän rekisteröity
- **Käytönvalvontajärjestelmä =** käyttöoikeusjärjestelmän ja lokitietojen muodostama looginen kokonaisuus

TSV:n ohjeiden tavoitteet

a) Taustaksi

a) Oikeudellisia lähtökohtia

b) Tavoitteet

c) Keskeiset kipupisteet

2. a) Taustaksi

- Syyttäjälausunnot
  - RL 38 luvun 10 §:n 3 mom.
  - Lokitiedot keskeinen todistusaineisto

- Havainnot
  - Rekisterinpitäjän käytännöissä eroja
  - Vaikeita tilanteita (usein kaksi tyytymätöntä osapuolta)
  - Luottamus

Luottamus potilastietojen lailliseen käsittelyyn

- EU:n Erobarometrit/luottamusindikaattori-mittaukset vuosina 2003 ja 2008
  - EU:n jäsenvaltioiden kansalaisten käsitys luottamuksesta (%) henkilötietojen käsittelyyn eri toimialoilla

EUROBAROMETRI / LUOTTAMUSINDIKAATTORI / prosenttia vastaajista (%)

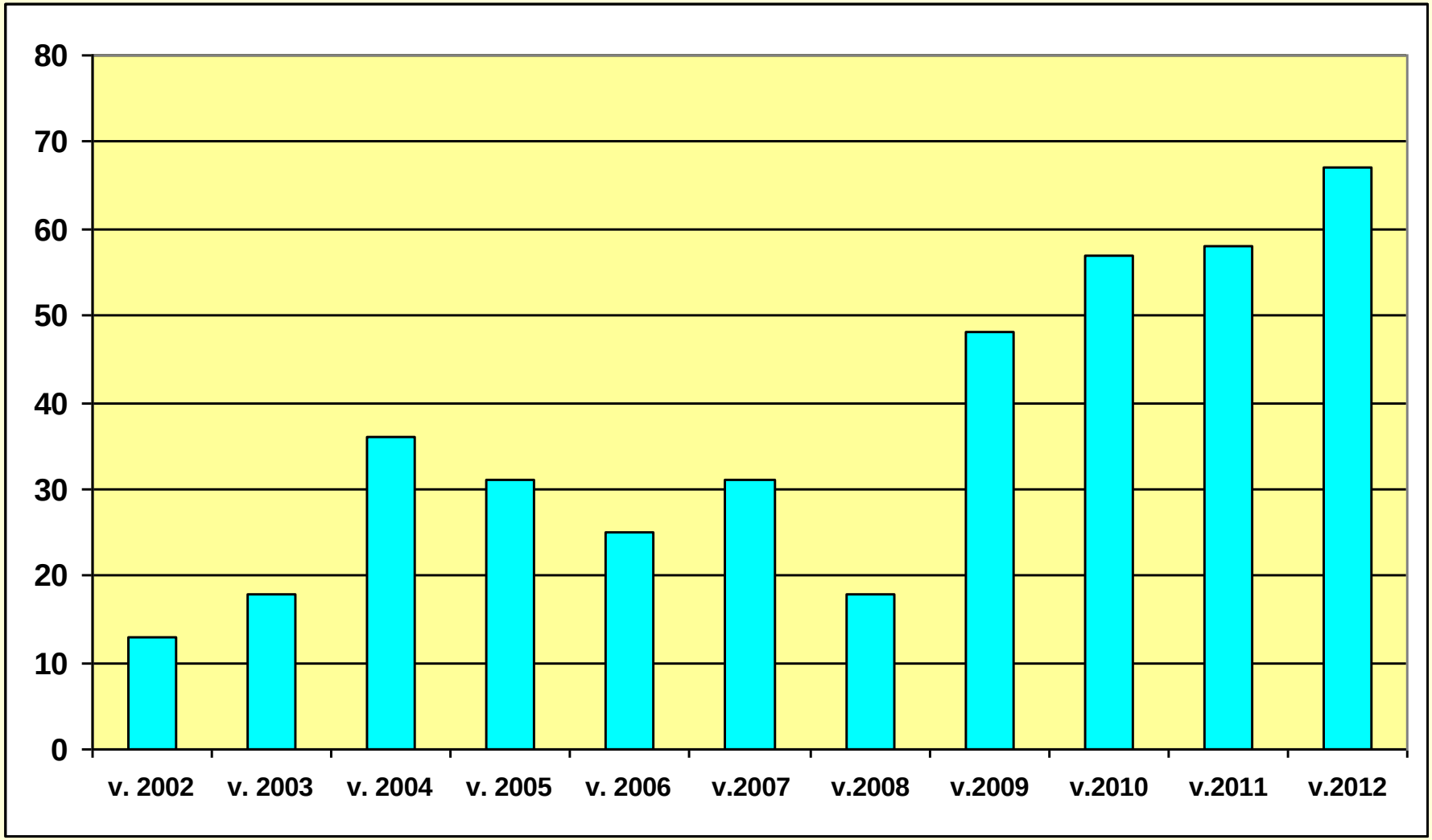
	v. 2003:				v. 2008:				
Toimiala:	SUOMI	EU-ka			SUOMI	EU-ka			
Terveydenhuolto	89	84			90	82			
Sosiaaliturva	80	69			87	74			
Vakuutusyhtiöt	72	42			80	51			
Luottokorttiyhtiöt	64	35			79	43			
Pankit, finanssiala	86	55			92	66			
Työelämä	64	55			73	63			
Luottotiedot	54	31			73	35			
Posti-, etämyynti	29	21			26	24			
Non profit	41	41			25	41			
Markkina- ym. tutkimus	42	43			33	33			
Poliisi	87	72			94	80			
Verotus	80	59			92	69			
Paikallishallinto	66	58			84	67			
Yleinen huoli tietosuojasta	49	60			64	36			

