Mittefunktsionaalsed nõuded

ID	Nõude liik	Kokkuvõte
PADIMF-1	**Ajakohasus**	Infosüsteeme uuendatakse (update & upgrade) ja paigatakse (patch) regulaarselt (nt. kord kuus).
PADIMF-2	Ajakohasus	Kõikide arendamisel kasutatavate komponentide (rakenduse, andmebaasi, kolmanda osapoole) eluea lõpp (inglise k End-of-Life, EOL) ei tohi teadaolevalt olla vähem kui 4 aastat.
PADIMF-3	Andmekaitse	Isikuandmete töötlemisel lähtub digiteeninduse platvormi pidaja talle antud juhistest ning õigusaktides sätestatust, sealhulgas Euroopa Parlamendi ja Nõukogu määruse (EL) 2016/679 (isikuandmete kaitse üldmäärus ehk GDPR) artiklis 28 toodud tingimustest. Andmetöötluskokkulepe dokument on koostatud ja poolte vahel sõlmitud.
PADIMF-4	Andmekaitse	Volitatud töötleja on kohustatud rakendama isikuandmete turvalisuse meetmeid nii, et töötlemine vastaks andmekaitsenormides (sh GDPR art 32) toodud nõuetele, võttes mh arvesse isikuandmete töötlemise laadi ja volitatud töötlejale kättesaadavat teavet. Volitatud töötleja nimetab, milliseid turvalisust tagavaid meetmeid ta rakendab.
PADIMF-5	Andmekaitse	Volitatud andmete töötlejal peab ulatusliku terviseandmete töötlemise korral (alates 5000 isikust) olema andmekaitsespetsialist. Andmekaitse spetsialisti andmed peavad olema registreeritud äriregistris.
PADIMF-6	**Krüptograafia**	Infosüsteemide vaheline teabe transportimine (in transit) toimub ajakohaseid (RIA krüptograafiliste algoritmide uuring) krüptograafilisi protokolle kasutades. *Näiteks välistes võrkudes kasutatakse andmeside kaitseks näiteks TLS-i ja HTTPS protokolli läbivalt või kaughoolduseks ja -halduseks kasutatakse sideprotokollidena vähemalt SSH v2, TLS v1.2, SNMP v3, IPSec IKEv2-ga.*
PADIMF-7	Andmekaitse	Enne kasutajate andmete töötlemist (või pärimist) peab kasutajalt küsitama vastavat nõusolekut kasutades RIA Nõusoleku teenust.

PADIMF-8	**Jälgitavus**	Infosüsteemide info allikas, selle muutmise ja hävitamise fakt on tuvastatavad ehk kõik teabe töötlemistoimingud on logitud ja säilitatud (nt aasta). (ISKE T2 või EITS I2 nõue)
PADIMF-9	**Jälgitavus**	Infosüsteemide turvasündmusi (sh pääsulogi) logitakse, säilitatakse (nt aasta) ja seiratakse regulaarselt.
PADIMF-10	Kasutajaliides	Kasutajaliides peab vastama WCAG kehtiva versiooni AA tasemele. Vastavust hinnatakse Google Lighthouse tööriistaga ja tulemus peab olema vähemalt 90%, kusjuures hindamiskriteeriumiteks on *accessibility* ja *performance* nii mobiili vaates kui desktop vaates.
PADIMF-11	**Pääsuhaldus**	Infosüsteemide info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele ja juurdepääs teabele on lubatav juurdepääsu taotleva isiku teadmisvajaduse korral. (ISKE S2 või EITS C2 nõue)
PADIMF-12	**Käideldavus**	Infosüsteemi töökindlus on vähemalt 99% ehk lubatud summaarne seisak kuni 2h nädalas või aastas kokku kuni 9h. (ISKE K2 või EITS A2 nõue)
PADIMF-13	**Küberturve**	Infosüsteemidele on paigaldatud minimaalselt ajakohane kahjurvaratõrje tarkvara (antiviirus) ja lokaalne lubamatu side kaitse (tulemüür).
PADIMF-14	**Küberturve**	Võtmeid, sertifikaate, salasõnu ja muud sensitiivset teavet ei talletata tarkvara koodis, koodihoidlas või veebidokumentides.
PADIMF-15	**Pääsuhaldus**	Infosüsteemide identiteedi- ja ligipääsuõiguste haldus võimaldab kaksikautentimist (2FA) või mitmikautentimist (MFA).

