Pirkimo sąlygų

Techninės specifikacijos

1 priedas

**REIKALAVIMAI PIRKIMO OBJEKTUI**

OpenEHR programinė įranga, jos konfigūravimas bei OpenEHR mokymai, OpenEHR panaudojimo studija Lietuvos sveikatos priežiūros įstaigose

Turinys

[1. Terminai ir santrumpa 3](#_Toc193730388)

[2. OpenEHR galimybių studijos parengimo ir Bandomojo projekto (PoC) bendrieji reikalavimai 3](#_Toc193730389)

[2.1. Projekto aprašymas ir pagrindiniai tikslai 3](#_Toc193730390)

[2.2. Projekto apimtis 4](#_Toc193730391)

[2.3. Projekto metu naudojama kalba 4](#_Toc193730392)

[2.4. Reikalavimai dokumentams ir jų derinimui 5](#_Toc193730393)

[2.5. Reikalavimai projektų valdymui 5](#_Toc193730394)

[2.6. Pokyčių valdymo reikalavimai 6](#_Toc193730395)

[2.7. Garantijos reikalavimai 6](#_Toc193730396)

[2.7.1. Incidentų valdymas 6](#_Toc193730397)

[2.8. Projekto tikslai ir rezultatai 7](#_Toc193730398)

[3. Funkciniai reikalavimai 12](#_Toc193730399)

[3.1. Sprendimas saugoti ir valdyti klinikinius duomenis pagal openEHR specifikacijas 12](#_Toc193730400)

[3.1.1. Klinikinių duomenų saugykla (CDR) 12](#_Toc193730401)

[3.1.2. FHIR pagrindu veikiantis pagrindinis pacientų registras (MPI) 12](#_Toc193730402)

[3.1.3. Duomenų integravimas 12](#_Toc193730403)

[3.1.4. Turinio kūrimo ir valdymo sprendimas 12](#_Toc193730404)

[3.2. Kiti funkciniai reikalavimai 13](#_Toc193730405)

[3.2.1. Bendrieji kiti reikalavimai 13](#_Toc193730406)

[3.2.2. Autorizacija ir praėjimo kontrolė 13](#_Toc193730407)

[3.2.3. Asmens duomenų tvarkymas. 13](#_Toc193730408)

[3.2.4. Darbo eigos valdymas ir automatizavimas. 13](#_Toc193730409)

[3.2.5. Vartotojo užduočių valdymas ir vidiniai pranešimai. 14](#_Toc193730410)

[3.2.6. Pritaikyti nefunkciniai reikalavimai 14](#_Toc193730411)

[3.2.7. Stebėsena ir atitiktis 14](#_Toc193730412)

[4. Nefunkciniai reikalavimai 14](#_Toc193730413)

[4.1. Patikimumo reikalavimai 14](#_Toc193730414)

[4.2. Saugumo reikalavimai 14](#_Toc193730415)

[4.2.1. Duomenų apsaugos ir informacijos saugumo valdymo reikalavimai 14](#_Toc193730416)

[4.2.2. Saugumą reglamentuojančių teisės aktų taikymo reikalavimai 16](#_Toc193730417)

[4.2.3. Duomenų saugumo reikalavimai teikiant paslaugas 16](#_Toc193730418)

[4.2.4. Naudotojų valdymo saugumo reikalavimai 17](#_Toc193730419)

[4.2.5. Audito reikalavimai 17](#_Toc193730420)

[4.2.6. Rizikos, grėsmių ir pažeidžiamumo valdymo reikalavimai 18](#_Toc193730421)

[4.2.7. Su nacionaliniu saugumu susiję reikalavimai 19](#_Toc193730422)

[4.2.8. Kiti saugumo reikalavimai 19](#_Toc193730423)

# Terminai ir santrumpa

Vartojami terminai ir santrumpos pateikti 1 lentelėje "Vartojami terminai ir santrumpos ".

