



Sveikatos duomenų mokslinės analitikos informacinės sistemos (SDMA IS) sukūrimo ir įdiegimo pirkimas

Techninė specifikacija

Kaunas, 2026

Turinys

1.	Santrumpos ir sąvokos.....	2
2.	Dokumento paskirtis.....	4
3.	Pirkimo kontekstas	4
3.1	Pirkimu įgyvendinamas projektas	4
3.2	Projekto tikslas, sprendžiamos problemos.....	4
4.	Pirkimo tikslai ir objektas.....	5
4.1	Pirkimo tikslas.....	5
4.2	Pirkimo objektas.....	5
4.3	Pirkimo uždaviniai ir apribojimai	Error! Bookmark not defined.
4.4	Tikslinės naudotojų grupės ir planuojamos rolės.....	5
5.	Reikalavimai SDMA IS	6
5.1	Bendrieji reikalavimai ir Sistemos architektūra.....	6
5.2	Nefunkciniai reikalavimai	8
5.3	Privalomų duomenų rinkinių aprašas.....	11
5.4	Funkciniai reikalavimai	14
6.	Reikalavimai paslaugų teikimui	22
6.1	Bendrieji reikalavimai SDMA IS sukūrimo ir įdiegimo paslaugoms	22
6.2	1 etapas: Analizė ir architektūrinis projektavimas	22
6.3	2 etapas: Sistemos instaliavimas ir konfigūravimas	23
6.4	3 etapas: Testavimas, mokymai ir perdavimas naudojimui	23
6.5	Informacijos saugumo ir konfidencialumo reikalavimai Tiekėjui paslaugų teikimo metu.....	25

1. Santrumpos ir sąvokos

lentelė 1

Sąvoka	Reikšmė
API	Programų integracijų sąsaja / taikomųjų programų sąsaja (angl. <i>Application Programming Interface</i>)
ACID	Reliacinių duomenų bazių transakcijų patikimumo savybės: atomiškumas, nuoseklumas, izoliuotumas, ilgaamžiškumas (angl. <i>Atomicity, Consistency, Isolation, Durability</i>)
BDAR	Bendrasis duomenų apsaugos reglamentas (2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679)

DAC	Lietuvos sveikatos mokslų universiteto duomenų mokslinės analitikos centras
DAP	Duomenų apsaugos pareigūnas
DI	Dirbtinis intelektas
DICOM	Skaitmeninis vaizdinimo ir komunikacijos medicinoje standartas (angl. Digital Imaging and Communications in Medicine)
ETL	Duomenų išgavimo, transformavimo ir įkėlimo procesas (angl. <i>Extract, Transform, Load</i>)
GUI / UI	Grafinė naudotojo sąsaja (angl. <i>Graphical User Interface / User Interface</i>)
HL7 FHIR	Tarptautinis sveikatos priežiūros duomenų mainų standartas (angl. <i>Fast Healthcare Interoperability Resources</i>)
IAM	Tapatybės ir prieigos valdymo komponentas (angl. <i>Identity and Access Management</i>)
KPI	Pagrindinis veiklos rodiklis (angl. <i>Key Performance Indicator</i>)
LDAP / AD	Naudotojų autentifikavimo infrastruktūra. Katalogų prieigos protokolas / Pirkėjo naudojama „Active Directory“ sistema
LSMU	Lietuvos sveikatos mokslų universitetas
MFA / 2FA	Kelių veiksmų (arba dviejų veiksmų) autentifikacija (angl. <i>Multi-Factor / Two-Factor Authentication</i>)
MVP	Bazinė, minimalaus gyvybingumo produkto versija (angl. <i>Minimum Viable Product</i>), apimanti esminius funkcionalumus
OAuth 2.0	Atviras autorizacijos standartas, skirtas saugiam prieigos delegavimui
OIDC	Atviro tapatybės patvirtinimo standartas (angl. <i>OpenID Connect</i>)
OMOP CDM	Bendras sveikatos stebėsenos duomenų modelis (angl. <i>Observational Medical Outcomes Partnership Common Data Model</i>)
PACS	Medicininis vaizdų archyvavimo ir perdavimo sistema (angl. <i>Picture Archiving and Communication System</i>)
Projektas	Projektas „Centralizuotos sveikatos duomenų valdymo ir analitikos infrastruktūros plėtra LSMU“. Projekto kodas 10-093-K-0072
PO, Pirkėjas	Perkančioji organizacija - Lietuvos sveikatos mokslų universitetas
RBAC	Vaidmenimis grįstas prieigos valdymas (angl. <i>Role-Based Access Control</i>)
SDMA IS	Sveikatos duomenų mokslinės analitikos informacinė sistema
SNOMED CT	Sistematizuota medicinos terminija (angl. <i>Systematized Nomenclature of Medicine – Clinical Terms</i>)
SSO	Vienkartinio prisijungimo mechanizmas (angl. <i>Single Sign-On</i>)
TBG	Turi būti galimybė Svarbu! Visur, kur naudojama formulė „turi būti galimybė“, turima galvoje, kad „siūlomame sprendime tokia funkcija turi būti realizuota ir įtraukta į siūlomo sprendimo apimtį bei sąmatą“, o ne „turi būti galimybė realizuoti Sistemoje tokią funkciją, užsakant papildomą, į sąmatą neįtrauktą darbą“
TLK-10	Tarptautinė ligų klasifikacija, 10-oji redakcija
TVS	Turinio valdymo sistema
UX	Naudotojo patirtis (angl. <i>User Experience</i>) – bendra naudotojo patirtis, pojūčiai ir patogumas, kylantys naršant bei atliekant veiksmus informacinėje sistemoje

URI / URL	Vieningas resurso identifikatorius / adresas (angl. <i>Uniform Resource Identifier / Locator</i>)
VPN	Virtualusis privatus tinklas (angl. <i>Virtual Private Network</i>)
WORM	Vienkartinio įrašymo ir daugkartinio skaitymo duomenų saugojimo technologija, užtikrinanti įrašų nekintamumą (angl. <i>Write Once Read Many</i>)

2. Dokumento paskirtis

Šiame dokumente apibrėžiami reikalavimai Lietuvos sveikatos mokslų universiteto (toliau LSMU) Sveikatos duomenų mokslinės analitikos informacinei sistemai (toliau – SDMA IS) įdiegimui.

3. Pirkimo kontekstas

3.1 Pirkimu įgyvendinamas projektas

Lietuvos sveikatos mokslų universitetas (toliau – LSMU), įgyvendina projektą pagal Sutartyje, 2022–2030 metų plėtros programos valdytojos Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos mokslo plėtros programos pažangos priemonės Nr. 12-001-01-02-01 „Stiprinti inovacijų ekosistemas mokslo centruose“ aprašo, patvirtinto Lietuvos Respublikos švietimo, mokslo ir sporto ministro 2025 m. spalio 2 d. įsakymu Nr. V-1020 „Dėl švietimo, mokslo ir sporto ministro 2022 m. rugpjūčio 17 d. įsakymo Nr. V-1250 „Dėl 2022-2030 metų plėtros programos valdytojos Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos mokslo plėtros programos pažangos priemonės Nr. 12-001-01-02-01 „Stiprinti inovacijų ekosistemas mokslo centruose“ aprašo patvirtinimo“ pakeitimo“, 17 priede „2022-2030 m. plėtros programos valdytojos Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos plėtros programos pažangos priemonės Nr. 12-001-01-02-01 „Stiprinti inovacijų ekosistemas mokslo centruose“ projektų finansavimo sąlygų aprašas Nr. 16“, Projektų administravimo ir finansavimo taisyklėse (toliau – Taisyklės) ir (arba) Finansinių priemonių įgyvendinimo taisyklėse, patvirtintose Lietuvos Respublikos finansų ministro 2022 m. birželio 22 d. įsakymu Nr. 1K-237 „Dėl 2021–2027 metų Europos Sąjungos fondų investicijų programos ir Ekonomikos gaivinimo ir atsparumo didinimo plano „Naujos kartos Lietuva“ įgyvendinimo“, ir juose nurodytuose ES ir Lietuvos Respublikos teisės aktuose nustatytas sąlygas ir tvarką. Taisyklės ir vėlesni jų pakeitimai laikomi Sutarties sąlygomis, Toliau - Projektas

Projekto pareiškėjas – Lietuvos sveikatos mokslų universitetas (kodas 302536989, A. Mickevičiaus g. 9, LT-44307, Kaunas)

Projekto veiklų vykdymo pabaiga – 2026-12-31.

3.2 Projekto tikslas, sprendžiamos problemos

Pagrindinis projekto tikslas yra įdiegti Sveikatos duomenų mokslinės analitikos informacinę sistemą (IS), siekiant sustiprinti LSMU mokslinės analitikos bazę, įteisinti patikimą duomenų valdyseną ir užtikrinti aukščiausią kibernetinio saugumo lygį, kas leis LSMU tapti pilnaverčiu ir patikimu tarptautinių mokslinės analitikos projektų partneriu, bei paspartins mokslo žiniomis grįstos sveikatos sistemos kūrimą. Numatoma ne vėliau kaip per 3 metus po projekto įgyvendinimo pabaigos panaudojant įsigytą įrangą pateikti bent vieną paraišką pagal Europos Sąjungos bendrosios mokslinių tyrimų ir inovacijų, įskaitant Europos partnerysčių ir Europos bendradarbiavimo mokslo ir technologijų srityje, programų kvietimus.

Projekto tikslinė grupė - MSI, mokslininkai ir kiti tyrėjai

Projektas skirtas spręsti LSMU infrastruktūros trūkumus, kurie riboja Universiteto galimybes užtikrinti aukšto lygio sveikatos duomenų valdyseną ir mažina pasirengimą aktyviai dalyvauti tarptautiniuose projektuose kaip patikimam mokslinės analitikos partneriui.

4. Pirkimo tikslai ir objektas

4.1 Pirkimo tikslas

Viešojo pirkimo tikslas – įgyvendinant projektą „Centralizuotos sveikatos duomenų valdysenos ir analitikos infrastruktūros plėtra LSMU“ Nr. 10-093-K-0072, finansuojamą Europos Sąjungos ir valstybės biudžeto lėšomis įdiegti centralizuotą, saugią ir pažangią Sveikatos duomenų mokslinės analitikos informacinę sistemą (SDMA IS), kuri pakeistų fragmentuotus ir rankinius duomenų valdymo procesus bei užtikrintų efektyvų, automatizuotą skirtingų šaltinių duomenų tvarkymą laikantis BDAR reikalavimų.

Tiekėjas, įgyvendindamas Sutartį turės užtikrinti, kad Sistema sudarys galimybes centralizuotai valdyti mokslinių tyrimų projektus ir su jais susijusius duomenis viso jų gyvavimo ciklo metu, įskaitant projektų registravimą, vykdymo stebėseną ir rezultatų atsekamumą. Sistema turi sudaryti sąlygas efektyviai valdyti dokumentus, informuotų asmenų sutikimus ir kitus susijusius patvirtinimus, užtikrinant jų saugumą, vientisumą ir prieinamumą. Taip pat sistema turi sudaryti galimybes vykdyti standartizuotą ir struktūrizuotą duomenų rinkimą, metaduomenų katalogavimą bei užtikrinti duomenų kokybę ir nuoseklumą. Sistema turi įgalinti saugų ir kontroliuojamą duomenų prieinamumą bei efektyvų bendradarbiavimą tarp skirtingų institucijų ir tyrėjų grupių.

Be to, sistema turi sudaryti technologinį pagrindą kaupti duomenis pažangiai duomenų analitikai, taip pat būti suprojektuota kaip plečiama ir modulinė, sudaranti sąlygas ateityje integruoti papildomus funkcionalumus, naujus duomenų šaltinius bei mašininio mokymosi ir dirbtinio intelekto sprendimus be esminių sistemos architektūros pakeitimų.

