Voimassa alkaen: 1.2.2015
Koskee kaikkia A-luokan tietojärjestelmiä joilta edellytetään auditointi ja vaatimustenmukaisuustodistus.

Käsitteet ”tietojärjestelmäpalvelu” ja ”tietojärjestelmä” kattavat tietojärjestelmätuotteet, erilaisilla palvelu- tai sovellusvuokrausmalleilla tarjottavat tietojärjestelmäpalvelut sekä sellaiset sovellusten tai tietojärjestelmien osat, jotka täyttävät A-luokkaan liittämisen kriteerit (myös silloin, kun niitä käyttää järjestelmä, joka ei muutoin itse suoraan täytä ko. kriteerejä)

Tietoturvavaatimukset:
- Kantaan liitettäville (A-luokka) potilastietojärjestelmille ja apteekkijärjestelmille ja välityspalveluille
- Järjestelmien käyttöympäristöön liittyvät vaatimukset (jos tietojärjestelmäpalvelun toimittaja vastaa käyttöympäristöstä, esim. SAAS-toimittajat)

Vaatimuksen kohderyhmä:
Y Yhteinen vaatimus kaikille A-luokkaan kuuluville tietojärjestelmäpalveluille
AP Apteekkijärjestelmän toiminnallisuuksia toteuttavan tietojärjestelmäpalvelun vaatimus
R Sähköisen lääkemääräysen käsittelyn toiminnallisuuksia toteuttavan tietojärjestelmäpalvelun vaatimus
A Potilastiedon arkistoon liittyvän tietojärjestelmäpalvelun vaatimus
VÄ Kanta-välityspalveluihin kohdistuva vaatimus

Vaatimuksen todentamistapa:
H Haastattelu
D Dokumentaatio
T Toiminnallinen testaus
V Validointi tai tekninen tarkastus (esim. lokit, sanomainstanssit, järjestelmän tuottamat raportit)
Mikäli todentamisessa on useita /-merkillä toisistaan erotettuja todentamistapoja, voidaan todentamiseen käyttää tilanteesta ja järjestelmästä riippuen erilaisia menettelyjä. Ensin mainittu on suositeltavin todentamistapa, mutta myös muut ovat hyväksyttäviä.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / sertifiointi	Lisätietoja
	Sähköinen allekirjoitus			
1 Y	Sähköisestä lääkemääräyksestä ja lääkintölaillisista lausunnoista tulee luotettavasti käydä ilmi sen	Sähköiset lääkemääräykset, näiden mitätöinnit ja korjaukset sekä lääkintölailliset lausunnot, todistukset sekä vastaavat asiakirjat on allekirjoitettava asiakastietolain mukaisella ammattihenkilön henkilökohtaisella, kehittyneellä sähköisellä	T: Varmennetaan, että järjestelmässä on toiminnallisuus, joka tarjoaa käyttäjälle kehittyneen sähköisen allekirjoituksen sähköisiin lääkemääräyksiin ja muihin henkilökohtaisesti allekirjoitettaviin	Allekirjoituksen voi toteuttaa niin, että allekirjoittajan voi allekirjoittaa sähköisesti yhdellä kerralla kaikki saman potilaan samalla kerralla

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / sertifiointi	Lisätietoja
	määrääjä tai allekirjoittaja	allekirjoituksella.Varmenteena on käytettävä terveydenhuollon ammattivarmennetta.	asiakirjoihin. T: Järjestelmän tulee vaatia allekirjoitusta ennen kuin lääkemääräys tai lääkintölaillinen lausunto tai sen muutos tai mitätöinti lähetetään Kanta-palveluihin.	määrätyt lääkemääräykset.
2 A	Asiakirjan muuttumattomuus tulee pystyä varmistamaan	Asiakirjojen muuttumattomuus tulee varmistaa sähköisellä allekirjoituksella. Muuttumattomuus on varmistettava sekä paikallisessa tallennuksessa että tiedonsiirrossa. Sähköiset potilasasiakirjat tulee allekirjoittaa organisaation tai tietoteknisen laitteen tekemällä kehittynyttä sähköistä allekirjoitusta luotettavuudeltaan vastaavalla allekirjoituksella, ns. järjestelmäallekirjoituksella. Järjestelmän tulee liittää asiakirjaan tietosisältöä vastaavat kuvailutiedot. Asiakirja (sen body-osio) allekirjoitetaan muuttumattomuuden takaamiseksi. Asiakirja ei saa sisältää asiakirjan sisältöä muuttavia elementtejä. Asiakirjan muodostamisesta tehdään lokimerkintä. Potilaskertomusta voidaan kerätä ja käsitellä järjestelmässä myös muussa kuin asiakirjamuodossa. Tällaisen potilaskertomuksen muuttumattomuus tulee taata ja muunnos asiakirjaksi tulee olla luotettava.	H/D: Todennetaan, onko järjestelmässä paikallisesti tallennettavia ei-allekirjoitettuja asiakirjoja, ja miten niiden muuttumattomuus varmistetaan. V/T/D/H: Tarkastetaan, että allekirjoitetun asiakirjan sisältö on yhtenevä sen kanssa, mitä merkinnän tekijä on nähnyt. H/D: Tarkastetaan miten muussa kuin asiakirjamuodossa olevien tietojen versiointi ja muutosten tallentaminen on toteutettu. V: Tarkistetaan, että asiakirjoista muodostuu lokimerkintä.	Lähetettävän ja vastaanotettavan asiakirjan vastaavuus tarkistetaan tarkemmin osana Kelan testausta.
3 AP	Lääketoimitusten allekirjoitukset	Lääketoimitukset, niiden korjaukset ja mitätöinnit sekä lääkemääräysten korjaukset ja mitätöinnit on	T: Järjestelmässä on toiminnallisuus, joka tarjoaa käyttäjälle kehittyneen sähköisen	Viittaus Laki 617/2009 Laki vahvasta sähköisestä