1 lentelė. Vartojami terminai ir santrumpos

| Terminas / santrumpa | Apibūdinimas |
| --- | --- |
| API | Programų programavimo sąsaja |
| Klientas | VĮ Registrų centras arba RC |
| Kauno klinikos | Lietuvos sveikatos mokslų universiteto ligoninė Kauno klinikos |
| Šiaulių ligoninė | Respublikinė Šiaulių ligoninė, VšĮ |
| HIS | Sveikatos priežiūros institucijos informacinė sistema *(angl. healthcare information system)* |
| ESPBI IS | Lithuania's Electronic Health Services and Cooperation Infrastructure Information System (lit. *Elektroninė sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinė sistema*) |
| FHIR | Medicininių duomenų standartas |
| Sistema, Sprendimas | OpenEHR pagrindu veikianti sistema, sprendimas. |
| JSON | "JavaScript" objekto žymėjimas |
| RC | State Enterprise Centre of Registers (lit. *Registrų centras*) |
| SAM | Ministry of Health (lit. *Sveikatos apsaugos ministerija*) |
| Paslaugų teikėjas | Įmonė, teikianti programinės įrangos kūrimo paslaugas projekto įgyvendinimui. |
| XML | "eXtensible" žymėjimo kalba |

# OpenEHR galimybių studijos parengimo ir Bandomojo projekto (PoC) bendrieji reikalavimai

# Projekto aprašymas ir pagrindiniai tikslai

1. Lietuvos registrų centras iniciavo galimybių studijos ir bandomojo projekto parengimo projektą, kuriuo siekiama įvertinti OpenEHR pagrindu veikiančios sveikatos priežiūros informacinės sistemos įdiegimo galimybes Lietuvos sveikatos priežiūros paslaugų įstaigose. Projektas orientuotas į galimų sveikatos informacinės sistemos (HIS) diegimo strategijų vertinimą ir integralumo rizikų bei galimybių su centrine ESPBI sistema analizę. Tačiau nacionalinės ESPBI sistemos migravimo į OpenEHR galimybė nėra šio projekto apimtyje t.y. vertinimas apsiriboja tik HIS migracija į OpenEHR standartą.
2. Galimybių studija turi apimti tiek profesionalias konsultacijas ir vertinimą, tiek techninio sprendimo parengimą, siekiant visapusiškai įvertinti, ar OpenEHR standarto sprendimai yra tinkama alternatyva Lietuvos rinkos subjektams.

# Projekto apimtis

1. Projekte dalyvauja 2 pagrindiniai subjektai, kurie dalyvaus konkurse: Kauno klinikos ir Šiaulių ligoninė. Be to, projekte gali dalyvauti ir Registrų centro naudotojai. **Visi projekto rezultatai, komunikacija, sistemos diegimas (instaliacijos) ir kt. turėtų būti užtikrinti tiek Kauno klinikose, tiek Šiaulių ligoninėje atskirai.**
2. Paslaugų teikėjas turi išanalizuoti esamus duomenis iš Kauno klinikų ir Šiaulių ligoninės dabartinės HIS arba peržiūrėti pateiktą pirminį kodą (angl. source code), siekdamas pateikti kuo išsamesnes rekomendacijas ir įžvalgas projekto metu.
3. **Šis projektas neapima galimybių studijos vertinimo dėl centrinės sveikatos duomenų sistemos ESPBI migravimo į OpenEHR standartą, todėl šis aspektas neturėtų būti vertinamas projekto apimtyje**. Dėmesys turėtų būti skiriamas vertinimui, ar OpenEHR standartą naudojanti ligoninės informacinė sistema (HIS) gali integruotis su esama ESPBI sistema, bei galimų su šia integracija ir bendru diegimu susijusių rizikų nustatymą
4. Projektas **neapima sistemos diegimo gamybinėje (PROD)** **aplinkoje**. Paslaugų teikėjas turi sukurti informacinę sistemą TEST aplinkoje, kad būtų užtikrintas visiškas testavimas ir visų projekto tikslų įgyvendinimas. Projekto tikslas – sukurti bandomojo projekto sprendimą, galintį pademonstruoti visą funkcionalumą. Siekiant įgyvendinti nustatytus tikslus, būtina parengti sistemos konfigūracijas, atlikti duomenų perkėlimą ar įdiegti papildomas funkcijas. Paslaugų teikėjas yra atsakingas už šių užduočių įgyvendinimą ir pilnai veikiančios sistemos pateikimą TEST aplinkoje.
5. Paslaugų teikėjas privalo užtikrinti visas reikalingas licencijas visam projekto laikotarpiui.
6. Projekte dalyvaus **iki 20 naudotojų**, iš kurių 10 turi programavimo (angl. development) patirtį, o 10 – veiklos atstovai. Šis naudotojų skaičius yra bendras tiek Kauno klinikoms, tiek Šiaulių ligoninei (iš viso 20, o ne 40).
7. PoC turi būti orientuotas į kardiologijos sritį.
8. Visos projekto metu parengtos medicininės formos (suderintu formatu) turi būti perduotos Klientui projekto pabaigoje, o visa šių nuosavybė turi priklausyti Klientui.
9. Paslaugų teikėjas yra atsakingas už visų duomenų transformacijų, kurių reikėtų norint perkelti duomenis iš esamų Kliento sistemų į OpenEHR sprendimą, užtikrinimą.
10. Sprendimas turėtų būti įdiegtas į Kliento (Registrų centras) infrastruktūrą. Debesijos sprendimai negali būti pateikti.
11. Projekto terminai:
    1. Informacinė sistema turi atitikti visus funkcinius ir nefunkcinius reikalavimus, o visi projekto rezultatai (projekto tikslai, atitikties ataskaitos) turi būti parengti ne vėliau nei Paslaugų sutartyje nurodyta data.
    2. **Pasibaigus projektui, turėtų būti taikoma 6 mėnesių garantija**. Reikalavimai garantijai pateikiami kitame skyriuje.