Luottamus potilastietojen lailliseen käsittelyyn

a) Tietosuojavaltuutetun lausunnot rikos-lausuntopyyntöihin syyttäjälle 2000 –luvulla

b) Poliisin tietoon tulleet tieto- ja viestintä-rikokset 2000 -luvulla

Tietosuojavaltuutetun antamat lausunnot rikoslausuntopyyntöihin syyttäjälle



Tieto- ja viestintärikokset
RL 38 luku / Poliisin tietoon tulleet

2. b) Oikeudellisia lähtökohtia

a) Henkilötietojen suojausvelvoite eli rekisterinpitäjän tekniset ja organisatoriset toimenpiteet (HetiL 32 §)
- henkilökohtaiset käyttövaltuudet / käyttäjätunnukset (http://www.tietosuoja.fi/46250.htm)
- työtehtävien mukaiset, rajatut käyttöoikeudet (HetiL 5,6,7 ja 32 §)
- uusilta työntekijöiltä salassapito ja käyttäjäsitoumus (esimies ja alainen)
- käytönvalvonnan toimintasuunnitelma (vastaava johtaja)

b) Sosiaali- ja terveydenhuollon erityislait (eReseptiL, eArkistoL, potilasasiakirja-asetus)
- Lokitietojen kerääminen ja pitkäaikaissäilytys
- Potilastietojen käytön seuranta ja valvonta

Oikeudellisia lähtökohtia

c) Euroopan ihmisoikeustuomioistuimen päätös 17.7.2008 asiassa I. v Suomi

- http://www.finlex.fi/fi/oikeus/eurooppa/feit/2008/20084401
- Potilaan käytännöllinen ja tehokas suoja puuttui
- Potilastietojen laittoman käsittelyn epäily on kyettävä jälkikäteen selvittämään

d) Kansalaisen omien tietojen katseluoikeus

- nyt jo Kelan Reseptikeskus ja
- lähitulevaisuudessa potilastiedon eArkisto

Oikeudellisia lähtökohtia

e) Ei ole kyse pelkästä asiakirjatilauspyynnöstä, vaan
  - nimenomaisesta rekisterinpitäjän sevittämisprosessista

f) Ei ole kyse työntekijän perusteettomasta valvonnasta, vaan lakiin perustuvasta
  - työntekijän oikeusturvan toteuttamisesta sekä
  - potilaan yksityisyyden suojaamisesta

EIT:n päätös 17.7.2008, I v. Suomi - lokitiedot sairaalassa

- Euroopan ihmisoikeustuomioistuimen päätös I v. Suomi:
  - koski suomalaisen sairaalan toimintaa v. 1992
  - Asianomistaja oli saanut HIV-tartunnan ja hän työskenteli samassa sairaalassa, jossa tartunta oli todettu
  - V. 1992 alussa asianomistajalle syntyi epäily, että työkaverit olivat tulleet tietoisiksi tästä sairaudesta
  - Jälkikäteisissä selvityksissä ilmeni, ettei potilastietojen yksittäisiä käyttäjiä kyetty selvittämään ts. tietojärjestelmällä ei ollut käyttäjiä yksilöivää käyttöoikeusjärjestelmää eikä sen avulla tuotettavaa ns. käyttölokitusta
  - V. 1992 ei ollut nimenomaisia säännöksiä – henkilörekisterilaissa-kaan – käyttäjäkohtaisesta kirjautumisesta ja käytönlokituksesta (STM A 99/2001, 4 § vrt. STM määräykset 1993:7)
  - Näin ollen säännösten valossa rekisterinpitäjiltä ei edellytetty v. 1992 käyttäjäkohtaisia käyttöoikeuksia ja käyttölokitusta ja sen pidempiaikaista säilyttämistä
  - Em. Ei estänyt Euroopan ihmisoikeustuomioistuinta antamasta langettavaa päätöstä henkilötietojen käytännöllisen ja tehokkaan suojan (“practical and effective protection”) puuttumisesta
  - Luvattoman käsittelyn epäily on kyettävä jälkikäteen selvittämään