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / sertifiointi	Lisätietoja
		allekirjoitettava asiakastietolain mukaisella ammattihenkilön henkilökohtaisella, kehittyneellä sähköisellä allekirjoituksella. Varmenteena on käytettävä terveydenhuollon ammattivarmennetta. Lääkkeen toimittajan oikeus toimittamiseen tulee olla varmennettu ennen allekirjoitusta. Farmaseutin ja proviisorin tulee voida (mutta ei ole pakko) allekirjoittaa sähköisesti yhdellä kerralla kaikki saman potilaan samalla kerralla toimitetut lääkkeet.	allekirjoituksen käyttäen terveydenhuollon ammattivarmennetta. T: Järjestelmän tulee vaatia sähköistä allekirjoitusta ennen kuin toimitus tai korjaus hyväksytään tai mitätöidään. D/T/H: Oikeuksien tarkistaminen tulee suorittaa ennen allekirjoitusta. T: Järjestelmässä on saman potilaan kaikkien samalla kerralla toimitettujen lääkemääräysten allekirjoittamisen mahdollistava toiminnallisuus.	tunnistamisesta ja sähköisestä allekirjoituksesta. Voi myös olla päätetty, että järjestelmään ei implementoida toiminnallisuutta, joka mahdollistaa useiden toimitusten allekirjoituksen samalla kertaa.
	Tunnistaminen (Sulkulistat, ammatti-oikeuden rajoitus)			
4 Y	Käyttäjän tunnistaminen	Tietojärjestelmän käyttäjä tulee tunnistaa ja todentaa yksiselitteisesti. Tunnistamisessa tulee käyttää terveydenhuollon varmennepalvelua ja varmenteita. Erityistilanteissa voi käyttää käyttäjätunnusta ja vahvaa salasanaa. Järjestelmässä ei saa olla yleisiä ylläpito- tai muita vastaavia oikeuksia ja toiminnallisuuksia, joiden avulla järjestelmän käyttö ilman käyttäjän yksiselitteistä tunnistamista olisi mahdollista.	D/T: Tarkistetaan kuvaukset ja kokeillaan, miten järjestelmään tunnistaudutaan. D: Tarkastetaan kuvaukset roolien, käyttäjätietojen ja käyttöoikeuksien hallinnan periaatteista ja ohjeet niiden toteuttamisesta käyttäjäorganisaatioille. T: Testataan tunnistamista varmennekortilla.	Käyttäjätunnuksen ja vahvan salasanan käyttö mahdollista kun ei haeta tietoja Kantasta. Käyttäjätunnuksen ja salasanan käyttö mahdollista käytettäessä esim. ateriatilausjärjestelmää, jolla ei ole pääsyä muuhun potilaan hoitoon liittyvään tietoon.
5 Y	Tunnistautuminen järjestelmiin	Tietojärjestelmiin tulee tuotantoympäristöissä sallia kirjautuminen ainoastaan varmennekorttia potilaan hoitoon liittyviä tietoja käsitellessä tai vahvaa salasanaa käyttäen. Muuta kuin varmennekortilla	D/H/T: Tarkastetaan autentikointimekanismit; joko vahva tunnistautuminen (varmennekortti) tai vahva salasana.	Salasanan pituus min 10 merkkiä, merkkejä min. kolmesta luokasta, salasanan ikä 1-90 päivää, salasana ei

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / sertifiointi	Lisätietoja
		kirjautumista käytettäessä voi käyttää ainoastaan organisaation omassa potilastietojärjestelmässä olevia tietoja. Mikäli järjestelmän käyttäjillä on käytössä salasanat, tulee niiden olla vahvat ja vaihto säännöllistä. Hyväksyttävät vahvan salasanan parametrit ovat Vahti-ohjeistuksen Sisäverkko-ohjeen mukaiset (noudatetaan Vahti 3/2010 tai uudempi ohjetta). Vanhenemisvaatimukset eivät koske järjestelmän teknisten ylläpitäjien tunnusten salasanoja. Järjestelmä ei saa välittää vahvaa salasanaa muille järjestelmille.	D/H/T: Tarkastetaan salasanaparametrit järjestelmästä. D/H: Varmistetaan ettei järjestelmä välitä vahvaa salasanaa toiselle järjestelmälle.	saa olla sama kuin 5 edellistä salasanaa, salasana lukitaan esim. viiden virheellisen yrityksen jälkeen. Esim. vahvasta salasanasta Kanta-2015 Apteekkijärjestelmissä varmennekorttikirjautumista käytetään siinä vaiheessa, kun muodostetaan yhteys Reseptikeskukseen
6 Y	Varmenteiden validointi	Varmenteiden eheys, voimassaolo ja mahdollinen sulkulistalla olo on tarkistettava VRK:n tiedoista. Varmenteiden validointi koskee kaikkia järjestelmissä käytettäviä varmennetyyppejä: ammattivarmenteita, henkilöstövarmenteita, toimijavarmenteita, palvelinvarmenteita ja järjestelmäallekirjoitusvarmenteita. Sulkulista jota vasten validointi tehdään on haettava vähintään kerran vuorokaudessa.	D/H/T: Tarkistetaan, että järjestelmä tarkistaa varmenteiden eheyden, voimassaolon ja sulkulistalla olon VRK:n tiedoista. D/H/T: Tarkastetaan, että järjestelmä hakee sulkulistatiedot vähintään kerran vuorokaudessa (tai kulloinkin voimassa olevan VRK:n varmennepolitiikan mukaisesti).	Varmenteen eheyden ja tilan tarkistus tulee tehdä aina, ei vain kerran vuorokaudessa.
7 Y	Ammattioikeuksien ja niihin liittyvien rajoitusten tarkistaminen	Valviran tiedot käyttäjien ammattioikeuksista, käyttäjistä joilla on ammattioikeuksien rajoituksia ja ammattioikeuksien rajoituksista on tarkistettava Valvira:n ylläpitämästä sanomapohjaisesta attribuuttipalvelusta. Jos ammattioikeuksissa on rajoituksia, niin järjestelmä ei saa sallia kirjautuneen käyttäjän tehdä sellaisia toimia, jotka ovat rajoitusten	H/D/T: Todennetaan kuinka tiedot käyttäjistä joilla on ammattioikeuksia ja käyttäjistä joilla on ammattioikeuksien rajoituksia haetaan Valviran attribuuttipalvelusta vähintään kerran vuorokaudessa.	Testauksen kautta tapahtuvaa todentamista helpottaa mikäli auditointia varten on luotuna testihenkilöitä, joilla on rajoitteita.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / sertifiointi	Lisätietoja
		piirissä ulkopuolelle. Tiedot käyttäjistä joilla on ammattioikeuksia ja käyttäjistä joilla on ammattioikeuksien rajoituksia on haettava vähintään kerran vuorokaudessa. Valviran rajoitustietojen mukaiset ammattihenkilön ammattioikeuden rajoitukset tarkastetaan aina käyttäjää tunnistettaessa (sisäänkirjautuessa) eikä niitä tallenneta pysyvästi käyttöoikeustietoihin. Jos esimerkiksi lääkemääräyksen kirjoitusoikeuden omaavan terveydenhuollon ammattihenkilön oikeutta määrätä lääkettä on rajoitettu tietyn lääkevalmisteen osalta, järjestelmä ei saa sallia hänen kirjoittaa, korjata, lisätä, mitätöidä (tai purkaa lukitusta) sellaisia lääkemääräyksiä, joissa määrätään rajoituksen piiriin kuuluvaa lääkevalmistetta. Lääkemääräyksen toimittavan henkilön ammattioikeudet ja niiden voimassaolo on tarkastettava ennen sähköistä allekirjoitusta Valviran tiedoista. Ei-ohjelmallisesti toteutettavissa olevat rajoitustiedot on näytettävä käyttäjälle ja niistä on jäätävä lokimerkintä.	H/D/T: Todennetaan kuinka käyttäjän ammattioikeuksien rajoitukset tarkistetaan aina käyttäjän sisäänkirjautumisen yhteydessä. D/H/T: Todennetaan kuinka käyttäjän ammatilliset rajoitukset vaikuttavat järjestelmän käyttöön. D/H/T: Todennetaan kuinka järjestelmä rajoittaa lääkemääräyksen liittyviä toimenpiteitä käyttäjillä, joilla on ammattioikeuden rajoituksia. D/H/T: Todennetaan, kuinka järjestelmä näyttää käyttäjälle ei-ohjelmallisesti toteutettavat rajoitustiedot. D/H/V: Todennetaan, kuinka järjestelmä tekee ei-ohjelmallisesti toteutettavista rajoitustiedoista lokimerkinnän.	