4.2 Pirkimo objektas

lentelė 2

Eil. Nr.	Pirkimo objektas	Mato vienetas	Kiekis
1.	Sveikatos duomenų mokslinės analitikos informacinės sistemos sukūrimas ir įdiegimas	Vnt.	1

4.3 Tikslinės naudotojų grupės ir planuojamos rolės

- 4.3.1.1 **Svečias:** Naudotojas, turintis prieigą tik prie viešosios informacijos portalo dalies (naujienu, atviros ir nuasmenintos statistikos).
- 4.3.1.2 **Naudotojas užsakovas (Tyrėjas):** Pagrindinė platformos naudotojo rolė, apjungianti duomenų teikėjo ir vartotojo funkcijas. Šis naudotojas savitarnos portale registruoja tyrimų projektus, teikia (įkelia) tyrimų duomenis bei bioetikos sutikimus, naudojami metaduomenų katalogu, formuoja duomenų apdorojimo užsakymus ir gauna rezultatus. Priklausomai nuo tyrimo protokolo, jis dirba su pseudonimizuotais arba (įkėlimo etape) identifikuojamais duomenimis.
- 4.3.1.3 **Analitikas / Duomenų mokslininkas:** Specialistas, vykdamas tyrėjų užsakymus. Jis apdoroja duomenis, validuoja modelius, atlieka skaičiavimus ir parengia reikiamus standartizuotus duomenų paketus saugiam atidavimui.
- 4.3.1.4 **Duomenų architektas:** Techninis darbuotojas, kuris tvarko ir prižiūri platformos duomenis, jų bazių struktūras, standartizavimą (pvz., į OMOP ar FHIR formatus) bei prižiūri automatizuotus duomenų srautus tarp modulių.
- 4.3.1.5 **Duomenų valdytojas (angl. Data Steward):** Asmuo, turintis plačias duomenų valdysenos teises. Jis peržiūri ir tvirtina tyrėjų prašymus gauti prieigą prie duomenų, prižiūri duomenų kokybę ir nustato prieigos taisykles bei terminus. Taip pat ši rolė turi išskirtinę teisę ir įrankius atlikti de-pseudonimizaciją (atkurti ryšį su asmens tapatybe), kai tam yra teisėtas pagrindas.

- 4.3.1.6 **Administratorius (IT administratorius):** Aukščiausio lygio techninės prieigos naudotojas, atsakingas už platformos parametrų konfigūravimą bei naudotojų paskyrų ir teisių (RBAC) valdymą. Administratorius užtikrina sklandų sistemos veikimą, tačiau jis neturi prieigos teisių peržiūrėti pirminių, jautrių sveikatos duomenų.
- 4.3.1.7 **Auditorius / Duomenų apsaugos pareigūnas (DAP):** Naudotojas, atsakingas už saugumo, atskaitomybės ir BDAR atitikties priežiūrą. Jis turi išskirtinę prieigą prie sistemos audito žurnalų ir stebi, kas, kada ir koku tikslu jungėsi prie jautrių duomenų.
- 4.3.1.8 **Padalinio (Centro) vadovas:** Rolė, skirta vadovams, kuriems nereikalinga tiesioginė prieiga prie jautrių pacientų duomenų. Jie platformos valdymo skydeliuose mato agreguotą statistiką, projektų apimtis, analitikų apkrovas ir priima duomenų analitikos centro išteklių valdymo sprendimus.

5. Reikalavimai SDMA IS

5.1 Bendrieji reikalavimai ir Sistemos architektūra

5.1.1 Reikalavimai licencijavimui

- 5.1.1.1 Tiekėjas, įdiegęs SDMA IS, privalo perduoti Pirkėjui visas išimtines turtines autorių teises į specialiai šiam projektui sukurtą unikalų programinį kodą (įskaitant, bet neapsiribojant, vartotojo sąsają, integracinius mikroservisus, duomenų srautų algoritmus), neribotam laikui ir neribotoje teritorijoje, suteikiant Pirkėjui teisę šį kodą naudoti, kopijuoti, keisti, adaptuoti, platinti, integruoti, perduoti tretiesiems asmenims ir kitaip juo disponuoti be atskirų Tiekėjo sutikimų ar papildomų mokesčių
- 5.1.1.2 Siekiant išvengti technologinės priklausomybės nuo vieno tiekėjo (angl. vendor lock-in) ir užtikrinti Sistemos perkeliamumą bei savarankišką naudojimą, Sistemos baziniams komponentams gali būti naudojami tiek atvirojo kodo, tiek komerciniai sprendimai. Tiekėjas privalo užtikrinti, kad visi parinkti komponentai atitiktų šioje specifikacijoje nustatytus funkcinius, techninius, saugumo, licencijavimo ir nuosavybės teisių reikalavimus bei būtų tinkami neterminuotam naudojimui, modifikavimui, plėtrai ir integracijai. Atvirojo kodo sprendimai laikomi tinkamais, jei jie platinami pagal standartines atvirąsias licencijas ir atitinka nustatytus reikalavimus. Komerciniai ir Tiekėjo sukurti sprendimai laikomi tinkamais tik tuo atveju, jei jie suteikiami Pirkėjui neterminuotai, suteikia teisę naudoti, modifikuoti ir adaptuoti programinę įrangą be papildomų apribojimų, neapriboja Sistemos perkeliamumo ir tolesnės plėtros bei nesukuria techninės ar teisinės priklausomybės nuo tiekėjo; sprendimai, kurių licencinės ar techninės sąlygos riboja šias teises, laikomi netinkamais
- 5.1.1.3 Tiekėjas privalo perduoti Pirkėjui visus SDMA IS diegimo, konfigūravimo, pritaikymo ar integravimo metu naudotus ar parengtus išeities tekstus (angl. source code), diegimo ir konfigūracijų parametrus, konteinerizacijos skriptus (pvz., Dockerfiles, Kubernetes manifestus), duomenų inžinerijos logiką (pvz., Apache Airflow DAGs) ir kitą dokumentaciją, reikalingą tam, kad Pirkėjas galėtų savarankiškai (arba su trečiųjų šalių pagalba) SDMA IS toliau palaikyti ir vystyti.
- 5.1.1.4 Nei SDMA IS licencijos, perduodamos teisės ar architektūrinis sprendimas turi neriboti vienu metu dirbančių naudotojų skaičiaus, apdorojamų duomenų apimtį, sukurtų projektų skaičiaus ar atliekamų transakcijų (skaičiavimų) kiekio.
- 5.1.1.5 Visos Sistemai naudoti būtinos licencijos (tiek specialiai sukurtos kodo, tiek atviro kodo komponentų) privalo būti suteikiamos (perduodamos) neterminuotam laikui, užtikrinant, kad Sistema visa jos apimtimi ir funkcionalumais Pirkėjas galės naudotis neribotą laiką be jokių papildomų licencijų pratęsimo mokesčių, nepriklausomai nuo to, ar yra sudaryta Sistemos priežiūros ar palaikymo sutartis su Tiekėju.

5.1.2 Architektūrinė koncepcija

- 5.1.2.1 Architektūrinė vizija ir modulinio projektavimo principas: Siekiant užtikrinti sprendimo lankstumą, tvarumą ir išvengti priklausomybės nuo vieno tiekėjo (angl. vendor lock-in), SDMA IS turi būti kuriama ne kaip monolitinė, o kaip modulinė sistema. Ji turi būti sudaryta iš tarpusavyje integruotų, nepriklausomai veikiančių komponentų, paremtų mikroservisų architektūra ir konteinerizavimu. Tiekėjas turi užtikrinti, kad sprendimas būtų pernešamas tarp skirtingų infrastruktūrų, sudarytų galimybes atnaujinti ar keisti atskirus komponentus nekeičiant visos sistemos bei leistų taikyti atvirus sveikatos duomenų standartus
- 5.1.2.2 „Sistemos“ sąvokos taikymas modulinės architektūros kontekste: Visur, kur šioje techninėje specifikacijoje nurodoma, jog funkcija ar savybė turi būti realizuota „Sistemoje“, tai apibrėžia bendrą galutinį SDMA IS sprendimą. Kadangi SDMA IS kuriama kaip atskirų komponentų visuma (angl. *composable architecture*), Tiekėjas turi teisę pats parinkti, kuris konkretus siūlomas komponentas ar jų kombinacija atliks reikalaujamą funkciją. Tiekėjas gali siūlyti tiek siauros paskirties (dedikuotus), tiek kelias funkcijas apimančius komponentus, tačiau diegimo metu visi jie privalo būti tarpusavyje integruoti ir sukonfigūruoti bendram darbui taip, kad naudotojui veiktų kaip viena vieninga sistema.
- 5.1.2.3 SDMA IS architektūra, nepriklausomai nuo Tiekėjo pasirinkto konkrečių techninių komponentų išskaidymo ar apjungimo, funkcinė ir logine prasme privalo apimti (realizuoti) ne mažiau kaip šiuos bazinius modulius (arba lygiaverčius jų funkcinius atitikmenis):
- Pagrindinį portalą;
 - Vartotojų valdymo posistemį;
 - Projekto gyvavimo ciklo valdymo funkcionalumą;
 - Metaduomenų katalogą;
 - Dokumentų tvarkymo aplinką;
 - Patvirtinimų ir aprobavimo mechanizmus;
 - Audito ir saugumo modulį;
 - Duomenų mainų ir API funkcijas;
 - Ataskaitų ir statistikos (analitikos) aplinką (Reporting);
- Pastaba:* Šis skaidymas atspindi loginę SDMA IS architektūros aprėptį. Tiekėjas turi teisę šiuos loginius modulius realizuoti naudodamas apjungtus atviro kodo ar komercinius įrankius, specializuotus mikroservisus ar kitus technologinius sprendimus, užtikrinant, kad galutinėje Sistemoje veiks visas šioje specifikacijoje numatytas funkcionalumas.
- 5.1.2.4 Sistemos modulių integracija ir duomenų vienkartinio pildymo principas: SDMA IS moduliai privalo būti glaudžiai tarpusavyje susieti (tiek naudotojų valdymo, tiek automatinio informacijos apskaitimo prasme) ir veikti kaip viena vieninga sistema. Tvarkant (įvedant, redaguojant, šalinant) duomenis bet kuriame modulyje, visoje Sistemoje esanti susijusi informacija privalo būti atnaujinama automatinio būdu. Sistema turi užtikrinti vienkartinį informacijos įvedimą, siekiant visiškai išvengti tų pačių duomenų dubliavimo skirtinguose moduluose.
- 5.1.2.5 Infrastruktūra ir saugus pasiekiamumas: Sistema privalo sklandžiai funkcionuoti virtualaus serverio (arba konteinerizuotoje) aplinkoje. Esant poreikiui, ji turi būti pasiekiamą ne tik vidiniame organizacijos tinkle, bet ir už jo ribų, visais atvejais užtikrinant saugų, šifruotą ryšį (pvz., naudojant VPN ar saugius HTTPS API vartus). 1
- 5.1.2.6 Naudotojo veiksmai, išskyrus sistemos administratoriaus veiksmus arba kai tai būtina vykdomų procesų korektiškumui užtikrinti, turi neblokuoti kito naudotojo veiksmų.
- 5.1.2.7 Suderinamumas su biuro programine įranga: Naudotojo darbo vietoje sistema turi būti suderinta su perkančiosios organizacijos naudojama „Microsoft Office“ programine įranga (pavyzdžiui, sistemos eksportuojamos ataskaitos, sąrašai ar dokumentai privalo būti atidaromi ir korektiškai peržiūrimi standartiniais MS Office įrankiais).
- 5.1.2.8 Turi būti galimybė taikyti/aktyvuoti duomenų saugojimo (retencijos) politikas.

5.2 Nefunkciniai reikalavimai

5.2.1 Reikalavimas tapatybės ir prieigos valdymui:

- 5.2.1.1 Sistema turi turėti centralizuotą tapatybės ir prieigos valdymo komponentą.
- 5.2.1.2 Turi būti realizuotas naudotojų prisijungimas vardu ir slaptažodžiu.
- 5.2.1.3 Turi būti palaikomas vienkartinis prisijungimas (SSO).
- 5.2.1.4 Palaikomi OAuth 2.0 ir OpenID Connect (OIDC) arba lygiaverčiai standartai.
- 5.2.1.5 Turi būti perspektyva integracijai su LDAP / Active Directory (šiuo metu naudojama Pirkėjo).
- 5.2.1.6 Užtikrinamas prieigos žetonų išdavimas, validavimas ir atšaukimas.
- 5.2.1.7 Turi būti vaidmenimis grįstas prieigos valdymas (RBAC): Sistemos autorizavimo mechanizmas turi būti realizuotas remiantis rolių modeliu. Sistemoje turi būti galima apibrėžti naujas roles ir keisti joms priskirtas prieigos teises prie atskirų sistemos objektų (duomenų struktūrų) ir programinių vienetų. Vienam naudotojui turi būti galima priskirti kelias roles – sistema turi nereikalauti papildomų prisijungimų kitu vardu atliekant kitos rolės funkcijas. Naudotojams, neatliekantiems administravimo funkcijų, negali būti suteikiamos administratoriaus teisės.