Työnantajan tulee informoida henkilökuntaa käytönvalvonnasta :

- Työnantajan informointivelvollisuus käytönvalvonnasta ja seuraamuksista väärinkäyttötapauksessa eli läpinäkyvyys ja tietoisuus työyhteisössä:
  - teknisestä valvonnasta on ilmoitettava työntekijöille YT-menettelyssä (Laki yksityisyyden suojasta työelämässä, 759/2004, 21 §)
  - kun työntekijä otetaan palvelukseen (mm. otetaan salassapito- ja käyttäjäsitoumus)
  - potilastietojen käsittelyn ohjeistuksessa ja työntekijöiden koulutuksessa
    - mm. tietoisuus siitä, mikä on luvatonta käsittelyä
- Näin rekisterinpitäjällä on oikeus luvattoman käsittelyn seurantaan ja valvontaan

Työntekijät saatettava tietoisiksi mikä on laitonta käsittelyä :

1) Potilasrekisteritietojen käyttötarkoituksen vastainen käyttö
   - Potilaslaki 12 § määrittelee käyttötarkoituksen
     - hoidon suunnittelu, järjestäminen, toteuttaminen ja seuranta
     - Mahdolliset korvausvaatimukset ja tieteellinen tutkimus
   - Potilasasiakirja-asetus 4 § täsmentää sallittua käyttöä
     - Potilaan hoitoon ja siihen liittyviin tehtäviin osallistuvat
     - Siinä laajuudessa kuin heidän tehtävät ja vastuunsa sitä edellyttävät
2) Suojausmääräyksien vastainen käsittely (HetiL 32 §)
3) Oikeudeton salassapidettävän asian paljastaminen / levittäminen sivulliselle (mm. Potilaslaki 13 §)

Työntekijät saatettava tietoisiksi laittoman käsittelyn seuraamuksista :

a) Työoikeudelliset seuraamukset
   - huomautus, varoitus, irtisanominen

b) Tietosuojaoikeudellinen turvaamistoimenpide
   - käyttöoikeuksien rajaaminen

c) Rikos- ja vahingonkorvausoikeudelliset seuraamukset
   - henkilörekisteririkos, henkilörekisteririkkomus
   - salassapitorikos
   - edelliset virkarikoksina
   - mm. kärsimysvahinko

2. c) Tavoitteet

- Ymmärretään jälkikäteinen käytönvalvonta rekisterinpitäjävetoisena prosessina
  - Ei pelkkänä asiakkaan lokitietopyyntönä
- Tehdään näkyväksi tämä prosessi
  - Jotta sitä voisi kehittää jopa automatisoida
- Yritetään osoittaa tällaiseen käsittelyyn liittyvät oikeudelliset ja tietotekniset haasteet sekä resurssitarpeet

Selvittämisprosessin 3 osa-aluetta

- Osa A.; ASIAN VIREILLESAATTAMINEN JA ESIKÄSITTELY
  - Potilas ja tietosuojavastaava tai muu henkilö
  - Potilaan informointi selvittämismenettelyn periaatteista
  - Tavoitteena epäilyn riittävä yksilöinti/kohdentaminen
- Osa B.; PERUSSELVITTÄMINEN
  - Tietosuojavastaava/tietoturvapäällikkö tai muu henkilö
  - Riittävän yksilöidyn/kohdennetun epäilyn selvittäminen
  - Hankitaan näyttöä - näytön arviointi ja johtopäätökset
- Osa C.; TYÖNANTAJAN LOPPUTOIMENPITEET
  - Esimies/henkilöstöjohtaja sekä epäilty työntekijä
  - Työntekijän kuuleminen (+ luottamusmies)
  - Johtopäätökset, työoikeudelliset + jatkotoimenpiteet
  - Päätös tiedoksi työntekijälle ja potilaalle