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
	Käyttövaltuushallinta			
8 Y	Käyttövaltuushallinta	Järjestelmän tulee mahdollistaa käyttövaltuuksien antaminen eri toiminnallisuuksiin, käyttäjäryhmittäin ja työrooleittain järjestelmän käyttötarkoituksen mukaisesti. Kantaan liittyvät toiminnallisuudet tulee rajata käyttäjäryhmittäin ja käyttäjien työroolin perusteella. Vain ne henkilöt, joille käyttöoikeus on annettu, voivat käyttää ko toiminnallisuuksia. Järjestelmä ei vaadi laajoja käyttöoikeuksia toimiakseen. Järjestelmässä tulee olla poikkeustilanteiden hallinnan edellyttämät toiminnot, joilla käyttöoikeus voidaan tilapäisesti ohittaa (tarkoittaa, että joku toimenpide voidaan tehdä esimerkiksi pääkäyttäjän oikeuksin, vaikka ko. toimenpide ei kuulu pääkäyttäjän työtehtäviin). Tekijä ja tehty toimenpide tulee silti luotettavasti yksilöidä ja kirjata. Tieto ohitustilanteista tulee saada järjestelmästä esim. erilliseen luetteloon, jonka käsittelystä on ohjeet käyttöympäristön tietoturvapolitiikassa.	D/H/T: Tarkistetaan, miten järjestelmän käyttöoikeudet luodaan ja käyttääkö järjestelmä ensisijaisesti Valviran tarjoamia rajapintoja, ammattioikeuden tarkistamisessa. Tarkastetaan, että järjestelmä mahdollistaa toiminnallisuuksien rajaamisen mainituille käyttäjäryhmille ja työrooleille. D/H/T: Tarkastetaan järjestelmästä, että sinne voidaan määritellä erilaisia käyttöoikeuksia, käyttäjäryhmiä ja työrooleja. T+V: Testataan käyttöoikeuksia todellisuuden kaltaisessa tilanteessa. Tarkastetaan ohitustilanteiden toiminnallisuus sekä lokeihin syntyvät merkinnät (V). T/V: Tarkastetaan kuinka ohistustilanteesta saadaan tiedot erilliseen luetteloon.	Järjestelmässä itsessään tulee olla mahdollisuus hallita käyttöoikeuksia näiden vaatimusten edellyttämällä tavalla, tai vaatimukset tulee toteuttaa ulkoisen järjestelmän, esimerkiksi käyttöoikeuksien hallintajärjestelmän IAM:n avulla. Erityyppisissä järjestelmissä näitä vaatimuksia on toteutettava eri tavoin. Tietoturvavaatimusten määräyksessä todetaan: ’Mikäli vaatimus ei ole relevantti arvioitavan tietojärjestelmäpalvelun osalta, maininta tästä perusteluineen’
9 A	Opiskelijoiden oikeudet kirjata merkintöjä	Opiskelijat voivat tehdä potilaskertomusmerkintöjä. Potilastietojärjestelmässä tulee olla toiminto, jolla opiskelijoiden tekemät merkinnät hyväksytään. Opiskelijan kirjaamat merkinnät voidaan hyväksyä päiväkohtaisesti kokonaisuutena.	T: Tarkastetaan, että opiskelijoiden tekemien merkintöjen hyväksymiseen on toiminto.	Potilasasiakirja-asetuksen 6§ mukaan opiskelijalla on oikeus tehdä potilaskertomusmerkintöjä hänen toimiessaan laillistetun ammattihenkilön tehtävässä. Tällöin käyttöoikeuksiin merkitään ammattihenkilön rooli, ja näitä merkintöjä ei

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
				tarvitse tarkastaa. Työharjoittelujaksolla opiskelija toimii opiskelijan roolissa, hänellä on oltava opiskelijan rooli käyttöoikeuksissa ja terveydenhuollon ammattihenkilön tulee hyväksyä erikseen merkinnät.
10 Y	Pääkäyttäjien ja teknisten tukihenkilöiden oikeudet Kantaan	Pääkäyttäjillä on oikeus tarkistaa oman organisaationsa tietoja Kantasta virhetilanteissa. Tietojärjestelmäpalvelun tuottajalla on oikeus tarkistaa virhetilanteissa sen organisaation tietoja Kantansa, jonka lukuun järjestelmäasiantuntijat selvityksen aikana toimivat. Tietojärjestelmiin on toteutettava käyttövaltuudet siten, että Kanta-oikeudet rajataan ed mainituissa virhetilanneselvityksissä ainoastaan omien tietojen hakuun. Kaikki selvityksessä tehdyt haut tulee näkyä lokeista.	D/H/T: Tarkastetaan pääkäyttäjien ja tietojärjestelmäasiantuntijoiden oikeudet potilastietojärjestelmään ja Kanta-palveluihin. T/D/V: Varmistetaan, että selvityksissä tehdyt haut näkyvät lokeissa.	
11 Y	Oletustunnusten estäminen	Järjestelmissä ei saa olla aktiivisia oletustunnuksia ja muita oletuksena tulevia tietoturvallisuuden kannalta huonoja asetuksia. Mikäli järjestelmästä ei voida joltakin osin poistaa oletustunnuksia, oletustunnukset tai niiden salasanat on vaihdettava jos mahdollista.	D/H: Tarkastetaan kuinka on varmistettu tai ohjeistettu ettei järjestelmässä ole aktiivia oletustunnuksia tai muita oletuksena tulevia huonoja asetuksia.	
	Valvonta ja lokitus			