5.2.2 Reikalavimas reliacinei duomenų bazei:

- 5.2.2.1 Turi būti naudojama reliacinė duomenų bazių valdymo sistema.
- 5.2.2.2 Turi būti užtikrinamos ACID savybės (vientisumas, nuoseklumas, izoliacija, patvarumas).
- 5.2.2.3 Turi būti palaikomas SQL arba lygiavertė užklausų kalba.
- 5.2.2.4 Turi būti palaikomas atsarginių kopijų kūrimas ir duomenų atkūrimas.
- 5.2.2.5 Turi būti palaikoma duomenų replikacija (sinchroninė arba asinchroninė).
- 5.2.2.6 Sistema turi būti tinkama analitinėms užklausoms ir struktūrizuotų duomenų saugojimui pagal tarptautinius modelius (pvz., OMOP CDM, openEHR arba lygiaverčius).

5.2.3 Reikalavimas objektinei duomenų saugyklai:

- 5.2.3.1 Sistema turi turėti paskirstytą objektinę duomenų saugyklą didelės apimties nestructūrizuotiems duomenims saugoti.
- 5.2.3.2 Palaikoma REST tipo objektų saugojimo sąsaja (pvz., S3-compatible API arba lygiavertė).
- 5.2.3.3 Palaikomos bazinės operacijos: įkėlimas, atsiuntimas, sąrašų gavimas, trynimas.
- 5.2.3.4 Palaikomas prieigos valdymas per IAM arba lygiavertį mechanizmą.

5.2.4 Reikalavimas pseudonimizavimo paslaugai:

- 5.2.4.1 Sistema turi turėti per API pasiekiamą pseudonimizavimo komponentą.
- 5.2.4.2 Turi būti užtikrinamas tiesioginių identifikatorių pašalinimas.
- 5.2.4.3 Turi būti palaikomas bent vienas moksliniais principais grįstas privatumo modelis (pvz., k-anonimiškumas, angl *k-anonymity* arba lygiavertis).

5.2.5 Reikalavimas sveikatos duomenų mainams:

- 5.2.5.1 Turi būti įdiegtas sveikatos duomenų mainų komponentas.
- 5.2.5.2 Palaikomas HL7 FHIR standartas arba lygiavertis.
- 5.2.5.3 Palaikoma REST tipo sąsaja.
- 5.2.5.4 Turi būti galimybė priimti didelės apimties duomenų paketus (batch / transaction).
- 5.2.5.5 Turi būti galima atlikti duomenų validavimą prieš tolimesnį apdorojimą.

5.2.6 Reikalavimas metaduomenų katalogui:

- 5.2.6.1 Turi būti naudojamas metaduomenų valdymo komponentas.
- 5.2.6.2 Turi būti galimybė automatiškai indeksuoti duomenų šaltinius (DB, objektinė saugykla, API).
- 5.2.6.3 Turi būti galimybė vykdyti duomenų paiešką.

5.2.7 Reikalavimas stebėsenos platformai:

- 5.2.7.1 Turi būti naudojama Sistemos parametrų ir duomenų stebėsenos ir metrikų rinkimo platforma.
- 5.2.7.2 Turi būti palaikomas laiko eilučių metrikų kaupimas.
- 5.2.7.3 Turi būti galimybė vizualizuoti duomenis (dashboard).
- 5.2.7.4 Turi būti generuojami įspėjimai apie sutrikimus ar anomalijas.

5.2.8 Reikalavimas užduočių valdymui:

- 5.2.8.1 Turi būti realizuota užduočių valdymo funkcija arba integracija su tokio tipo sistema.
- 5.2.8.2 Turi būti palaikomas užduočių būsenų valdymas.
- 5.2.8.3 Turi būti galimybė priskirti terminus.
- 5.2.8.4 Turi būti galimybė fiksuoti komentarus ir komunikaciją tarp naudotojų.
- 5.2.8.5 Turi būti palaikomas užduočių planavimas pagal laiką arba įvykius.
- 5.2.8.6 Turi būti galimybė stebėti darbo seką vykdymą, būsenas ir žurnalus.

5.2.9 Reikalavimai naudotojo sąsajai:

- 5.2.9.1 Naudotojo sąsajos (GUI/UI/UX) sprendimai: Naudotojo sąsajos sprendimai turi būti patogūs ir intuityvūs, atitikti WCAG 2.1 AA prieinamumo reikalavimus bei būti pagrįsti pripažintomis naudotojo patogumo gairėmis (pvz., Nielsen Norman Group heuristikomis arba lygiavertėmis). Sąsaja turi atitikti šiuolaikinius web taikomųjų sistemų projektavimo principus, užtikrinant aiškią navigaciją, nuoseklų išdėstymą, vizualinį vientisumą ir minimalią naudotojo veiksmų sąnaudą atliekant tipines operacijas.
- 5.2.9.2 Sąveikos modelis: Naudotojo ir sistemos sąveika turi būti realizuota per interaktyvią grafinę naudotojo sąsają (web GUI). Sistemoje duomenų įvedimas, išvedimas, valdymo komandų inicijavimas ir rezultatų atvaizdavimas turi būti atliekamas realiuoju arba artimu realiajam laikui režimu, užtikrinant aiškų sistemos atsaką į naudotojo veiksmus (grįžtamąjį ryšį).
- 5.2.9.3 Nuoseklumas ir standartizacija – Naudotojo portalo sąsaja turi būti nuosekli, naudojant vienodus dizaino elementus, terminiją ir veiksmų logiką, atitinkančią įprastus šiuolaikinių web sistemų standartus (netaikoma specializuotiems, integruotiems atviro kodo Sistemos komponentams ir/ar posistemėms).
- 5.2.9.4 Struktūrizuotas duomenų įvedimas: Naudotojas turi turėti galimybę pildyti įvedimo laukus pasirinkdamas reikšmes iš anksto apibrėžtų sąrašų ir klasifikatorių (pvz., išskleidžiamų sąrašų).
- 5.2.9.5 Automatinis duomenų užpildymas: Sistema turi užtikrinti, kad dalis duomenų būtų užpildoma automatiškai pagal kontekstą (pvz., įrašo sukūrimo ar pateikimo data), siekiant sumažinti naudotojo veiksmų kiekį ir klaidų tikimybę.
- 5.2.9.6 Išplėstinė paieška: Sistema turi suteikti galimybę atlikti išplėstinę metaduomenų paiešką ekraninėse formose, naudojant vieną ar kelis kriterijus, įskaitant paiešką pagal dalinę reikšmę (fragmentą) ir kitus filtravimo parametrus.
- 5.2.9.7 Duomenų rikiavimas: Atvaizduojamuose sąrašuose ir lentelėse naudotojas turi turėti galimybę rikiuoti duomenis pagal pasirinktus atributus ar laukus.
- 5.2.9.8 Klaidingų veiksmų valdymas: Sistema turi užtikrinti korektišką naudotojo klaidų ir neleistinų veiksmų valdymą: įvykus klaidai, naudotojui turi būti pateikiamas aiškus pranešimas, o sistema turi išlikti stabilioje darbo būsenoje be duomenų praradimo.
- 5.2.9.9 Pranešimų adresavimas: Sistemos pranešimai apie klaidas ar neteisingus veiksmus turi būti pateikiami tik tam naudotojui, kuris inicijavo atitinkamą veiksmą.

5.2.10 Reikalavimai naudotojų paskyrų valdymui ir saugai

- 5.2.10.1 Tiesioginės prieigos prie duomenų bazės apribojimas: Sistemos naudotojai neturi turėti galimybės keisti duomenų tiesiogiai duomenų bazėje. Visi pakeitimai privalo būti atliekami tik per naudotojo sąsają ar integracines sąsajas.
- 5.2.10.2 Individualus duomenų rinkinių valdymas: Nepaisant naudotojui priskirtos bendros rolės (pvz., „Tyrėjas“), prieiga prie konkrečių iš duomenų suformuotų duomenų rinkinių privalo būti valdoma ir suteikiama griežtai individualaus naudotojo lygmeniu. Sistema turi užtikrinti, kad konkretus naudotojas turėtų prieigą tik prie tų duomenų rinkinių, kurie jam buvo individualiai priskirti arba kuriems buvo patvirtinta jo individuali prieigos užklausa.
- 5.2.10.3 Funkcijų ir matomumo ribojimas pagal teises: Sistemos naudotojas turi matyti tik tiek meniu punkty, peržiūrėti, pildyti bei koreguoti tik tokią informaciją ir naudotis tik tokiu funkcionalumu, kuris numatytas jam priskirtos rolės ar organizacinės struktūros teisėmis. Visa kita informacija jam turi būti neprieinama ir nematoma, užtikrinant skirtingo lygio prieigą prie duomenų bei modulių.
- 5.2.10.4 Naudotojų administravimas ir aktyvių sesijų stebėseną: Sistemos administratorius turi turėti įrankius peržiūrėti naudotojų bei jiems priskirtų teisių sąrašus. Sistemoje taip pat turi būti realizuotos specializuotos stebėsenos priemonės, leidžiančios administratoriui matyti aktyvius, tuo metu prie sistemos prisijungusius ir su ja dirbančius naudotojus.
- 5.2.10.5 Slaptažodžių sudėtingumo politika: Sistema privalo užtikrinti griežtą slaptažodžių sudėtingumo kontrolę. Slaptažodis turi būti ne trumpesnis nei 12 simbolių, jame privalo būti didžiųjų ir mažųjų raidžių, skaičių bei specialiųjų simbolių.
- 5.2.10.6 Apsauga nuo slaptažodžių spėliojimo (Brute-force apsauga): Sistemoje turi būti realizuota paskyrų blokavimo funkcija. Po administratoriaus nustatyto nesėkmingų bandymų prisijungti skaičiaus (pvz., 5 kartų), naudotojo paskyra turi būti laikinai blokuojama arba reikalaujama papildomo patvirtinimo, o šie incidentai privalo būti fiksuojami audito žurnaluose.
- 5.2.10.7 Slaptažodžių galiojimas ir istorija: Sistemoje turi būti galimybė priverstinai reikalauti naudotojo pakeisti slaptažodį pirmojo prisijungimo metu bei praėjus administratorių nustatytam terminui (pvz., 90 dienų). Sistema turi neleisti naudoti nustatyto skaičiaus paskutinių naudotų slaptažodžių.
- 5.2.10.8 Kriptografinis slaptažodžių saugojimas: Naudotojų slaptažodžiai duomenų bazėje jokia būdu neturi būti saugomi atviru tekstu. Jie privalo būti saugomi tik kriptografiškai apdoroti, naudojant stiprias, tarptautinius standartus atitinkančias vienakryptes maišos funkcijas.
- 5.2.10.9 Saugus prisijungimo duomenų perdavimas: Visi autentifikacijos duomenys (naudotojų vardai, slaptažodžiai, sesijų žetonai ir kt.) privalo būti perduodami tik šifruotais ryšio kanalais (HTTPS/TLS protokolu), atitinkančiais tarptautinius saugos standartus.