Osa A.; ASIAN VIREILLESAATTA-MINEN JA ESIKÄSITTELY

- Potilas saattaa luvattoman käsittelyn epäilyn vireille ja potilaalle on informoitu selvittämisprosessin kulun yleiset periaatteet (vaihe 1.)
- Tavoitteena täsmennetty/riittävän tarkasti rajattu
  - ensisijaisesti tiettyyn henkilöön yksilöity tai aikaväliin kohdennettu luvattoman käsittelyn epäily (vaihe 2.)
  - tarvittaessa potilas kohdentaa epäilyään potilaskohtaisen lokitulosteen avulla (vaihe 3.)
- Mikäli epäilyn yksilöinti henkilöllisesti tai ajallisesti ei ole riittävää, voidaan potilaalle todeta, että selvitetään 2 vuoden ajalta käyttö
- Asia etenee ns. perusselvittämiseen (Osa B; vaiheet 4-6.)

Osa B.; PERUSSELVITTÄMINEN

- Perusselvityksessä hankitaan tarpeellinen käytettävissä oleva näyttö epäilystä / tutkittavasta kohteesta
  - lokituloste, ajanvaraus- ja hoitotiedot sekä tarvittaessa
  - työvuorolistat, kulunvalvonta, kameravalvonta ym. (vaihe 4.)
- Arvioidaan hankitun näytön perusteella tukeeko näyttö väitettyä luvattoman käytön epäilyä - tehdään johtopäätökset (vaiheet 5. ja 6.)
  - Näyttö ei tue epäilyä eli potilasaloitteisessa tapauksessa ilmoitetaan potilaalle ettei havaintoja luvattomasta käsittelystä
  - Jos näyttö tukee epäilyä niin laaditaan raportti toimenpiteitä varten tiedoksi epäillyn esimiehelle ja henkilöstöhallintoon

Osa C.; TYÖNANTAJAN LOPPU-TOIMENPITEET

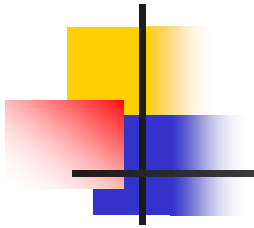
- Järjestetään epäillyn työntekijän kuuleminen suullisesti tai kirjallisesti (vaiheet 7. ja 8.)
  - Jos epäillyn kiistämisen perusteet uskottavia niin ilmoitetaan potilaalle ettei havaintoja luvattomasta käsittelystä
  - Jos epäilty myöntää väärinkäytön niin harkitaan selvittämisen laajentamista tekijäkohtaisen lokitulosteen avulla. Samoin, jos epäilty ei kykene esittämään uskottavia perusteita kiistämiselle (vaihe 9.)
- Päätetään työoikeudellisista toimenpiteistä ja siitä viedäänkö asia esitutkintaan poliisille (vaihe 10.)
  - Annetaan päätös tiedoksi työntekijälle ja potilaalle

2. d) Keskeiset ”kipupisteet”

- Miten henkilökunta sitoutetaan lokivalvontaan ?
- Miten asiakasta voidaan auttaa ?
  - Voiko organisaatio jättää selvityksen tekemättä, jos potilaan selvityspyyntö/epäily ei ole perusteltu/kohdennettu ?
- Selvittämisen sisäinen organisointi ?
- Mistä organisaatio saa riittävät/tarpeelliset lokitiedot ?
- Milloin organisaation tulee harkita selvityksen laajentamista mahdollisiin muihinkin asiakkaisiin kohdistuvaan väärinkäyttöön ?
- Kuka tekee asiassa tutkintapyynnön poliisille ?

YHTEENVETO

- Terveydenhuollon mahdollisuutena ja haasteena
  1. TIEVAn jaTSVn SWOT-analyysi 2011: Mahdollisuutena kun johto sitoutuu; laatii kirjalliset ohjeet ja kouluttaa henkilöstön sekä hyödyntää tietosuojavastaavan
     a. henkilöstön osaaminen ja oikeusturva paranevat sekä
     b. potilasturvallisuus ja yksityisyyden suoja paranevat.
  2. Ottamalla käyttöön mm. käyttäjäsitoumukset, sekä YT-menettelyn käytönvalvonnasta ja väärinkäytön seuraamuksista
     a. Mahdollistuu henkilöstön sitouttaminen ja
     b. tietoisuuden lisääminen paranee ennakollisin suojaustoimin
  3. Haasteena rekisterinpitäjän oma-aloitteinen ja suunnitelmallinen jälkikäteinen seuranta ja valvonta
     a. käyttölokien erilaisuus eri järjestelmissä sekä
     b. käytönvalvonnan automatisointi.



- KIITOS, mielenkiinnostanne !