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
12 Y	Lokitietojen muuttumattomuus	Lokitietojen muuttumattomuus tulee varmistaa. Vaatimus koskee käyttölokia ja teknistä lokia. Järjestelmän tulee mahdollistaa lokitietojen muuttumattomuuden varmistaminen joko järjestelmätasolla tai organisaation omien toimenpiteiden kautta. Järjestelmän tulee mahdollistaa lokitietojen hävittäminen.	D: Tarkastetaan miten järjestelmän lokiympäristö on toteutettu.	Ohjeita lokitetojen käsittelyyn Vahti 3/2009. Tarkastuslista, liite 1. Tulee pyrkiä varmistamaan, että valvonnan kohteena olevat henkilöt eivät itse pääse muuttamaan lokitietoja. Lokitietojen säilyttämiseen ei toistaiseksi vaadita esim. kertakirjoittavaa mediaa.
13 Y	Käyttöloki	Tietojärjestelmä ylläpitää käyttölokia, josta löytyy riittävän yksityiskohtaiset tiedot tietojen haun ja käytön osalta (esim. tilanteissa, joissa järjestelmä hakee reseptikeskuksesta tai arkistosta enemmän tietoa kuin mitä käyttäjälle näytetään perusjärjestelmän suodattaessa tietoja). Tarkemmat vaatimukset käyttölokille kuvataan dokumentissa ’Potilastietojärjestelmien käyttötapaukset’ liite 5 Vaatimukset käyttölokeille Kaikki järjestelmän pääkäyttäjän ja ylläpitäjän asiakas- ja potilastietojen käsittelyyn liittyvät toimet järjestelmässä on lokitettava. Käyttölokin säilytysaika on vähintään 12 vuotta.	D/V: Tarkastetaan järjestelmän lokiasetukset ja määritysmahdollisuudet ja käydään läpi otos lokitiedoista. Varmistetaan joko järjestelmän tuottamasta lokitiedosta tai dokumentaatiosta, että vaatimukset täyttyvät.	Lokitiedot hävitetään kun ne eivät enää ole tarpeen asiakastietojen käytön ja luovutuksen lainmukaisuuden seuraamiseksi.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
14 Y	Tekninen loki	Kanta-palvelun ja sen asiakkaiden välisestä viestinnästä on pidettävä lokia. Lokia tulee pitää kaikissa järjestelmissä joiden kautta potilastietoja välitetään Kantaan. Järjestelmän tekniset virheet on lokitettava.	D/V: Tarkastetaan, että lokia kirjataan yhteyksien muodostamisesta.	
15 Y	Lokien seurantaväline	Tietojärjestelmässä on väline lokitietojen seuraamiseen tai järjestelmä mahdollista ulkopuolisen seurantavälineen liittämisen. Lokit on pystyttävä hakemaan saataville säännöllistä seurantaa ja valvontaa varten.	T/D/H: Tarkastetaan että järjestelmässä on väline lokitietojen seuraamiseen, tai järjestelmä mahdollistaa ulkopuolisen seurantavälineen liittämisen.	
16 Y	Verkkoliikenteen tietoliikenneprofiili	Verkkoliikenteen normaali tietoliikenneprofiili (baseline) on tiedossa; on olemassa menettely, jolla normaalista tietoliikenneprofiilista eroava liikenne pyritään havaitsemaan; järjestelmän osalta on pystyttävä kuvaamaan, millaista verkkoliikennettä normaali käyttö aiheuttaa.	D/H: Tarkastetaan, kuinka on kuvattu ja dokumentoitu järjestelmän tuottama normaali tietoliikenne ja onko kuvattu, miten normaalista tietoliikenneprofiilista eroava liikenne on mahdollista havaita.	
	Tietojen käsittely			
17 Y	Käyttöohjeet ja ohjeistus	Järjestelmän käyttötarkoituksen mukaista käyttöä sekä sen asennusta ja ylläpitoa varten tulee olla saatavilla tarpeelliset ohjeet. Ohjeiden on vastattava käytössä olevaa versiota. Mikäli ohjeet on tarkoitettu päivitettäväksi tai täydennettäväksi käyttöympäristökohtaisesti, on päivityksestä tai täydennyksestä oltava saatavilla selkeä ohjeistus.	D: Tutustutaan käyttö-, asennus- ja ylläpito-ohjeisiin ja tarkistetaan niiden vastaavuus järjestelmän auditoitavan version kanssa. D/H: Selvitetään ohjeistuksen päivitys-täydennys ja jakelukäytännöt.	
18 Y	Haettujen tietojen säilytys	Potilastiedon arkistosta haetut tiedot voidaan tallettaa paikalliseen järjestelmään siksi ajaksi kun potilaalla on hoitosuhde ao. yksikköön. Tiedot voidaan säilyttää yhtenä asiakirjana tai purkaa paikallisen järjestelmän käyttämään muotoon. Hoitosuhteen päättyessä tiedot	D/T/H: Tarkastetaan, että järjestelmässä on toiminto arkistosta ladattujen tietojen tuhoamiseksi. Toiminnan tulisi olla automaattinen ja liittyä palvelutapahtuman päättymiseen.	Lisätietoja Vahti-ohjeiden tietoturva-asetuksessa Lääkemääräyksiin liittyen välttämättömät tiedot lokeille

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
		on voitava tuhota niiden paikallisesta tallennustavasta riippumatta. Reseptikeskuksesta haettuja lääkemääräyksiin liittyviä asiakirjoja (mm. lääketoimitukset jne.) ei saa pysyvästi (seuraavia erikseen määriteltyjä poikkeuksia lukuun ottamatta) tallentaa terveydenhuollon tietojärjestelmään. Väliaikaisesti tallennetut tiedot tulee tuhota kokonaan välittömästi käytön jälkeen, kun niitä ei enää tarvita. Erikseen määritellyt poikkeukset: Järjestelmään voi kuitenkin tallentaa sellaiset tiedot, jotka ovat välttämättömiä lokeille asetettujen vaatimusten täyttämiseksi.	D/H: Tarkastetaan , että järjestelmä ei talleta lääkemääräyksiä tai niiden toimituksia pysyvästi, pl. mainitut poikkeukset.	asetettujen vaatimusten täyttämiseksi sisältävät sähköisten lääkemääräysten tunnisteet ja versionumerot sekä potilaskertomusjärjestelmällä luotujen lääkemääräysten uudet versiot ja mitätöintitiedot, mikäli nämä on tehty muulla potilaskertomusjärjestelmällä tai apteekin tietojärjestelmällä.
19 AP	Lääkemääräyksen toimitustiedon tallennus	Lääketoimituksen tulee olla onnistuneesti tallennettu Reseptikeskukseen ennen toimitustiedon tulostusta. Järjestelmä tulostaa toimitukseen liittyvän tarran vasta, kun se on tallentanut onnistuneesti toimituksen. Ennen lääkkeen luovuttamista lääkkeen ostajalle, tulee aina varmistua siitä, että lääketoimitus on tallentunut reseptikeskukseen.	D/T/H: Tarkastetaan, että toimitustietoa ei ole mahdollista tulostaa ennen kuin toimitus on onnistuneesti tallennettu. T/D/H: Tarkastetaan, että järjestelmässä on olemassa toiminnallisuus, jolla käyttäjä voi varmistua ennen lääkkeen luovuttamista, että lääketoimitus on tallentunut reseptikeskukseen.	
20 AP	Haettujen tietojen säilytys	Apteekki ei saa tallentaa tietojärjestelmäänsä reseptikeskuksesta hakemiaan tietoja pidemmäksi aikaa kuin mitä toimituksen käsittely tai muu lainmukainen tarkoitus vaatii. Poislukien: Lääkemääräysten tunniste- ja versiotiedot, Säädöksiin perustuvia tietoja, kuten suorakorvausta ja reseptipäiväkirjaa varten tarvittavat tiedot. Reseptikeskuksesta haetut tiedot tulee poistaa apteekkijärjestelmästä välittömästi käsittelyn päätyttyä. Myöskään muissa apteekeissa tehtyjen toimitusten	D/H: Tarkastetaan, että järjestelmä ei tallenna hakemiaan tietoja (poikkeuksia lukuun ottamatta) muuta kuin toimituksen käsittelyn vaatiman ajan.	