5.2.11 Reikalavimai saugos užtikrinimui ir auditavimui

- 5.2.11.1 Viešaisiais ryšių tinklais perduodamos sistemos elektroninės informacijos konfidencialumas turi būti užtikrintas, naudojant šifravimą.
- 5.2.11.2 Sistemoje turi būti įgyvendintos kontrolės priemonės, užtikrinančios perduodamų ar gaunamų duomenų vientisumą ir konfidencialumą, kad duomenys nebuvo iškraipyti ar neleistinais atskleisti jų perdavimo metu.
- 5.2.11.3 Turi būti naudojama centralizuota žurnalų kaupimo ir analizės platforma.
- 5.2.11.4 Visi sistemos įvykiai turi būti registruojami ir saugomi centralizuotai.
- 5.2.11.5 Turi būti užtikrintinas Sistemos naudotojų auditavimas, fiksuojant: a) sėkmingus ir nesėkmingus bandymus prisijungti ir atsijungti; b) veiksmą atlikusio naudotojo vardą (prisijungimo identifikatorių); c) naudotojo atliktą veiksmą (turi būti fiksuojamas naudotojo sąsajoje atliktas veiksmas); d) su kokiais duomenimis atliktas veiksmas; e) veiksmo arba įvykio datą ir tikslų laiką, įvykio rezultatą ir kitą informacijos saugai svarbią informaciją (veiksnius su duomenimis, naudotojų ar jų grupių bei administratorių teisių naudotis sistemos ištekliais pakeitimus, sistemos parametrų, laiko ir / ar datos pakeitimus).
- 5.2.11.6 Naudotojų veiksmų auditavimo įrašai privalo būti saugomi ne trumpiau kaip 12 mėnesių bei turi būti galimybė Pirkėjui (atsakingiems jo darbuotojams) auditavimo įrašus peržiūrėti (pagal konkretų naudotoją) ir konvertuoti patogiu formatu.

- 5.2.11.7 Turi būti galimybė vykdyti paiešką ir analizę žurnaluose.
- 5.2.11.8 Turi būti užtikrintas žurnalinių įrašų nekintamumas (append-only, WORM arba lygiavertis sprendimas).

5.3 Privalomų duomenų rinkinių aprašas

5.3.1 Bendrieji reikalavimai duomenų rinkiniams:

- 5.3.1.1 Duomenų saugojimo architektūra: Tiekėjas privalo parinkti ir įdiegti tinkamas duomenų saugojimo technologijas bei struktūras, atsižvelgiant į skirtingų duomenų tipų (pvz., struktūrizuotų, pusiau struktūrizuotų, nestruktūrizuotų, didelės apimties failų) pobūdį, apimtį ir naudojimo scenarijus. Turi būti taikomas optimalus duomenų saugojimo modelis (pvz., reliacinės duomenų bazės, objektinės saugyklos, failų saugyklos ar lygiaverčiai sprendimai), užtikrinant duomenų vientisumą, saugumą ir efektyvų pasiekiamumą.
- 5.3.1.2 Duomenų rinkinių apimties lankstumas: Pradinis pateikiamas duomenų rinkinių sąrašas laikomas minimaliu ir privalomu sistemos diegimo metu. Šalims sutarus, duomenų rinkinių apimtis gali būti plečiama ar modifikuojama, nepažeidžiant bendros sistemos architektūros ir užtikrinant kitų techninės specifikacijos reikalavimų įgyvendinimą.
- 5.3.1.3 Privalomi metaduomenys duomenų rinkiniams: Visiems duomenų rinkiniams turi būti saugomi baziniai metaduomenys, leidžiantys identifikuoti ir valdyti duomenis, įskaitant: už duomenų rinkinį atsakingą instituciją ar valdytoją, duomenų rinkinio sukūrimo ar įkėlimo Sistemoje datą, taip pat duomenų rinkinio naudojimo rodiklius (pvz., eksporto ar atsisiuntimų skaičių). Sistema turi užtikrinti, kad būtų kaupiami pakankami ir struktūrizuoti metaduomenys, reikalingi vėliau techninėje specifikacijoje aprašytų ataskaitų formavimui ir statistinei analizei.

5.3.2 SDMA IS naudotojų duomenys

- 5.3.2.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos duomenis apie kiekvieną registruotą SDMA IS naudotoją:
- Asmens tapatybės ir kontaktiniai duomenys: asmens vardas (-ai), pavardė (-ės), telefono ryšio numeris bei elektroninio pašto adresas;
 - Instituciniai duomenys: darbovietė ar mokslo institucija, kuriai asmuo atstovauja, institucijos struktūrinis vienetas bei užimamos pareigos;
 - Naudotojo rolės ir teisės: naudotojui suteiktos rolės, naudotojui suteiktos prieigos prie konkrečių duomenų rinkinių teisės, teisių galiojimo terminas;
 - Audito duomenys: paskyros sukūrimo data, paskyros būseną (pvz.: aktyvi, blokuota, deaktyvuota), su naudotoju susieti prisijungimo audito duomenys, apimantys prisijungimų datą ir laiką bei atliktus veiksmus.

5.3.3 Mokslo tiriamosios veikos užsakymų duomenys

- 5.3.3.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos duomenis apie kiekvieną registruotą mokslo tiriamosios veikos užsakymą:
- Identifikaciniai duomenys: registruoto SDMA IS naudotojo (užsakovo) identifikatorius ir sisteminis užsakymo identifikatorius;
 - Projekto aprašomieji ir teisiniai duomenys: projekto aprašymas bei Bioetikos komisijos leidimo informacija;
 - Duomenų rinkinio informacija: užsakomų duomenų rinkinio aprašas;
 - Užsakymo administravimo duomenys: užsakymo pateikimo data ir laikas, užsakymo statuso pasikeitimo (patvirtinimo/atmetimo/pabaigos ir pan.) data ir laikas, prieigos prie duomenų terminas (nurodant datą „nuo“ ir datą „iki“);
 - Ryšiai: nuoroda į užsakymą vykdantį (priskirtą) naudotoją, sąsajos su vidiniais duomenų rinkiniais;

- Esamas užsakymo statusas.

5.3.4 Sveikatos duomenų registrai

5.3.4.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos pseudoniminių sveikatos duomenų rinkinių archyvo duomenis:

- **Kardiologijos duomenys:** nuoroda į duomenų tiekėją, įrašo sukūrimo data, pseudonimo identifikatorius, asmens lytis, asmens gyvenamoji vieta rajono tikslumu, ligos anamnezės duomenys, gyvenimo anamnezės duomenys, ūgis, svoris, laboratorinių tyrimų rezultatų santraukos, elektrokardiografinių tyrimų metaduomenys (pvz., tyrimo atlikimo data, tyrimo tipas, nuoroda į išorinę sistemą ar failą), širdies kompiuterinės tomografijos tyrimų metaduomenys, širdies echoskopijos tyrimų metaduomenys, galvos smegenų kompiuterinės tomografijos tyrimų metaduomenys ir jų atlikimo data, indeksai, vertinantys fizinę ir psichoemocinę būklę, indeksai, vertinantys organizmo funkcinę būklę, kognityviniai indeksai bei galutinė klinikinė diagnozė.
- **Slaugos fakulteto padalinių duomenys:** nuoroda į duomenų tiekėją, įrašo sukūrimo data, pseudonimo identifikatorius, sociodemografiniai duomenys (amžius, lytis, išsilavinimas, šeiminių padėtis), ūgis, svoris, ligos anamnezės duomenys, gyvenimo anamnezės duomenys, funkcinės būklės duomenys, kiti klinikiniai rodikliai, su sveikata susijusios gyvenimo kokybės klausimyno aprašas ir duomenys, pirmą kartą atvykusio sportininko apklausos anketa ir metaduomenys.
- **Slaugos ir sporto medicinos registro duomenys:** nuoroda į duomenų tiekėją, identifikatoriai (Eil. Nr. metai, Eil. Nr. mėn.), Vardas Pavardė, Gimimo data, Amžius, Lytis, Paciento kodas, Pagrindinė diagnozė, Lydinti liga, konsultacijos identifikatoriai, Nuotolinė konsultacija, Klinikinis tyrimas, Profilaktinis patikrinimas, Paslaugos mokėtojas, Traumos, Ligos, Sporto šaka, Taikytas gydymas, Atsiradimo vieta, Atsiradimo laikas, Traumos mechanizmas, Pažeista kūno sritis, Traumos tipas, Organų sistemos, Etiologija, Pažeista kūno sritis, Instrumentinių tyrimų (Rentgenas, Echoskopija, MRT, GNRB, Biodex, Kraujo tyrimai, EKG, Echokardiografija, VEM, Masės komponentai, Dinamometrija) atlikimo faktas, Gydomoji mankšta, Individuali kineziterapija, Buvęs chirurginis gydymas, Siuntimas kitam gydytojui, Mitybos korekcija/papildai, Fizioterapija, Medikamentinis gydymas.

5.3.5 Medicininių vaizdų archyvo (PACS) metaduomenys.

5.3.5.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos medicininių vaizdų archyvo (PACS) metaduomenis:

- duomenys apie medicininius vaizdus: identifikacinis numeris, nuoroda į vaizdą padariusios laboratorijos duomenis, medicininio vaizdo padarymo data ir laikas, nuoroda į vaizdo saugojimo vietą.

5.3.6 Genetinių tyrimų sekoskaitos duomenų rinkinių archyvo metaduomenys.

5.3.6.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos genetinių tyrimų sekoskaitos duomenų rinkinių archyvo metaduomenis:

- Projekto duomenys: pavadinimas, unikalus projekto kodas, projekto tikslas ir aprašymas;
- Mėginio aprašas: tiriamo organizmo lotyniškas pavadinimas, taksonominis identifikatorius, unikalus mėginio identifikatorius, mėginio pobūdis, mėginio surinkimo metodas, vieta, kurioje buvo surinktas mėginys (šalis, regionas, įstaiga, koordinatės), donorų demografiniai duomenys, mėginio paėmimo data, laikymo sąlygos ir kiti svarbūs parametrai;
- Sekoskaitos eksperimentų aprašymas: tyrimo metodika, atrankos metodika, naudotos technologijos tipas ir prietaiso modelis, techniniai parametrai (vidutinis skaitymo ilgis, duomenų gilumas ir kiti svarbūs kokybės rodikliai, skaitymų išdėstymas);
- Pirminių duomenų rinkmenos, formatai ir kokybės kontrolės rodikliai: duomenų failų formatas, struktūra ir dydis, kokybės kontrolės metrikos, nuoroda į duomenų failą;

- Duomenų apdorojimo ir analizės santrauka: tyrimo apdorojimo etapų aprašymas, naudotų įrankių aprašymas (pagrindinių programinės įrangos įrankių pavadinimai ir jų versijos), duomenų apdorojimo rezultatų aprašas, gautų rezultatų duomenų failai.

5.3.7 Mokslinių tyrimų ir aprašymų dokumentų archyvo duomenys.

- 5.3.7.1 Sistema privalo turėti duomenų bazės struktūras ir kaupti šiuos mokslinių tyrimų ir aprašymų dokumentų archyvo duomenis:
- Mokslinio projekto duomenys: pavadinimas, unikalus projekto kodas, projekto tikslas ir aprašymas, nuoroda (-os) į išorinius straipsnius, tyrimo metodika, atrankos metodika, tyrėjas (-ai), projekto vadovas;
 - Tyrimo aprašymas: duomenų failų formatas, struktūra ir dydis, kokybės kontrolės metrikos, gautų rezultatų duomenų failai.