# Projekto metu naudojama kalba

1. Projekto dokumentacija turi būti parengta tiek lietuvių, tiek anglų kalbomis. Tarpiniai dokumentai (negalutiniai) gali būti rengiami viena kalba, tačiau visi galutiniai rezultatai turi būti pateikti abiem kalbomis.
2. Projekto komunikacija gali vykti lietuvių arba anglų kalbomis.
3. Naudotojų mokymai gali vykti lietuvių arba anglų kalbomis

# Reikalavimai dokumentams ir jų derinimui

1. Visa Paslaugų teikėjo parengta projekto dokumentacija turi būti parengta vadovaujantis atitinkamos kalbos gramatikos ir formatavimo taisyklėmis, iliustruotomis diagramomis, lentelėmis, grafikais ir kitomis vaizdinėmis priemonėmis, pateikta medžiaga išdėstyta aiškiai, nuosekliai ir išsamiai.
2. Projekto dokumentacija turi būti atnaujinama atsižvelgiant į projekto etapus, veiklas ir visus patvirtintus sprendimus. Galutinėse versijose turi atsispindėti visi pakeitimai (net ir anksčiau patvirtinti dokumentai), nebent susitarta kitaip.
3. Projekto dokumentacija turi būti saugoma ir derinama Kliento Confluence aplinkoje, o projekto užduočių valdymas turi būti vykdomas Kliento Jira aplinkoje. Prieigą prie šių sistemų Klientas suteiks projekto pradžioje.
4. Paslaugų teikėjas privalo suderinti visus dokumentų šablonus su Klientu. Nors projekto metu dokumentų struktūra gali keistis, jie turėtų būti pateikiami kiekvieno dokumento rengimo etapo pradžioje, kad būtų suderinti pradiniai lūkesčiai.
5. Galutinės dokumentų versijos turi būti pateikiamos elektroniniu būdu redagavimui tinkamu formatu (pvz., .doc, .docx ar kitu sutartu formatu), įskaitant diagramas ir kitą turinį, nebent būtų susitarta kitaip. Diagramos turi būti parengtos naudojant draw.io įrankį.
6. Klientas ir kitos susijusios šalys įsipareigoja peržiūrėti dokumentus ir pateikti pastabas ne vėliau kaip per **10 darbo dienų**