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
		tietoja ei saa tallentaa.		
21 AP	Tietojen näyttö	Lääkemääräyksestä näytetään ensisijaisesti uusin versio ja vain uusinta versiota voidaan käsitellä/muokata. Apteekkijärjestelmän tulee selkeällä visuaalisella tavalla näyttää lääkemääräyksen versiotiedot (esim. vanha, ei voimassaoleva versio).	T/D/H: Tarkastetaan, että: Järjestelmä näyttää reseptikeskuksesta hakemistaan lääkemääräyksistä ensisijaisesti eri versioista uusimman version. Järjestelmällä voi käsitellä/muokata vain uusinta versiota, ei muita lääkemääräyksen versioita. Järjestelmä näyttää lääkemääräyksen eri versiotiedot tavalla, joka näkyy käyttäjälle selvästi. Testitapaus: Haetaan henkilön lääkemääräyksen tiedot. Tarkastetaan, että em. kohdat hoidetaan asianmukaisesti vastausta käyttäjälle näytettäessä.	
22 AP	Tietojen näyttö	Järjestelmän tulee näyttää selkeällä visuaalisella tavalla käyttäjälle lääkemääräyksen ja toimituksen tilatiedot (mitätöity, lukittu, varattu jne..) sekä tilaan liittyvän selityksen, jossa sellainen on. Jos lääkemääräys on toimitusvarattu, varattu, annosjakelussa tai lukittu toisen apteekin toimesta, järjestelmän tulee näyttää varaustilan/lukituksen asettaneen apteekin tiedot.	T: Tarkastetaan, että: Järjestelmä näyttää lääkemääräyksen ja toimituksen tilatiedot ja tilaan mahdollisesti liittyvän selityksen selkeästi käyttäjälle. Järjestelmää näyttää varaustilan/annosjakelutiedon/lukituksen asettaneen apteekin tiedot, jos apteekki ei ole asettanut näitä tietoja itse. Testitapaus: haetaan lääkemääräyksen ja toimituksen tietoja, joilla on erilaisia tilatietoja (mitätöity, lukittu, varattu jne..) ja tarkastetaan, että järjestelmä näyttää nämä tiedot käyttäjälle selkeästi. Testitapaus: Haetaan lääkemääräys, jonka toinen apteekki on toimitusvarannut, varannut, merkinnyt annosjakeluun tai lukinnut ja tarkastetaan näyttääkö järjestelmä toisen apteekin tiedot	

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
23 AP	Reseptin tekninen korjaaminen	Farmaseutin ja proviisorin tulee voida tehdä teknisiä korjauksia reseptiin kuten iteroinnin siirtäminen oikeaan kenttään. Tekniset korjaukset, kuten iteroinnin siirtäminen oikeaan kenttään, eivät muuta reseptin sisältöä. Tekniset korjaukset voidaan tehdä ilman lääkärin hyväksyntää. Farmaseutin ja proviisorin on voitava tehdä lääkärin suostumuksella myös sisältöä muuttavia korjauksia. Resepti tulee tallentaa uutena versiona Reseptikeskukseen, jossa on muutettu vain korjattuja tietoja. ” 10§ Lääkettä apteekista toimittava proviisori ja farmaseutti voi lisäksi tehdä toimituksen yhteydessä tarpeelliset tekniset korjaukset. Jos lääkemääräyksen sisältö on epäselvä tai puutteellinen, on korjaukseen saatava lääkkeen määrääjän suullinen suostumus.” Resepti tulee tallentaa uutena versiona Reseptikeskukseen, jossa muutettu vain korjattuja tietoja	T: Todennetaan, että järjestelmä mahdollistaa tekniset korjaukset. V/D/H: Tarkastetaan, että korjattu resepti on muuttunut vain korjattujen tietojen osalta ja se tallennetaan uutena versiona.	
	Muut pakolliset vaatimukset			
24 Y	Istunnon katkaisu	Potilastietojärjestelmän on mahdollistettava kertomusjärjestelmän käyttöliittymän lukittuminen asiakasorganisaation määrittelemän ajan jälkeen.	T/D/H: Tarkastetaan, että kertomusjärjestelmän käyttöliittymä voidaan lukita tai yhteys katkaistaan asiakasorganisaation määrittelemän ajan mukaisesti.	Jos kyseisen pt-järjestelmän kaikki asiakkaat huolehtivat lukitsemisesta käyttöjärjestelmän tasolla, lukitustoiminnallisuutta ei tarvitse toteuttaa ptj-järjestelmään. Aikakatkaisu voi olla eripituinen eri käyttäjäryhmillä ja/tai