5.3.8 Klasifikatorių valdymo reikalavimai

- 5.3.8.1 Sistema turi turėti galimybę apibrėžti ir naudoti vidinius klasifikatorius, skirtus struktūrizuotam duomenų įvedimui (pvz., veiklų grupių klasifikatorius, veiklų ir duomenų užsakymo tikslų klasifikatorius, duomenų rinkinių tipų klasifikatorius, tyrimų metodikų klasifikatorius, atstovaujamų institucijų (partnerių) klasifikatorius, mokslo publikacijų šaltinių klasifikatorius).
- 5.3.8.2 Sistema turi turėti sisteminius klasifikatorius, reikalingus sistemos veikimui (pvz., naudotojų rolės, paslaugų tipai, būsenos).
- 5.3.8.3 Sistema turi palaikyti standartizuotų išorinių medicininių klasifikatorių integravimą ir naudojimą (pvz., TLK-10, SNOMED CT ar kt.). Šie klasifikatoriai turi būti importuojami arba įkeliami automatizuotai per integracijas ir naudojami diagnozių, procedūrų ar medicininių terminų kodavimui.
- 5.3.8.4 Sistemoje turi būti techninė galimybė sukurti neribotą kiekį klasifikatorių.
- 5.3.8.5 Vientisumo kontrolė ir šalinimo apribojimai: Sistemoje turi būti realizuotos kontrolės priemonės, užtikrinančios, kad nebūtų galima panaikinti ar ištrinti klasifikatorių (ar jų reikšmių), jeigu jie jau yra panaudoti operacijose ar susieti su esamais duomenimis. Tokiais atvejais reikšmė gali būti tik deaktyvuojama (padaroma negaliojančia naujiems duomenų įvedimams).
- 5.3.8.6 Masinis duomenų importas, eksportas ir dublikatų prevencija: Sistemoje turi būti galimybė klasifikatorius masiškai importuoti ir eksportuoti naudojant standartinius duomenų apsikeitimo formatus (pvz., .xlsx, .csv ar .xml). Importuojant klasifikatorių duomenis, sistema pagal nustatytas taisykles privalo automatiškai patikrinti duomenų formato korektiškumą ir išvengti dublikatų.
- 5.3.8.7 Klasifikatorių naudojimas duomenų įvedimui: Sistemos naudotojai, pildydami duomenis portale ar kituose moduluose, privalo turėti galimybę pasirinkti reikšmes iš šių sudarytų ir administratorių patvirtintų klasifikatorių sąrašų.
- 5.3.8.8 Klasifikatorių struktūra, kodavimas ir saugojimas: Klasifikatoriai ir jų reikšmės turi būti saugomi centrinėje reliacinėje SDMA IS duomenų bazėje, užtikrinant duomenų vientisumą ir greitą prieigą kitiems sistemos moduliams. Klasifikatorių duomenų struktūra turi palaikyti tiek paprastus (plokščius) sąrašus, tiek hierarchines struktūras (pvz., TLK-10 hierarchinį medį). Objektų identifikavimui turi būti galima naudoti kodus, pagal nustatytas taisykles sudarytus iš raidžių bei skaitmenų.

5.4 Funkciniai reikalavimai

5.4.1 Funkciniai realizavimo reikalavimai (Sistemos elgsena ir UI)

lentelė 3

Kodas, Scenarijaus pavadinimas ir tikslas	Funkciniai realizavimo reikalavimai (Sistemos elgsena ir UI)
A. Viešasis informacijos portalas	
A1. Svečio prieiga: Užtikrinti viešosios informacijos, naujienų, renginių bei atvirų duomenų statistikos prieinamumą neprisijungusiems naudotojams.	A1.1. Sistemoje turi būti realizuotas viešas pradinis langas su navigacijos meniu (Naujienos, Renginiai, Atviri duomenys, Kontaktai) bei mygtuku „Prisijungti“.
	A1.2. Turi būti realizuotas „Naujienų“ polapis, kuriame informacija atvaizduojama kortelėmis (data, nuotrauka, antraštė), o paspaudus – atidaromas pilnas tekstas.
	A1.3. Turi būti realizuotas „Renginių“ polapis, atvaizduojantis artėjančius įvykius chronologiniu sąrašu arba kalendoriaus formatu, nurodant renginio tipą (gyvai/nuotoliu).
	A1.4. Atvirų duomenų skiltyje turi būti realizuotas automatizuotų grafinių suvestinių (pvz., sukaupytų rinkinių ar išleistų publikacijų skaičiaus) atvaizdavimas.
A2. Atvirų duomenų ir informacijos skelbimas: Įgalinti atvirų duomenų, metaduomenų suvestinių ir pranešimų publikavimą naudojant turinio valdymo sistemą (TVS).	A2.1. Autentifikuoto naudotojo aplinkoje turi būti realizuota turinio valdymo sąsaja (WYSIWYG redaktorius), leidžianti formatuoti tekstą, įkelti failus bei nuotraukas.
	A2.2. Redagavimo lange turi būti realizuotas žymimasis langelis (angl. checkbox) „Publikuoti viešai“, kurį pažymėjus informacija automatiškai atvaizduojama A1 viešojo erdvėje.
	A2.3. Turi būti realizuotas publikuotų įrašų versijavimas, redagavimo ir archyvavimo funkcionalumas.
B. Naudotojų savitarna ir paslaugų užsakymas	
B1. Metaduomenų katalogo naršymas ir išplėstinė paieška: Suteikti naudotojams patogius įrankius ieškoti, filtruoti ir peržiūrėti informaciją apie Sistemoje sukauptus duomenų rinkinius	B1.1. Savitarnos portale turi būti realizuotas interaktyvus duomenų katalogo paieškos langas, leidžiantis atlikti paiešką pagal raktinius žodžius laisvu tekstu (ieškant per visus metaduomenų laukus).
	B1.2. Turi būti realizuoti daugelio kriterijų, dinaminiai filtrai, leidžiantys siaurinti paiešką pagal: duomenų tipą (Klinikiniai, genominiai, vaizdų ir kt.), pacientų populiaciją (amžius, lytis), klinikinius kodus, tyrimo laikotarpį ir duomenų šaltinį.

	<p>B1.3. Paieškos rezultatai turi būti atvaizduojami sąrašo arba kortelių formatu, rodant pagrindinę santrauką (rinkinio pavadinimą, tipą, eilučių/pacientų skaičių ir atnaujinimo datą).</p>
	<p>B1.4. Pasirinkus konkretų duomenų rinkinį, turi būti atidaromas detalus metaduomenų atvaizdavimo langas, kuriame struktūruotai pateikiama: duomenų kilmė, aprašymas, struktūra (lentelių ir stulpelių aprašymai), kokybės metrikos bei susijusios (jei taikoma, publikuotos) analizės.</p>
	<p>B1.5. Detalios peržiūros lange turi būti integruotas mygtukas „Teikti prieigos paraišką“, kuris automatiškai perkeltų naudotoją į užsakymo formavimo žingsnį (siejama su B2 scenarijumi).</p>
<p>B2. Duomenų rinkinio prieigos užsakymas: Suteikti galimybę tyrėjams ieškoti duomenų kataloge ir teikti užklausas jiems gauti.</p>	<p>B2.1. Turi būti realizuotas prisijungimas per SSO (Keycloak ar lygiaverčio), po kurio naudotojas nukreipiamas į asmeninę darbo aplinką (Savitarną).</p>
	<p>B2.2. Savitarroje turi būti realizuotas metaduomenų katalogo paieškos langas su daugiakriteriniais filtrais (TLK-10/Snomed, amžiaus grupės, lytis, duomenų tipas, formatas).</p>
	<p>B2.3. Pasirinkus rinkinį, atidaroma detali kortelė (metaduomenys, kilmė) su mygtuku „Teikti prieigos paraišką“.</p>
	<p>B2.4. Paraiškos formoje turi būti privalomi laukai tyrimo tikslui aprašyti ir, jei naudotojas yra studentas, laukas darbo vadovui nurodyti.</p>
	<p>B2.5. Turi būti realizuotas užklausos būsenos („Pateikta“, „Vertinama“, „Patvirtinta“) atvaizdavimas ir automatinių el. pašto pranešimų siuntimas pasikeitus būsenai.</p>
	<p>B2.6. Savitarroje turi būti galima rasti ir pasirinkti visus asmeninius teiktus (esamus ir buvusius) užsakymus. Matyti jų statusą. Turi būti galimybė atsidaryti/atsisiųsti gautą atsakymą, tyrimo rezultatą</p>
	<p>B2.7. Duomenų valdytojo aplinkoje turi būti realizuota speciali prieigos paraiškų valdymo sąsaja (darbų eilė), kurioje atvaizduojamas gautų, vertinamų ir patvirtintų / atmestų paraiškų sąrašas. Turi būti realizuota galimybė šį sąrašą filtruoti pagal paraiškos gavimo datą, būseną bei pareiškėją</p>

	B2.8. Atidarius konkrečią tyrėjo paraišką, Duomenų valdytojas privalo matyti visus pateiktus duomenis: tyrimo tikslą ir aprašymą, prašomo duomenų rinkinio aprašą. Turi būti galimybė pateikti tyrimo rezultata/atsakymą.
B3. Naudotojo prieigos užsakymas: Įgalinti išorinius naudotojus (tyrėjus) saugiai pateikti paraiškas, pasirašyti sutartis ir prisijungti prie sistemos.	B3.1. Viešajame portale turi būti realizuota išorinio naudotojo registracijos anketa (Vardas, Pavardė, Įstaiga, Pareigos, paskyros galiojimo terminas).
	B3.2. Teikiant prieigos paraišką, sistema privalo turėti privalomą lauką, kuriame išorinis tyrėjas nurodo susijusį LSMU atstovą (bendradarbį).
	B3.3. Sistema privalo automatiškai išsiųsti patvirtinimo užklausą nurodytam LSMU atstovui į jo savitarną.
	B3.4. Turi būti realizuotas duomenų naudojimo sutarties šablono generavimas ir el. sutikimo fiksavimas.
	B3.5. Administratoriui patvirtinus, sistema automatiškai sukuria IAM paskyrą naudotojui ir išsiunčia prisijungimo duomenis.
	B3.6. Naudotojui pirmą kartą prisijungus prie sistemos (per suteiktą IAM paskyrą), sistema privalo pareikalauti pasikeisti pradinį slaptažodį ir pritaikyti dviejų veiksmių autentifikaciją (MFA) saugiam darbui.
	B3.7. Pasibaigus numatytam prieigos laikotarpiui arba tyrimo projektą pažymėjus kaip baigtą (jei paskyra sukurta išoriniam tyrėjui), sistema privalo automatiškai panaikinti išorinio tyrėjo prieigos teises prie duomenų ir deaktyvuoti (užblokuoti) jo IAM paskyrą.
C. Tyrimų projektų ir analitikos valdymas	
C1. Duomenų analizės užsakymas: Užtikrinti tyrėjų ir analitikų bendradarbiavimą naudojant vidinę užduočių (<i>ticketing</i>) sistemą.	C1.1. Tyrėjo aplinkoje turi būti realizuota naujos analizės užduoties formavimo forma (tyrimo tikslas, laukiamas rezultatas, terminai).
	C1.2. Turi būti realizuotas komentarų (žinučių) modulis prie užduoties lango, leidžiantis tyrėjui ir analitikui saugiai susirašinėti ir prisegti papildomus failus.
	C1.3. Analitiko aplinkoje turi būti atvaizduojamas gautų užduočių sąrašas ir mygtukas „Įkelti rezultata“ (kartu pridedant naudotus skriptus, programų versijas).
	C1.4. Sistema privalo sekti ir atvaizduoti užduoties būsenas („Nauja“, „Vykdoma“, „Koreguojama“, „Baigta“).

C2. Duomenų eksportas: Suteikti galimybę tyrėjams ir analitikams saugiai išeksportuoti patvirtintus duomenis atvirais formatais.	C2.1. Prie patvirtinto duomenų rinkinio ar analizės rezultato turi būti atvaizduojamas mygtukas „Eksportuoti duomenis“.
	C2.2. Paspaudus mygtuką, turi atsirasti išskleidžiamasis sąrašas formato pasirinkimui (CSV, JSON, Parquet, PDF ir kt.).
	C2.3. Sistema privalo sugeneruoti failą, pateikti saugią atsisiuntimo nuorodą ir automatiškai išsiųsti įrašą į audito žurnalą (kas, ką ir kada atsisiuntė).
D. Duomenų valdysena ir tvarkymas	
D1. Naujo duomenų rinkinio įkėlimas: Suteikti įrankius tyrėjams įkelti naujus duomenų rinkinius.	D1.1. Turi būti realizuotas žingsninis duomenų įkėlimo vedlys (angl. <i>Wizard</i>): Prieigos lygis -> Tipas -> Šaltinis -> Struktūra -> Formatas -> Privatumo lygis.
	D1.2. Turi būti realizuotas metaduomenų anketos langas ir privalomas laukas Bioetikos leidimo (PDF formatu) įkėlimui (jei pasirinktas atitinkamas duomenų tipas).
	D1.3. Failo įkėlimo lange sistema privalo vykdyti dydžio kontrolę ir klaidos atveju rodyti informacinį pranešimą.
	D1.4. Įkėlus failą, turi būti rodomas apdorojimo būsenos indikatorius (nukreipiama į pseudonimizavimą ir saugyklą).
D2 Genominių tyrimų ir sekoskaitos duomenų metaduomenų įkėlimas bei susiejimas: Suteikti įrankius tyrėjams ir duomenų valdytojams per naudotojo sąsają įkelti genomo sekoskaitos metaduomenis.	D2.1. Naudotojo sąsajoje turi būti realizuota specializuota įvedimo forma arba „Excel“ / CSV failų importo instrumentas, skirtas genominių tyrimų metaduomenims įkelti. Forma privalo apimti privalomus duomenų blokus: projekto duomenis, mėginio aprašą, sekoskaitos eksperimento parametrus bei duomenų apdorojimo santrauką.
	D2.2. Pildant ar importuojant metaduomenis, turi būti realizuotas specialus laukas „Nuoroda į duomenų failą“. Sistemos naudotojas šiame lauke turi galėti įvesti išorinėje failinėje ar objektinėje (pvz., S3) saugykloje gulinčio fizinio failo (FASTQ, BAM, VCF) URI / URL adresą ar unikalų identifikatorių.
	D2.3. Sistema privalo turėti techninį mechanizmą, kuris, naudotojui išsaugant metaduomenis, foniniu režimu automatiškai patikrintų nurodytos išorinės nuorodos (failo kelio) pasiekiamumą ir suformuotų validacijos pranešimą ekrane (pvz., „Failas sėkmingai susietas“ arba „Klaida: failas išorinėje saugykloje nerastas“).