PADIMF-16	**Pääsuhaldus**	Infosüsteemide kasutajakontod määratakse identiteedipõhiselt ehk kõik kontod on seotud konkreetsete isikutega (isikustatud kontod).
PADIMF-17	**Krüptograafia**	Infosüsteemides teabe salvestamine/talletamine (at rest) toimub ajakohaseid (RIA krüptograafiliste algoritmide uuring) krüptograafilisi protokolle kasutades. *Näiteks failisüsteemi põhist krüpteeringut (nt Encrypting File System, EFS) või kõvaketta krüpteerimist (nt Windows BitLocker, FileVault) kasutades.*
PADIMF-18	**Taastevõime**	Infosüsteeme ja teavet varundatakse regulaarselt (nt. kord päevas) ning taasteteste teostatakse regulaarselt (nt. kord kvartalis).
PADIMF-19	**Jälgitavus**	Infosüsteemide info õigsuse, täielikkuse ja ajakohasuse kontrolle teostatakse regulaarselt või on teostatavad vastavalt vajadusele. (ISKE T2 või EITS I2 nõue) ***Peamiselt mõeldakse selle nõude all logide olemasolu ja tervikluse kontrollimise võimalikkust.*** *Näiteks salvestatakse logisse või logifaili ajatemplid (timestamp) iga kord kui toimub info loomine, muutmine või hävitamine.* *Lisaks infot või faile räsitakse (hashing) nende transportimisel või salvestamisel ja antud räsiväärtusi (hash) võrreldakse hilisema kontrolli raames.* *Andmete edastamisel kasutatakse andmete tervikluse tagamiseks kontrollkoodide (nt CRC) võrdlemist või tundliku teabe tervikluse säilitamiseks kasutatakse digitaalsignatuure ja ajatempleid.*
PADIMF-20	**Turvatest**	Infosüsteem on läbinud enne toodangusse minemist turvatestimise ehk läbistustestimise (ingl penetration testing). Veebirakenduste turvalisust kontrollitakse ja testitakse regulaarselt (nt OWASP TOP 10). *Minimaalne nõue on OWASP ASVS Level 1 ehk kui turvatestimist pole kunagi varem teostatud ja OWASP ASVS Level 2 siis, kui turvatestimist on juba varem teostatud.*

Funktsionaalsed nõuded

ID	Nõue
PADIF-1	Patsient ja meditsiiniasutus (töötajad) saavad suhelda sõnumite, teadete, piltide ja juhtmaterjalide näol, sh on võimalus pöördumisi täiendada nii patsiendi kui ka meditsiiniasutuse töötaja poolt
PADIF-2	Patsient saab küsida retseptipikendust
PADIF-3	Patsient saab töövõimetuslehe avamise soovi edastada
PADIF-4	Patsiendile kuvatakse informatsioon milleks ja kuidas digiteenindusplatvormi kasutatakse, lisaks missuguseid alternatiivseid kanaleid saab veel kasutada oma perearsti poole pöördumiseks
PADIF-5	Patsient saab tellida tervisetõendeid (tervise-, relva jms)
PADIF-6	Patsient saab automaatse kinnituse pöördumise edastamise kohta

Kasutajatugi

ID	Nõue
PADIF-7	Digiteenindusplatvormi ettevõte peab pakkuma kasutajatele (nii patsiendile kui tervishoiuteenuse osutajale) kasutajatuge, mille sisuks on tehnilise- ja kasutamisega seotud pöördumiste lahendamine.
PADIF-8	Kasutajatoe pöördumiste reageerimise aeg võib olla kuni 24h ja sellekohast statistikat peab saama välja võtta.

Statistika

ID	Nõue
PADIF-9	Platvormi haldaja peab Tervisekassa pöördumisel väljastama statistikat CSV või mõnes muud kokku lepitud andmeid töödeldavas formaadis.
PADIF-10	Tervisekassa võib teenuste kvaliteedi ja põhjendatuse kontrolliks küsida platvormi pidajalt kasutajate meiliaadresse tagasisideküsitluste saatmiseks.

PADIF-11	Platvorm peab hoidma ajalugu, et oleks võimalik välja võtta vähemalt järgnevat statistikat (*Patsientide pöördumised TTO poole platvormi vahendusel*): • *Liitunud nimistute arv - kuude kaupa;* • *Patsientide pöördumiste koguarv - kuude kaupa;* • *Patsientide pöördumiste keskmine arv nimistu kohta - kuude kaupa;* • *Patsientide pöördumiste kellaajaline / päevaline jaotus - kuude kaupa;* • *Keskmine pöördumise vastamise aeg - kuude kaupa.*