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
				käyttöympäristöissä (esim. leikkaussali vs poliklinikka). Aikakatkaisun raja määritellään palvelun antajan omavalvontasuunnitelmassa.
25 Y	Syötteen tarkastus	Järjestelmän tulee tarkastaa ennen tietojen hakua, että potilaan yksilöintitiedot ja mahdollinen lääkemääräyksen tunnus ovat oikeassa muodossa.	T: Tarkastetaan, että järjestelmässä on syötteen tarkastus, joka tarkastaa esimerkiksi henkilötunnuksen oikean muodon sekä lääkemääräyksen viivakoodin muodostumisen oikein. Testataan, että hakua ei voi tehdä virheellisillä syötteillä.	Jatkossa henkilötunnus voi olla muu kuin suomalainen (esim. epSOSin myötä).
26 Y	Tietojen päivitys Lääketietokannasta	Järjestelmän on mahdollistettava tietojen päivitys Lääketietokannasta vaaditulla tietosisällöllä ja intervallilla.	T/D: Tarkastetaan, että järjestelmä mahdollistaa tietojen päivittämisen Lääketietokannasta ja toiminto on kuvattu.	Fimean ohjeissa määritellään lääketietokannasta päivitettävä tietosisältö ja päivityksen intervalli (esim. 2*kk v. 2013).
27 Y	Tietojen päivitys THL:n koodistopalvelustasta	Kansallisesti ylläpidettävät perustiedot ja koodistot on päivitettävä THLn koodistopalvelusta.	T/D: Tarkastetaan, että järjestelmä mahdollistaa tietojen päivittämisen THL:n koodistopalvelusta ja päivittämisen tapa on kuvattu järjestelmän näkökulmasta.	Päivittämisen ei tarvitse tapahtua automaattisesti.
28 A	Hoitosuhteen varmistaminen	Potilastietojärjestelmä varmistaa käyttäjän hoitosuhteen potilaaseen. Normaalisti varmistus tuotetaan automaattisesti järjestelmässä olevien tietojen (esim. ajanvaraus) perusteella. Tekninen varmistus edellyttää, että palveluyksikössä tai rajatussa yksiköiden joukossa vähintään yksi henkilö on osallistunut potilaan tietojen kirjaamiseen käyttäjän lisäksi. Jos hoitosuhdetta ei voida varmistaa teknisesti, annetaan erityinen syy	T+V: Testataan hoitosuhteen teknisen varmistuksen toteutus. Tarkistetaan käyttöloki.	Myöhemmin tarkennetaan yksityisen ammatinharjoittajan käyttämän web-järjestelmän sekä sosiaalihuollon vaatimuksia.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
		tietojen käsittelylle.		
29 R	Sähköisen lääkemääräyksen potilasohjeen vastaanottaminen ja tallentaminen	Sähköisen lääkemääräyksen potilasohje voidaan tallentaa väliaikaisesti potilaskertomusjärjestelmään (mahdollisen tulostuksen epäonnistumisen varalta), mutta se on tuhottava 12 tunnin kuluessa tulostuksesta, jonka jälkeen sitä ei enää saa tulostaa.	D/H: Tarkastetaan, että sähköisen lääkemääräyksen potilasohjeet eivät tallennu pysyvästi ja että on olemassa toiminne, joka tuhoaa ko potilasohjeen viimeistään 12 tunnin kuluttua tulostuksesta.	
30 A	Rekisterien erottaminen ja muiden kuin terveydenhuollon rekisterien Kantaan arkistoinnin estäminen	Järjestelmässä tulee voida erotella eri palveluissa syntyvät rekisterit toisistaan. Muita kuin terveydenhuollossa, esim. sosiaalihuollossa syntyviä ja sosiaalihuollon rekistereihin kuuluvia potilastietoja ei toistaiseksi arkistoida Kantaan, joten ko. rekisterit tulee voida erottaa terveydenhuollon rekistereistä ja estää tallentaminen Kantaan.	D/H/V: Tarkastetaan, miten rekisterien erottaminen ja tallentamisen estäminen Kantaan on toteutettu	Rekisterien erottaminen ei edellytä erillistä tietokantaa.
31 Y	Kellojen synkronoinnin kuvaus	Kuvattava miten Kanta-palveluun yhteydessä olevien tietojärjestelmäpalvelujen kellojen synkronointi Mittatekniikan keskuksen toimittaman Suomen virallisen ajan kanssa on toteutettu.	D: Todennetaan tietojärjestelmäpalvelun tuottajan dokumentaatiosta.	Kanta-palvelut: tieto- ja sanomaliikenteen tietoturvavaatimukset.
32 AP	Reseptikeskukseen muodostetun yhteyden katkaiseminen	Apteekkijärjestelmän on huolehdittava, että yhteys reseptikeskukseen katkeaa, kun käyttäjä ei käytä järjestelmän reseptikeskukseen liittyviä toimintoja aktiivisesti 30 minuutin kuluessa (reseptikeskuksen tiedot eivät tämän jälkeen käytettävissä ilman tunnistamista uudelleen).	T/D/H: Tarkastetaan, että yhteys reseptikeskukseen katkaistaan, mikäli käyttäjä ei käytä järjestelmän reseptikeskukseen liittyviä toimintoja aktiivisesti 30 minuutin kuluessa	
33 AP	Syötteen tarkastus	Järjestelmän tulee tarkastaa ennen reseptikeskukseen suoritettavaa hakua, että käyttäjän (apteekin farmaseutti, proviisori tai farmasian opiskelija) syöttämät potilaan yksilöintitiedot ja lääkemääräyksen tunnus ovat oikeassa muodossa.	T/D/H: Tarkastetaan, että järjestelmässä on syötteen tarkastus, joka tarkastaan esimerkiksi henkilötunnuksen oikean muodon tai lääkemääräyksen yksilöintitiedoin oikean muodon. T: Testataan, että hakua ei voi tehdä	

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
			tiedoilla, jotka eivät ole muodoltaan oikeita	
34 AP	Potilaan suostumuksien dokumentointi	Tieto potilaan tai hänen laillisen edustajan antamasta suostumuksesta (esim. yhteenveto potilaan sähköisistä lääkemääräyksistä ja määräysten toimittamatta olevasta määrästä tai potilasohje) ja sen tyypistä (suullinen tai kirjallinen) lähetetään reseptikeskukseen.	T: Tarkastetaan, että järjestelmässä on ominaisuus, jonka avulla on mahdollista dokumentoida potilaan antamat suostumukset.	
35 AP	Suostumuksien kysely ja dokumentointi	Apteekin on annettava potilaan suullisen suostumuksen perusteella (potilaan pyynnöstä) tiedot hänen reseptikeskukseen tallennetuista lääkemääräyksistään ja määräysten toimittamatta olevasta määrästä (esim.Yhteenveto potilaan sähköisistä lääkemääräyksistä). Jos yhteenvedon noutaa joku muu kuin potilas itse tai hänen laillinen edustajansa, tulee noutajalla olla potilaan tai hänen laillisen edustajansa allekirjoittama suostumus.	T: Tarkastetaan, että järjestelmästä on mahdollista tulostaa yhteenveto potilaan sähköisistä lääkemääräyksistä	
36 AP	Tietojen päivitys	Lääketietokannan mukaiset tiedot lääkkeistä, korvattavista perusvoiteista, kliinisistä ravintovalmisteista ja määräaikaisista erityislupavalmisteista on päivitettävä toimitusohjelmistoihin kunkin kuukauden 1. ja 15. päivänä.	D/T: Tarkastetaan, että järjestelmä mahdollistaa lääketietokannan mukaisten tietojen päivittämisen. Tarkastetaan, että tiedot päivitetään vaaditulla intervallilla. Tarkastetaan onko tähän olemassa automatisoitu prosessi tai muu määrämuotoinen tapa, joka varmistaa päivitysten ajantasaisuuden	
37 AP	Valittavan lääkemääräyksen tilatiedon tarkistaminen	Apteekkijärjestelmä tarkistaa toimitettavaa lääkemääräystä valittaessa, että lääkemääräys ei ole lukittu, mitätöity, kokonaan toimitettu tai että siihen ei liity hyväksyttyä uusimispyyntöä (lääkemääräystä	T: Testataan, että järjestelmä tarkistaa onko valittu lääkemääräys lukittu, mitätöity, kokonaan toimitettu tai liittyykö siihen hyväksyttyä uusimispyyntöä. Jos näin on,	