	<p>D2.4. Turi būti užtikrintas saugus prieigos suteikimas: tyrėjui ar analitikui gavus patvirtintą prieigą prie genominių duomenų rinkinio, sistema privalo automatiškai sugeneruoti ir pateikti laikiną, riboto galiojimo saugią nuorodą (pvz., S3 pre-signed URL). Ši nuoroda turi leisti naudotojui atsisiųsti fizinį „žaliąjį“ failą į savo kompiuterį arba tiesiogiai jį nuskaityti su paties pasirinktais analitikos įrankiais.</p>
<p>D3. Duomenų katalogavimas ir indeksavimas: Automatizuoti naujų duomenų indeksavimą bei suteikti įrankius priskirti žymas.</p>	<p>D3.1. Sistema privalo atlikti automatinį naujų failų / lentelių metaduomenų nuskaitymą ir sukatalogavimą.</p> <p>D3.2. Duomenų architekto aplinkoje turi būti realizuota sąsaja, kurioje jis gali rankiniu būdu priskirti standartizuotas žymas (pvz., TLK-10 kodus iš klasifikatoriaus) suindeksuotiems rinkiniams.</p>
<p>D4. Automatinis asmens duomenų ar zavimas: Identifikuoti asmens duomenis ir pakeisti juos pseudonimais užrakinant raktus.</p>	<p>D4.1. Turi būti realizuotas foninis procesas (ARX ar lygiaverčio įrankio integracija), kuris skenuoja gaunamus duomenis pagal administratoriaus įvestas paieškos taisykles (RegEx) asmens kodams ir vardams atpažinti.</p> <p>D4.2. Sistema privalo automatiškai deterministiškai pakeisti rastus identifikatorius pseudonimais prieš įrašant į galutinę DB.</p> <p>D4.3. Atkodavimo (de-pseudonimizavimo) raktų lentelė turi būti kriptografiškai užrakinama ir pasiekama tik tokią teisę turinčiam naudotojui.</p>
<p>D5. Sveikatos duomenų registrų pildymas per naudotojo sąsają (GUI importas): Suteikti galimybę naudotojams rankiniu būdu, per grafinę sąsają įkelti ir atnaujinti struktūrizuotus sveikatos duomenų registrų (pvz., kardiologijos, slaugos) įrašus iš failų.</p>	<p>D5.1. Naudotojo sąsajoje turi būti realizuotas duomenų importo įrankis, leidžiantis pasirinkti atitinkamą sveikatos duomenų registrą ir tiesiogiai įkelti duomenų failus. Turi būti palaikomi .xlsx (Microsoft Excel), .csv bei .xml duomenų apsiųtimo formatai.</p> <p>D5.2. Sistemoje turi būti instrumentas (sąsaja), leidžiantis sukurti ir pakartotinai naudoti duomenų importo formato šablonus (angl. <i>mapping</i>). Naudotojas turi galėti susieti įkeliamo failo stulpelius su atitinkamais registro duomenų bazės laukais (atributais).</p> <p>D5.3. Įkeliant duomenis, sistema privalo automatiškai (pagal nustatytas taisykles ir/ar šabloną) patikrinti duomenų formato korektiškumą (pvz., raidinis, skaitinis) bei atlikti unikalų identifikacinių laukų dublikatų kontrolę. Aptikus neatitikimų, sistema ekrane turi pateikti detalią informaciją naudotojui apie rastos klaidas prieš jas išsaugant.</p>

	<p>D5.4. Importo metu sistema turi automatiškai audituoti procesą: registruoti duomenis importavusį naudotoją, tikslią importavimo datą ir laiką.</p>
	<p>D5.5. Sveikatos duomenų registrų pavienių įrašų pildymas per grafinę sąsają: Sistema turi suteikti galimybę naudotojams per grafinę naudotojo sąsają (GUI) rankiniu būdu sukurti, peržiūrėti ir redaguoti pavienius sveikatos duomenų registro įrašus (pvz., sporto ir traumų registro duomenis), juos pildant po vieną realiu laiku. <i>Paiškinimas:</i> <i>Ši funkcija skirta operatyviam duomenų registravimui, kai įrašai atsiranda individualiai (pvz., po paciento vizito). Forma turi būti struktūruota pagal registro duomenų modelį, naudoti klasifikatorius (išskleidžiamus sąrašus), validuoti įvedamus duomenis bei užtikrinti privalomų laukų kontrolę.</i></p>
	<p>D5.6. Pavienių įrašų pildymo UX reikalavimai:</p> <p>Naudotojo sąsajoje pateikiama duomenų įvedimo forma turi būti logiškai suskirstyta į sekcijas pagal duomenų grupes (pvz., paciento duomenys, diagnozė, tyrimai, išvados ir pan.).</p> <p>Visi laukai, kuriems taikomi klasifikatoriai, turi būti pateikiami kaip išskleidžiami sąrašai (dropdown), radijo mygtukai arba pasirinkimo sąrašai.</p> <p>Privalomi laukai turi būti aiškiai pažymėti (pvz., * arba spalva), o validacijos klaidos – rodomos realiu laiku šalia konkretaus lauko.</p> <p>Forma turi būti optimizuota greitam vieno įrašo sukūrimui (minimalus paspaudimų skaičius, galimybė išsaugoti vienu mygtuku, galimybė „Išsaugoti ir kurti naują“)</p> <p>Duomenų saugos ir klaidų prevencija (Sistema turi perspėti prieš uždarančią formą neišsaugojus duomenų).</p>
<p>D6. Duomenų validavimas ir standartizavimas: Suteikti įrankius duomenų valdytojui peržiūrėti ir standartizuoti gautus duomenis.</p>	<p>D6.1. Duomenų valdytojo aplinkoje turi būti atvaizduojamas laukiančių (naujai įkeltų ar importuotų) duomenų sąrašas.</p> <p>D6.2. Turi būti realizuotas peržiūros įrankis ir mygtukai „Patvirtinti“ / „Atmesti“.</p> <p>D6.3. Patvirtinus duomenis, UI mygtukas privalo iššaukti automatizuotą ETL darbo seką (pvz., Airflow ar lygiavertis), kuri transformuos duomenis į OMOP CDM formatą ir perkels į pagrindinį archyvą.</p>
<p>E. Sistemos administravimas, auditas ir statistika</p>	
<p>E1. Naudotojų administravimas: Suteikti centralizuotus įrankius kurti paskyras, priskirti roles bei valdyti RBAC visoje platformoje.</p>	<p>E1.1. Turi būti integruota grafinė IAM valdymo sąsaja administratoriams, leidžianti kurti naudotojus, priskirti jiems vieną ar kelias roles ir nustatyti slaptažodžių politiką.</p> <p>E1.2. Turi būti realizuotas aktyvių (prisijungusių) sesijų sąrašo atvaizdavimas su galimybe mygtuko paspaudimu priverstinai nutraukti pasirinktą sesiją.</p>
<p>E2. Kibernetinis saugumas ir auditavimas: Užtikrinti sistemos atsparumą grėsmėms</p>	<p>E2.1. Auditoriui turi būti pasiekiami specialieji audito paieškos sąsaja (Kibana/OpenSearch Dashboards arba lygiavertės) su išplėstiniais filtrais pagal IP, naudotoją, įvykio datą ir veiksmą.</p> <p>E2.2. Turi būti realizuotas automatinis perspėjimų (Alerts) funkcionalumas ekrane fiksavus anomalijas (pvz., 5 nesėkmingi prisijungimai iš eilės, masinis eksportas).</p>

	<p>E2.3. Turi būti realizuota paskyrų blokavimo funkcija: po nustatyto nesėkmingų bandymų prisijungti skaičiaus, naudotojo paskyra turi būti laikinai blokuojama, o šie incidentai privalo būti fiksuojami audito žurnaluose.</p>
	<p>E2.4. Tapatybės valdymo (IAM) komponente turi būti realizuota ir priverstinai taikoma griežta slaptažodžių sudėtingumo kontrolė, reikalaujanti ne trumpesnio nei 12 simbolių slaptažodžio, kuriame privalo būti didžiųjų ir mažųjų raidžių, skaičių bei specialiųjų simbolių. Taip pat turi būti galimybė priverstinai reikalauti pakeisti slaptažodį po nustatyto laiko (pvz., 90 dienų) bei techninis draudimas naudoti nustatytą skaičių buvusių slaptažodžių.</p>
	<p>E2.5. Turi būti realizuotas saugus sesijų valdymas, užtikrinantis sesijų žetonų (angl. <i>tokens</i>) apsaugą nuo perėmimo, ir automatiškai nutraukiantis naudotojo sesiją (atjungiantis iš sistemos) po iš anksto nustatyto pasyvumo (neveiklumo) laiko.</p>
	<p>E2.6. Administratoriui turi būti suteikta galimybė per centralizuotą tapatybės valdymo sąsają įjungti ir priverstinai reikalauti dviejų veiksmų autentifikacijos (MFA / 2FA) prisijungiant visiems arba tik pasirinktiems (privilegiuotiems ar dirbantiems su jautriais duomenimis) naudotojams.</p>
	<p>E2.7. Sistemoje turi būti realizuotas centralizuotas, izoliuotas kriptografinių raktų bei pseudonimizavimo parametrų („druskų“) valdymo komponentas (pvz., „HashiCorp Vault“), užtikrinantis saugų šių duomenų saugojimą ir atskyrimą nuo pagrindinių duomenų bazių.</p>
<p>E3. DAC veiklos valdymas ir statistika: Suteikti centro vadovui interaktyvią stebėsenos švieslentę (<i>dashboard</i>) su realiojo laiko statistika.</p>	<p>E3.1. Vadovo savitarroje turi būti realizuota interaktyvi grafinė švieslentė, rodanti KPI rodiklius (aktyvūs projektai, apdorojami duomenys, analitikų užduotys).</p>
	<p>E3.2. Švieslentėje turi būti integruotas mygtukas „Generuoti metinę veiklos ataskaitą“, kuris iš visų modulių surenka suvestinę į vieną struktūruotą dokumentą.</p>

5.4.2 Reikalavimai duomenų/dokumentų importui ir eksportui

- 5.4.2.1 Sistemoje turi būti galima importuoti ir eksportuoti neribotą duomenų eilučių skaičių (atsižvelgiant į objektyvias technologines galimybes).
- 5.4.2.2 Sistemoje turi būti importuojami ir eksportuojami duomenys naudojant populiariausius duomenų apsikeitimo formatus *xlsx*, *xml*, *csv*, *json*, *pdf* ar pan.