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
		ei ole uusittu). Jos lääkemääräys on jossain edellä mainituista tiloista, järjestelmä ilmoittaa käyttäjälle, että ko. lääkemääräystä ei voida toimittaa ja syyn siihen. Järjestelmä tarkastaa myös, että lääkemääräys ei ole varattu, toimitusvarattu tai annosjakelussa toisessa apteekissa. Mikäli lääkemääräys on jossain edellä mainituista varaus-tiloista toiselle apteekille, apteekkijärjestelmä ilmoittaa käyttäjälle, että ko. lääkemääräystä ei voida toimittaa, lääkemääräyksen tilan ja tilan asettaneen apteekin tiedot.	järjestelmä ilmoittaa ettei ko. lääkemääräystä voi toimittaa ja syyn siihen. Lisäksi järjestelmä estää lääkemääräyksen toimittamisen. Käsitellään lääkemääräystä jonka varaustilatieto on jokin vaatimuksessa kuvatuista. T: Tarkastetaan, että järjestelmä ilmoittaa käyttäjälle ettei lääkemääräystä voida toimittaa ja ilmoittaa myös syyn. Lisäksi tarkastetaan, että järjestelmä estää kyseisen lääkemääräyksen toimittamisen.	
38 AP	Lääkemääräyksen uudistaminen	Järjestelmä mahdollistaa uusimispyynnön tekemisen sähköiseen lääkemääräykseen 16 kuukauden kuluessa alkuperäisen lääkemääräyksen antamisesta. Järjestelmä ei saa mahdollistaa uusimispyynnön tekemistä kun 16 kuukauden määräaika on kulunut umpeen	D/H+T: Tarkastetaan järjestelmädokumentaatiosta tai muuten, että järjestelmä mahdollistaa uusimispyynnön tekemisen 16 kuukauden kuluessa alkuperäisen lääkemääräyksen antamisesta. Testataan lääkemääräyksen uusimispyynnön tekemistä.	Nykyisen tulkinnan mukaisesti laista tulee kaksivaatimusta: - reseptejä pitää voida uudistaa 16 kuukautta - yli 16kk ikäisiä reseptejä ei saa voida uudistaa
39 AP	Reseptikeskuksesta haettujen tietojen tarkastelu	Lääketoimitusta tehdessä apteekkijärjestelmä saa hakea ja nähdä ainoastaan toimituksen kohteena olevan yhden henkilön tiedot kerrallaan. Apteekkijärjestelmä saa hakea ja nähdä toimittamisessa tarvittavat sähköisen lääkemääräyksen tiedot mukaan lukien sairausvakuutuskorvausoikeuteen vaikuttavat tiedot.	T/H/D: Tarkastetaan, että järjestelmällä ei voi hakea muiden kuin toimituksen kohteena olevan yhden henkilön tietoja reseptikeskuksesta. T/D/H: Tarkastetaan mitä tietoja järjestelmä hakee lääketoimituksia varten.	
	Sovellusturvallisuus			

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
40 Y	Turvallisen ohjelmoinnin periaatteet järjestelmän toteutuksessa	On pystyttävä kuvaamaan: 1. kuinka tietoturvatietous on huomioitu järjestelmän kehitysprosessin aikana 2. kuinka tietoturvauhat ja riskit on tunnistettu ja kontrolloitu 3. kuinka rajapinnat on testattu viallisilla syötteillä sekä suurilla syötemäärillä 4. kuinka valvotaan helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöä 5. kuinka katselmoidaan arkkitehtuuri ja lähdekoodi 6. kuinka tarkastetaan ohjelmakoodi esim. automaattisella staattisella analyysillä 7. kuinka ohjelmakoodien versionhallinta on toteutettu, kuinka vanhempiin ohjelmistoversioihin on tarvittaessa päästävissä ja kuinka ohjelmakoodin muutosten dokumentointi on toteutettu	D: Kohdat 1-2, 4-7 todennetaan tietojärjestelmäpalvelun tuottajan dokumentaation avulla. Dokumentaation ei tarvitse olla järjestelmäkohtaista. T: Kohta 3 todennetaan testausraportista. Testausraportti voi olla tietojärjestelmäpalvelun tuottajan toimittama tai sen tuottaminen voi olla osa auditointia.	Kansallisen turvallisuusauditointikriteeristön suositusten mukaisia kriteerejä ovat mm: 1) Ohjelmistokehittäjien riittävä tietoturvatietous on varmistettu. 2) Ohjelmistokehityksen aikana on suoritettu tietoturvauhka-analyysi ja havaitut riskit on joko kontrolloitu tai nimenomaisesti hyväksytty. 3) Rajapinnat (ainakin ulkoiset) on testattu viallisilla syötteillä sekä suurilla syötemäärillä. 4) Riippuen ohjelmointiympäristöstä, helposti ongelmia aiheuttavien funktioiden ja rajapintojen käyttöön on määritelty politiikka ja sitä valvotaan (esim. listat kielletyistä funktioista). 5) Arkkitehtuuri ja lähdekoodi on katselmoitu. 6) Ohjelmakoodi on tarkastettu automatisoidulla staattisella analyysillä. 7) Ohjelmakoodin versionhallinnan ja kehitystyökalujen eheys on varmistettu.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
41 Y	Yleisiin hyökkäysmenetelmiin varautuminen	Järjestelmässä on kuvattu miten varaudutaan yleisiin hyökkäysmenetelmiin siten, että palvelussa/sovelluksessa käsiteltävien suojattavien tietojen luottamuksellisuus tai eheys ei vaarannu.	D/H: Käydään haastatteluin ja dokumentaation pohjalta läpi se, mitkä yleisistä hyökkäysmenetelmistä ovat relevantteja tietojärjestelmän / tietojärjestelmäpalvelun kannalta ja kuinka niihin on varauduttu. Relevanttien hyökkäysmenetelmien osalta on pystyttävä kuvaamaan varautumistapa.	Esim. OWASP Top10 2013 Alkuvaiheessa ei edellytetä kattavaa ulkoista testausta.
42 Y	Sovelluksen käyttämät verkkoportit	Järjestelmässä ei ole auki tarpeettomia portteja eikä turvattomia, ei-salattuja protokollia. Liikenne on sallittu vain tarvittuun suuntaan.	D/H: Todennetaan haastatteluin sekä dokumentaatiosta miten sovelluksen käyttämät verkkoportit on määritelty ja suojattu ja miten varmistutaan siitä että tarpeettomia portteja ja turvattomia protokollia ei ole käytössä.	Alkuvaiheessa ei edellytetä kattavaa ulkoista testausta.
43 Y	Poikkeavan toiminnan havainnointi	Järjestelmässä tulee olla menettely, jolla luvaton käyttö ja luvattomat käyttöyritykset voidaan havaita.	D/H/T: Tarkistetaan, miten järjestelmässä voidaan havaita ja raportoida luvaton käyttö tai käyttöyritys.	
Järjestelmän <u>käyttöympäristöön</u> liittyvät vaatimukset, kun tietojärjestelmäpalvelun tuottaja tai Kanta-välityspalvelun tuottaja vastaa käyttöympäristöstä				
	Luottamuksellisuus ja eheys			
44 Y	Tiedonsiirron salaus ja tietoliikenteen luottamuksellisuus sekä eheys Kanta-palveluihin on turvattu	Sivulliset eivät saa saada selville suojattuja tietoja (myös asiointi terveyspalveluissa on salassa pidettävä tieto). Tiedot eivät saa muuttua tiedonsiirron aikana. Sähköisen lääkemääräyksen, potilasasiakirjojen ja niihin liittyvien luottamuksellisten tietojen siirtäminen kansallisiin palveluihin tai niistä muualle on salattu (esim. SSL/TLS) ja sähköisesti allekirjoitettu.	D/T: Tarkastetaan kuvaukset, asetukset ja/tai järjestelmän ohjeet salauksesta, allekirjoituksesta ja avainten/sertifikaattien käsittelystä järjestelmässä ja mahdollisten VPN-yhteyksien käsittelystä.	Kansaneläkelaitos antaa tekniset ohjeet hyväksyttävästä SSL/TSL-salaustasosta. Järjestelmien ja käyttäjäorganisaatioiden on sitouduttava noudattamaan ohjeita ja tekemään tarvittavat muutokset. Salaustasoa on sovellettava riittävän vahvalla algoritmilla ja avaimella.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
		Asiakirjat ja tiedot voidaan välittää salaamattomana käytettäessä point-to-point VPN- yhteyksiä.		Asia testataan tarkemmin viimeistään käyttöönottojen yhteydessä.
45 Y	Sähköisen viestinnän molemmat osapuolet tulee tunnistaa Yhteyden, osapuolten ja laitteiden tunnistaminen	Apteekit, palveluntuottajat ja käyttäjäorganisaatiot sekä niiden ko. palveluun liittyvät palvelimet tulee luotettavasti tunnistaa muodostettaessa yhteyttä Kanta-palveluun ennen sähköisen yhteyden aloittamista. Yhteyden osapuolten identiteetti varmennetaan ennen varsinaisen yhteyden muodostamista.	D/T/H: Tarkastetaan kuinka tunnistaminen ja toisen osapuolen identiteetin varmentaminen on toteutettu. Tarkastetaan sertifikaattien avainten bittimäärä ja salausalgoritmin toteutus.	Kansaneläkelaitos antaa tekniset ohjeet hyväksyttävästä salaustasosta (sertifikaattien avainten bittimäärä ja salausalgoritmi) Kanta-palvelut: Tieto- ja sanomaliikenteen tietoturvavaatimukset. Asia testataan tarkemmin viimeistään käyttöönottojen yhteydessä.
46 Y	Poikkeamien havainnointi	Palvelun antajilla on kirjallinen lokien keräys-, luovutus-, hälytys- ja seurantapolitiikka/-ohje, joka on muodostettu ottaen huomioon toiminnan vaatimukset. Järjestelmän on mahdollistettava lokien kerääminen ja se voi tukea myös luovutus- hälytys- ja seurantatoimintoja.	D: Tarkastetaan, kuinka järjestelmän lokien kerääminen ja hallinta on toteutettu ja saatavilla, tukeeko se muita lokien valvonnan toimintoja.	
47 Y	Verkkoyhteyden suojaus	Liittyvän organisaation järjestelmien tulee olla palomuurilla suojatut. Kyseeseen voi tulla joko tilallinen palomuuri tai erilliset sovelluspalomuurit. VAHTI 2/2010, liite 5, vaatimus 2.5. Vähintään perustason vaatimukset. Mikäli organisaatiosta on useita yhteyksiä reseptikeskukseen / arkistoon, riittää kun ne ovat saman palomuurin takana. Järjestelmän on tuettava verkkoyhteyden suojaamista palomuurilla ja mikäli se vaatii erityisiä palomuuriasetuksia, ne on kuvattava.	D: Tarkastetaan, kuinka järjestelmä tukee verkkoyhteyden suojaamista palomuurilla, sisältääkö se erillisiä palomuuripiirteitä jakuinka mahdollisesti vaadittavat palomuuriasetukset on kuvattu. .	VAHTI 2/2010, liite 5, vaatimus 2.5