- 5.4.2.3 Sistemoje turi būti realizuotas būti instrumentas, leidžiantis sukurti ir pakartotinai naudoti duomenų importo formato šabloną (t.y. išsaugoti informaciją apie tai, kokių sistemos objektų kokie atributai užpildomi pagal kiekvieną importuojamų duomenų struktūros lauką).
- 5.4.2.4 Sistemoje turi būti galima importuojant duomenis tikrinti kontrolinę ar kitą patiekiamos informacijos apsaugos informaciją ir pateikti informaciją apie aptiktas klaidas.
- 5.4.2.5 Sistemoje turi būti galima pagal nustatytas taisykles automatiškai patikrinti importuojamų duomenų formato korektiškumą, pvz.: raidinis, skaitinis.
- 5.4.2.6 Sistemoje turi būti registruojamas duomenis importavęs Sistemos naudotojas, duomenų importavimo data ir laikas, duomenų failo, iš kurio importuoti duomenys pavadinimas.

5.4.3 Bendrieji reikalavimai ataskaitoms

- 5.4.3.1 Sistema turi registruoti ir kaupti visą reikiamą informaciją numatytų ataskaitų suformavimui.
- 5.4.3.2 Sistemoje turi būti galima formuoti (generuoti), atsispausdinti suderintu formatu nustatytas ataskaitas pagal naudotojo pasirenkamus parametrus. Sistemos naudotojas gali keisti ataskaitos parametrus.
- 5.4.3.3 Sistemoje turi būti galima suformuotas spausdinimui ataskaitas ar kt. dokumentus eksportuoti į failus (pvz.: .docx, .xlsx, .pdf).
- 5.4.3.4 Sistemoje turi būti galima suformuotus įrašų rodinius ar sąrašus eksportuoti į duomenų apdorojimui tinkamus skaitmeninius formatus (pvz.: .xlsx ar .csv).

5.4.4 Ataskaitų sąrašas:

- 5.4.4.1 **Prieigos užklausų apdorojimo efektyvumo ataskaita:** Sistema turi generuoti ataskaitą, kurioje pateikiamas visų pateiktų prieigos užklausų skaičius, jų būsenos (laukiančios, patvirtintos, atmestos), vidutinis ir maksimalus nagrinėjimo laikas bei užklausų pasiskirstymas pagal duomenų rinkinius ir naudotojų tipus. *Paskirtis:* Įvertinti prieigos suteikimo procesų efektyvumą ir identifikuoti vėlavimus
- 5.4.4.2 **Prieigos prie duomenų ataskaita:** Sistema turi leisti suformuoti ataskaitą apie aktyvias prieigas prie duomenų rinkinių, nurodant naudotojus, turinčius prieigą, jų roles, prieigos galiojimo laikotarpius bei išskiriant pasibaigusias ar artėjančias prieigos pabaigos datas. *Paskirtis:* Užtikrinti prieigos teisėtumą, kontrolę ir atitiktį duomenų apsaugos reikalavimams.
- 5.4.4.3 **Duomenų rinkinių skaičiaus dinamikos ataskaita:** Sistema turi pateikti bendrą kaupiamų duomenų rinkinių skaičių, naujai įkeltus rinkinius per ataskaitinį laikotarpį ir jų pasiskirstymą pagal duomenų tipus ar valdytojus. *Paskirtis:* Stebėti duomenų bazės plėtrą ir planuoti saugojimo bei administravimo resursus.
- 5.4.4.4 **Duomenų pakartotinio naudojimo ataskaita:** Sistema turi kaupti ir atvaizduoti informaciją apie tai, kiek kartų konkretūs duomenų rinkiniai buvo naudoti, naudojimo tikslus (projektus, tyrimus) bei identifikuoti nenaudojamus rinkinius. *Paskirtis:* Įvertinti duomenų rinkinių vertę ir jų faktinį pritaikymą moksliniuose tyrimuose.
- 5.4.4.5 **Naudotojų bazės augimo ataskaita:** Sistema turi generuoti registruotų naudotojų skaičiaus suvestines, išskiriant naujai prisijungusius ir deaktyvuotus naudotojus bei pateikiant jų pasiskirstymą pagal atstovaujamas institucijas. *Paskirtis:* Matuoti sistemos pasiekiamumą ir naudojimą tyrėjų bendruomenėje.
- 5.4.4.6 **Naudotojų aktyvumo koeficiento ataskaita:** Sistema turi skaičiuoti ir atvaizduoti aktyvių naudotojų skaičių, naudotojų (kurie per apibrėžtą laikotarpį pateikė bent vieną užklausą ar registraciją) dalį bei aktyvumo pokytį per laiką. *Paskirtis:* Atskirti aktyvius naudotojus nuo formaliai registruotų paskyrų.
- 5.4.4.7 **Konsultacijų teikimo ataskaita:** Remiantis sistemoje registruotomis užduotimis (konsultacijomis), turi būti formuojama ataskaita apie suteiktų konsultacijų skaičių, temas, konsultacijų trukmę ir analitikų apkrovos pasiskirstymą. *Paskirtis:* Vertinti Centro konsultacinės veiklos mastą ir planuoti specialistų darbo krūvį.
- 5.4.4.8 **Analitikų darbo krūvio (apkrovos) ataskaita:** Sistema turi teikti informaciją apie analitiko aptarnautų užklausų ir konsultacijų skaičių, bendrą darbų pasiskirstymą tarp analitikų ir laikotarpio apkrovos tendencijas. *Paskirtis:* Pagrįsti darbo krūvio paskirstymą ir personalo poreikį.

- 5.4.4.9 **Duomenų prieigos ir veiksmų atsekamumo (audito) ataskaita:** Remiantis audito žurnalu, sistema turi generuoti ataskaitą, rodančią naudotojų prisijungimų ir veiksmų registrus, prieigos prie jautrių duomenų atvejus bei fiksuotas anomalijas ar neatitiktis. *Paskirtis:* Užtikrinti BDAR laikymąsi ir pasirengimą auditams.
- 5.4.4.10 **Duomenų mainų ir eksporto ataskaita:** Sistema turi atvaizduoti įvykdytus duomenų eksporto atvejus, eksportuotų duomenų apimtį, gavėjų tipus ir tikslus. *Paskirtis:* Valdyti ir prižiūrėti duomenų antrinį naudojimą bei išorinę sąveiką.
- 5.4.4.11 **Vadovo suvestinė (angl. Dashboard):** Sistemoje turi būti realizuota grafinė vadovo suvestinė, kurioje realiu laiku atvaizduojami pagrindiniai veiklos rodikliai (naudotojai, duomenų rinkiniai, paslaugos), tendencijos per pasirinktą laikotarpį bei apkrovos ir rizikų indikatoriai. *Paskirtis:* Greita apibendrinta Centro veiklos apžvalga.
- 5.4.4.12 **Metinė SDMA IS veiklos ataskaita:** Sistema turi turėti funkcionalumą sugeneruoti apibendrintą metinę visų pagrindinių rodiklių suvestinę, atspindinčią Centro veiklos apimtį ir pasiektų rezultatų apžvalgą. *Paskirtis:* Atskaitomybė Universiteto vadovybei ir finansuotojams.

6. Reikalavimai paslaugų teikimui

6.1 Bendrieji reikalavimai SDMA IS sukūrimo ir įdiegimo paslaugoms

- 6.1.1.1 Projektų valdymo metodologija ir įgyvendinimo etapai: Sistemos sukūrimo ir įdiegimo paslaugos privalo būti vykdomos taikant lanksčius (angl. Agile) programinės įrangos kūrimo ir projektų valdymo principus. Siekiant efektyvaus projekto valdymo, paslaugų teikimas skirstomas į etapus.
- 6.1.1.2 Paslaugų teikimo reglamento parengimas: Prieš pradėdant faktišką paslaugų teikimą, Tiekėjas privalo parengti ir oficialiai suderinti su Perkančiąja organizacija detalų paslaugų teikimo reglamentą. Šiame dokumente privalo būti aiškiai apibrėžta:
- paslaugų suteikimo grafikas ir terminai;
 - naudojama programinės įrangos kūrimo metodika ir įrankiai;
 - taikomi standartai ir kokybiniai reikalavimai;
 - šalių komunikavimo principai ir atsakomybės;
 - paslaugų teikimo problemų, rizikų nustatymo ir valdymo procedūros;
 - nenumatytų reikalavimų ar pakeitimų (angl. change requests) valdymo tvarka;
 - tarpinių ir galutinių rezultatų priėmimo kriterijai.
- 6.1.1.3 Projekto stebėseną ir tarpinis atsiskaitymas: Tiekėjas projekto įgyvendinimo metu privalo reguliariai (pagal suderintame reglamente nustatytą dažnumą) informuoti Perkančiąją organizaciją apie atliktus darbus, spręstinas problemas bei kylančias rizikas.

6.2 1 etapas: Analizė ir architektūrinis projektavimas

- 6.2.1.1 Poreikių analizė ir architektūros projektavimas: Tiekėjas privalo atlikti detalų Perkančiosios organizacijos poreikių ir šiuo metu vykdomų procesų analizę bei parengti ir suderinti galutinį Sprendimo techninės architektūros dokumentą.
- 6.2.1.2 Naudotojų teisių ir rolių matricos parengimas: Tiekėjas, vadovaudamasis gautais ir suderintais Perkančiosios organizacijos naudotojų grupių ir teisių reikalavimais, privalo parengti IS naudotojų grupių ir jų teisių nustatymo aprašymą (teisių matricą) ir pagal ją apibrėžti naudotojų grupių atitinkamas teises ir vaidmenis Sistemoje.
- 6.2.1.3 Naudotojo sąsajos ir ataskaitų parengimas ir parametrizavimas: Tiekėjas privalo pateikti visų šioje specifikacijoje įvardintų bei analizės metu apibrėžtų naudotojo sąsajos (GUI) langų, ataskaitų ir dokumentų dizainus bei preliminarinius vizualinius šablonus (angl. wireframes, mockups). Šie dizaino šablonai privalo būti pristatyti, suderinti ir patvirtinti Perkančiosios organizacijos prieš pradėdant Sistemos įdiegimą.

- 6.2.1.4 Analizės sesijų organizavimas: Analizės sesijos turi vykti Perkančiosios organizacijos patalpose arba, Šalims atskirai susitarus, nuotoliniu būdu (pvz., per „Microsoft Teams“ platformą).
- 6.2.1.5 Etapo rezultatas ir priėmimas: Šio etapo rezultatas – parengti ir Perkančiosios organizacijos oficialiai patvirtinti dokumentai: detalus Sprendimo techninės architektūros dokumentas, naudotojų teisių matrica bei patvirtinti naudotojo sąsajos (GUI) vizualiniai šablonai (dizainai). Etapo atlikimas fiksuojamas Šalims pasirašant pirmojo etapo tarpinį paslaugų perdavimo–priėmimo aktą.