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
48 Y	Hallintayhteydet järjestelmään	Mikäli järjestelmään ylläpidollisista tai muista syistä sallitaan etäyhteyksiä, yhteydet järjestelmään tulee olla salattuja päästä päähän (ylläpitäjän koneelta ylläpidettävään järjestelmään asti) esim. VPN-tunnelilla. Lisäksi etäyhteyksien käyttäjät tulee tunnistaa käyttämällä luotettavaa vahvaa tunnistautumismenetelmää (ei pelkästään salasanaa ja käyttäjätunnusta) Hallintayhteydet järjestelmään tulee joko salata vahvasti tai rakentaa käyttäen omaa suojattua verkkoa hallintayhteyksille. Vaatimus koskee myös sisäverkon yhteyksiä.	D/H: Selvitetään ja kuvataan, onko järjestelmään ylläpidollisia tai huollollisia etäyhteyksiä, ja miten mahdolliset etäyhteydet järjestelmään on toteutettu. D/H: Tarkastetaan että mahdolliset hallintayhteydet on toteutettu salatulla yhteydellä, esim. VPN, SSH, SSL/TLS tai hallintayhteyksille on oma suojattu verkkonsa.	
49 Y	Salaukseen käytettävät avaimet pysyvät vain haluttujen tahojen käytössä Käyttöympäristön puolelle	Organisaation järjestelmien tulee tukea hyvien käytäntöjen mukaista salausavainten ja sertifikaattien hallintaa, jonka tulee kattaa a) Avainten/sertifikaattien luonti (tai siirto järjestelmään) b) Avainten/sertifikaattien säilytys c) Avainten/sertifikaattien käyttö d) Avainten/sertifikaattien tuhoaminen/arkistointi/poisto	D: Salausavainten hallintaan liittyvä dokumentaatio, tarkastetaan että vaaditut hyvät käytännöt a-d toteutuvat.	Vaatimus koskee vähintään Kanta-palveluhin liittymisessä käytettyjä avaimia ja sertifikaatteja.
50 Y	Järjestelmän kovennus	Järjestelmissä ei saa olla ylimääräisiä palveluita päällä eikä turhia avonaisia portteja. Organisaatiolla tulee olla olemassa määritetty laitekokoonpano ja järjestelmäalusta (esim. käyttöjärjestelmä ja tietokannat), joiden mukaan järjestelmän tietoturva-asetukset tehdään.	D/H: Tarkastetaan, miten järjestelmät kovennetaan ja testataan ennen käyttöönottoa ja ettei niissä ole ylimääräisiä palveluita tai turhia avonaisia portteja, tai kuinka tämä on ohjeistettu. D: Tarkastetaan, kuinka laitekokoonpano ja järjestelmäalusta sekä niiden tietoturva-asetukset on kuvattu.	Esitettyä vaatimusta tarkempi todennustapa on palveluiden skannaaminen ja alustan konfigurointiasetusten tarkastaminen, jollaista ei kattavasti toistaiseksi edellytetä.

#	Kriteeri / kontrollitavoite	Vaatimus/Kontrolli	Vaatimustenmukaisuuden todentaminen / auditointi	Lisätietoja
51 Y	Haittaohjelmasuojaus palvelimilla	Palvelimet ja työasemat, joilla järjestelmät toimivat, tulee olla suojattu haittaohjelmilta. On suositeltavaa, että haittaohjelmien torjuntaohjelmat päivittyvät automaattisesti.	D/H: Tarkastetaan että palvelimilla on käynnissä haittaohjelmien suojaus, joka pystyy tunnistamaan virukset, vakoiluohjelmat ja muut haittaohjelmat ja että suojaus päivittyy säännöllisesti ja mahdollisuuksien mukaan automaattisesti.	Vaatimus koskee sellaisia järjestelmiä, jotka tyypillisesti ovat alttiita viruksille, ja joihin on saatavilla virustarkastusohjelma.