6.3 2 etapas: Sistemos instaliavimas ir konfigūravimas

- 6.3.1.1 Infrastruktūros suteikimo ir komponentų atsakomybių pasiskirstymas: Pirkėjas suteikia fizinę infrastruktūrą, virtualizacijos platformą, serverinius resursus, skirtus testinei ir gamybinei aplinkai, taip pat VPN infrastruktūrą ar kitą saugaus tinklinio pasiekiamumo priemonę, reikalingą prieigai prie Pirkėjo resursų užtikrinti. Tiekėjas savo ruožtu privalo parengti, pateikti, įdiegti, sukonfigūruoti ir tarpusavyje integruoti visus kitus SDMA IS sudarančius programinius komponentus ir bazines technologines priemones, numatytas techninėje specifikacijoje ir Tiekėjo pasiūlyme.
- 6.3.1.2 Infrastruktūros ir bazinės programinės įrangos diegimas: Tiekėjas privalo parengti, sukonfigūruoti ir įdiegti Sistemos veikimui būtiną programinę įrangą Pirkėjo infrastruktūroje: virtualizacijos ar konteinerizacijos platformas, atviro kodo duomenų bazes, objektų saugyklas, tapatybės valdymo bei kitus bazinius (angl. core) sisteminius komponentus.
- 6.3.1.3 Sistemos modulių konfigūravimas ir programavimas: Tiekėjas privalo atlikti visą reikalingą Sistemos komponentų (mikroservisų, API sąsajų, atviro kodo įrankių) konfigūravimą, integraciją, modifikavimą ir papildomą programavimą, kad atskiri moduliai sklandžiai keistųsi duomenimis ir veiktų kaip viena vieninga Sistema, pilnai paruošta naudotojų darbui.
- 6.3.1.4 Sistemos pradinį duomenų parengimas: Tiekėjas privalo sukomplektuoti, importuoti ir sukonfigūruoti visus Sistemos veikimui būtinus pradinis duomenis (naudotojų roles ir teisių matricas, specifikacijoje numatytus klasifikatorius bei žinytus, saugumo komponentų kriptografinius raktus ir eksperimentinius pseudonimizavimo parametrus) bei atlikti bazinių sveikatos duomenų rinkinių bandomąjį įkėlimą ir pseudonimizavimo bandymą, kad atskiri moduliai turėtų reikiamą pradinę informaciją ir nuo pat perdavimo momento Sistema būtų paruošta naudotojų darbui.
- 6.3.1.5 Saugus diegimas ir testavimas gamybinėje aplinkoje: Prieš atliekant bet kokius diegimus gamybinėje aplinkoje (angl. production), Tiekėjas privalo visus pakeitimus pilnai ištestuoti izoliuotoje testinėje aplinkoje. Turi būti griežtai užtikrinta, kad diegiama programinė įranga neturi kenksmingo kodo ar neautorizuotos prieigos spragų (angl. backdoors), o naujų komponentų įdiegimas nesutrikdys bendros Pirkėjo infrastruktūros ar atskirų jos dalių veikimo.
- 6.3.1.6 Etapo rezultatas ir priėmimas: Šio diegimo ir konfigūravimo etapo (arba atskirų jo dalių pagal suderintą paslaugų teikimo grafiką) rezultatas – sėkmingai įdiegta, sukonfigūruota, ištestuota ir Pirkėjo aplinkoje veikianti Sistema (arba atitinkamas jos modulis / MVP versija). Etapo (ar jo dalies) atlikimas fiksuojamas Šalims pasirašant tarpinį paslaugų perdavimo–priėmimo aktą.

6.4 3 etapas: Testavimas, mokymai ir perdavimas naudojimui

- 6.4.1.1 Sistemos testavimas ir bandomoji eksploatacija: Prieš perduodant Sistemą galutiniam naudojimui (gamybinei eksploatacijai), Tiekėjas privalo atlikti baigiamuosius funkcinio veikimo, saugumo (pažeidžiamumų paieškos) ir našumo (apkrovos) testavimus bei ištaisyti visus nustatytus trūkumus. Testavimo rezultatai privalo būti įforminti oficialiose testavimo ataskaitose.
- 6.4.1.2 Naudotojų ir administratorių mokymai: Atlikęs visus SDMA IS kūrimo ir diegimo darbus, Tiekėjas privalo apmokyti Pirkėjo paskirtus asmenis. Turi būti organizuojamos atskiros mokymų sesijos Sistemos administratoriams (dėl techninės priežiūros, konfigūracijų ir IAM valdymo) bei pagrindiniams naudotojams (tyrėjams, duomenų valdytojams, analitikams).

- 6.4.1.3 Programinės įrangos dokumentacijos parengimas: Tiekėjas privalo parengti ir Pirkėjui perduoti išsamią techninę bei naudotojų dokumentaciją lietuvių arba anglų kalba. Šį paketą privalo sudaryti ne mažiau kaip: sistemos administratoriaus vadovas, naudotojo vadovas (pritaikytas skirtingoms rolėms) ir galutinis, faktinę realizuotą būklę atspindintis Sistemos architektūros aprašas.
- 6.4.1.4 Sistemos kodo, konfigūracijų ir licencijų perdavimas: Perduodamas Sistemą naudojimui, Tiekėjas kartu privalo Pirkėjui pateikti saugiose kodo saugyklose perduoti:
- Visas Sistemai naudoti būtinas licencijas (taikomas tiek specialiai sukurtam kodui, tiek integruotiems komponentams, įskaitant atviro kodo);
 - Pilną atvirą išėitį ir modifikavimo kodą (angl. source code);
 - Sistemos infrastruktūros, diegimo ir konfigūracijų failus, įskaitant konteinerizacijos skriptus (pvz., „Docker“ vaizdus, „Kubernetes“ manifestus) ir duomenų inžinerijos algoritmus (pvz., „Apache Airflow DAGs“);
 - Duomenų bazių struktūrų aprašymus ir API integracinių sąsajų specifikacijas ir dokumentaciją;
 - Paruoštą virtualią mašiną (VM) su pilnai sukonfigūruota kūrimo (programavimo) aplinka (angl. Development Environment). Šioje aplinkoje turi būti įdiegti ir sukonfigūruoti visi reikalingi įrankiai, kompiliatoriai, bibliotekos ir priklausomybės (angl. dependencies), leidžiantys Pirkėjo programuotojams be papildomų konfigūravimo darbų iš karto savarankiškai peržiūrėti, keisti, kompiliuoti ir sukurti (angl. build) veikiančią Sistemos versiją iš perduoto išėitio kodo.
- 6.4.1.5 Etapo rezultatas ir priėmimas: Šio etapo pabaiga ir galutinis Sistemos priėmimas fiksuojamas pasirašant galutinį Paslaugų perdavimo–priėmimo aktą. Aktas gali būti pasirašomas tik atlikus Sistemos perdavimo ir priėmimo procedūras, aprašomas žemiau.
- 6.4.1.6 Sistemos perdavimo ir priėmimo bendroji tvarka: Prieš inicijuodamas galutinį Sistemos perdavimą, Tiekėjas privalo būti užbaigęs visus pagal techninę specifikaciją numatytus Sistemos sukūrimo, konfigūravimo, integravimo, testavimo, dokumentavimo ir mokymų darbus bei pateikti Pirkėjui perdavimui skirtą Sistemos versiją kartu su visa privaloma perdavimo medžiaga. Sistemos priėmimas vykdomas Pirkėjui atliekant priėmimo testavimą, kurio metu vertinama bendra Sistemos veikimo visuma, modulių tarpusavio sąveika, atitiktis techninės specifikacijos reikalavimams, analizės etape suderintiems dokumentams ir perdavimo metu pateiktos medžiagos pilnumas.
- 6.4.1.7 Perdavimo metu Tiekėjas privalo pateikti ne mažiau kaip šiuos testavimo ir perdavimo dokumentus: testavimo planą, testavimo scenarijų ar testinių atvejų rinkinį, testavimo rezultatų ataskaitą, nustatytų ir ištaisytų trūkumų registrą, o kai taikoma – saugumo testavimo, pažeidžiamumų vertinimo ir našumo testavimo ataskaitas, taip pat visą 6.4 punkte nurodytą dokumentaciją, išėitį kodą, konfigūracijas, licencijas ir kitą perduotiną medžiagą.
- 6.4.1.8 Priėmimo metu nustatyti trūkumai turi būti fiksuojami rašytiniame trūkumų sąrašė arba protokole. Tokiame sąrašė turi būti nurodytas bent trūkumo numeris, trūkumo aprašymas, su trūkumu susijęs techninės specifikacijos ar suderinto projekto dokumento punktas, trūkumo reikšmingumas (kritinis arba nekritis), Tiekėjo siūlomas ar Šalių suderintas ištaisymo terminas bei pakartotinio patikrinimo rezultatas.
- 6.4.1.9 Kritiniu trūkumu laikomas toks Sistemos neatitikimas, klaida ar defektas, dėl kurio neveikia bent vienas techninėje specifikacijoje numatytas privalomas funkcionalumas, pažeidžiami informacijos saugumo ar prieigos valdymo reikalavimai, neįmanomas duomenų įkėlimas, paieška, prieigos valdymas, auditavimas ar kitas esminis Sistemos naudojimas pagal paskirtį, Sistema veikia nestabiliai arba kyla duomenų praradimo, sugadinimo ar iškraipymo rizika. Kritiniai trūkumai blokuoja Sistemos priėmimą.
- 6.4.1.10 Nekritiniais trūkumais laikomi tokie neatitikimai ar defektai, kurie netrukdo naudoti Sistemą pagal paskirtį, nepaneigia privalomų funkcionalumų veikimo, nesukelia duomenų praradimo ar saugumo pažeidimo rizikos ir gali būti pašalinti po priėmimo per Šalių suderintą terminą. Esant tik nekritiniams trūkumams, Sistema gali būti priimama su pastabomis, jeigu tokie trūkumai yra aiškiai užfiksuoti trūkumų sąrašė ar protokole ir nustatyti konkretūs jų pašalinimo terminai.
- 6.4.1.11 Jeigu priėmimo testavimo metu nustatomi trūkumai, Tiekėjas privalo juos ištaisyti per suderintą terminą ir pakartotinai pateikti Sistemą tikrinimui. Po trūkumų ištaisymo Pirkėjas atlieka pakartotinį tikrinimą ta apimtimi, kuri reikalinga įsitikinti, kad nustatyti trūkumai pašalinti ir kad atlikti pakeitimai nesukėlė naujų neatitikimų ar Sistemos veikimo sutrikimų.

- 6.4.1.12 Galutinis Paslaugų perdavimo–priėmimo aktas gali būti pasirašomas tik tada, kai: a) Sistema atitinka techninės specifikacijos reikalavimus ir analizės etape suderintus dokumentus; b) nėra kritinių trūkumų; c) perduota visa pagal 6.4 ir šį skyrių privaloma dokumentacija, išėties kodas, konfigūracijos, licencijos ir kita perduotina medžiaga.

6.5 Informacijos saugumo ir konfidencialumo reikalavimai Tiekėjui paslaugų teikimo metu

- 6.5.1.1 Konfidencialumo užtikrinimas ir paslapties saugojimas: Tiekėjas turi užtikrinti ir garantuoti, kad jo darbuotojai, kurie atliks Paslaugą, saugos Paslaugos teikimo metu gautos informacijos paslaptį tiek Paslaugos teikimo metu, tiek pasibaigus Paslaugos sutarčiai, tiek pasibaigus Tiekėjo darbuotojų darbo ar kitokiems santykiams su Tiekėju. Visi informacijos saugumo ir konfidencialumo reikalavimai, taikomi Tiekėjui, tiesiogiai taikomi ir jo subtiekJams.
- 6.5.1.2 Medžiagos grąžinimas ir duomenų sunaikinimas: Po paslaugos atlikimo, Tiekėjui pateikta medžiaga turi būti grąžinta Perkančiajai organizacijai (jei tai medžiaga popieriniu formatu), o elektroniniai dokumentai ir kopijos turi būti negrįžtamai sunaikinti. Medžiagos grąžinimą ir gautų elektroninių dokumentų sunaikinimą Tiekėjas privalo patvirtinti raštu.
- 6.5.1.3 Testavimas ir sintetinių duomenų naudojimas: Testavimas negali būti vykdomas su realiais asmens ar sveikatos duomenimis. Sistemos kūrimo, konfigūravimo ir testavimo metu Tiekėjas privalo naudoti tik nuasmenintus, sintetinius (netikrus) duomenis. Išimtiniais atvejais, suderintais su Perkančiąja organizacija, kai testavimui būtini realūs duomenys, privalo būti naudojamos organizacinės ir techninės duomenų saugumo priemonės, užtikrinančios šių duomenų saugumą.
- 6.5.1.4 Saugus programavimas ir kenksmingo kodo prevencija: Atliekant diegimus į Perkančiosios organizacijos infrastruktūrą, Tiekėjas privalo užtikrinti ir patikrinti, kad diegiama programinė įranga yra be kenksmingo programinio kodo, neautorizuotos prieigos galimybių (angl. backdoors) ir atitinka gerosios saugaus programavimo praktikos standartus.
- 6.5.1.5 Saugos incidentų ir pažeidžiamumų valdymas: Tiekėjas, paslaugų teikimo metu pastebėjęs informacijos saugumo incidentą, duomenų nutekėjimo riziką, neautorizuotos prieigos galimybę, kenksmingą kodą ar architektūrinį pažeidžiamumą, saugumo spragą privalo nedelsiant (tačiau ne vėliau kaip per 24 valandas) apie tai informuoti Perkančiąją organizaciją. Tiekėjui griežtai draudžiama viešai atskleisti informaciją apie rastus SDMA IS saugumo trūkumus. Saugumo trūkumai turi būti išsprendžiami, panaikinami, arba, jei to padaryti neįmanoma, tokie komponentai nenaudojami.