# Reikalavimai projektų valdymui

1. Paslaugų teikėjas privalo tiesiogiai bendradarbiauti su Klientu, Projekto partneriais ir kitomis suinteresuotomis šalimis, dalyvaujančiomis Projekte. Tai apima nuolatinį komunikavimą ir bendradarbiavimą viso projekto įgyvendinimo laikotarpiu.
2. Paslaugų teikėjas reguliariai informuoja Klientą apie Paslaugų teikimo eigą ir Kliento prašymu, rengia bei pristato rezultatus skirtinguose paslaugų teikimo etapuose.
3. Paslaugų teikėjas turi parengti ir suderinti su Klientu Paslaugų teikimo reglamentą, kuriame turi būti detalizuoti paslaugų teikimo etapai ir jų rezultatai (pristatymų forma), numatytas etapų įgyvendinimo kalendorius su Kliento nustatytais detalizuotais terminais, aprašytos komunikacijos ir rizikų valdymo priemonės bei dokumentų derinimo tvarka.
4. Paslaugų teikėjas parengia ir pateikia Klientui mėnesines tarpines ataskaitas apie paslaugų teikimą, kurios turi apimti:
   1. Atnaujinimus apie Paslaugų sutarties vykdymo eigą.
   2. Informaciją apie per ataskaitinį mėnesį užfiksuotas rizikas ir problemas.
   3. Atnaujintus įrašus apie bet kokius suderintus pakeitimus pakeitimų registre.
5. Tarpinės paslaugų teikimo ataskaitos turi būti pateiktos Klientui per 5 darbo dienas po ataskaitinio laikotarpio pabaigos.
6. Paslaugų teikėjas privalo ir toliau tiesiogiai bendradarbiauti su Klientu, Projekto partneriais ir kitomis suinteresuotomis šalimis viso projekto metu, užtikrindamas, kad visi dalyviai būtų įtraukti ir informuoti.

# Pokyčių valdymo reikalavimai

1. Klientas pasilieka teisę (bet neprivalo) užsakyti papildomas paslaugas iš Paslaugų teikėjo pagal pasiūlyme nurodytą valandinį įkainį. Papildomų paslaugų apimtis yra iki 1000 darbo valandų.
2. Paslaugų teikėjas privalo taikyti valandinį įkainį, ne didesnį nei nurodyta pasiūlyme. Prieš pradėdamas papildomus darbus, Paslaugų teikėjas privalo pateikti detalų užduoties aprašymą, laiko sąmatą su pagrindimu ir įgyvendinimo tvarkaraštį, dėl kurių visa tai turi būti suderinta su Klientu. Klientas pasilieka teisę patvirtinti arba atmesti pakeitimo prašymą, remdamasis įvertinimu. Sąmatos parengimas turi būti atliekamas Paslaugų teikėjo sąskaita.
3. Paslaugų teikėjas turi nustatyti ir susitarti su Klientu dėl išsamios papildomų paslaugų teikimo tvarkos, įskaitant papildomų paslaugų užsakymų nustatymo, apskaičiavimo ir dokumentavimo taisykles.
4. Toliau nurodyti preliminarūs galimų papildomų paslaugų tipai:
   1. Nenumatytų sričių ar funkcionalumo pakeitimai.
   2. Papildomų integracijos sąsajų diegimas.
   3. Papildomi mokymai ar konsultacijos.
   4. Kitos su Klientu sutartos užduotys.
5. Paslaugų teikėjas privalo atsiskaityti ir į savo skaičiavimus įtraukti visus projekto dokumentus, kurie turi būti parengti ar atnaujinti, kartu su visais būtinais pakeitimais, kad būtų pasiekti pakeitimo užklausos tikslai.

# Garantijos reikalavimai

1. Paslaugų teikėjas privalo užtikrinti sprendimo garantiją, kad Klientas galėtų išbandyti sistemą.
2. Garantija netaikoma paties Kliento atliktiems pakeitimams.
3. Garantinis laikotarpis yra **6 mėnesiai** nuo galutinio pristatymo-priėmimo akto pasirašymo.
4. Paslaugų teikėjas privalo suderinti išsamią garantinės priežiūros procedūrą su Klientu iki garantinio laikotarpio pradžios.

### Incidentų valdymas

1. Kritiniai incidentai. Sistemos gedimai, kritinių funkcijų gedimai arba tokios problemos kaip saugumo pažeidimai ar duomenų sugadinimas.
2. Nekritiniai incidentai. Nedideli sutrikimai, kosmetinės klaidos arba problemos, susijusios su galimais sprendimo būdais.
3. Incidentai turi būti registruojami ir stebimi Kliento problemų valdymo programinėje įrangoje JIRA.
4. Incidentų valdymas turi būti vykdomas pagal toliau pateiktą lentelę:

| Veidas | Taisyklė |
| --- | --- |
| Taikomas laikotarpis | 6 mėnesiai po galutinio pristatymo-priėmimo akto pasirašymo |
| Atitinkamos darbo valandos | Garantinis aptarnavimas turi veikti nuo 08:00 iki 18:00 (Lietuvos laiko juosta), atsižvelgiant į kliento darbo dienas |
| Kritinio reagavimo į incidentą laikas | Turi būti atsakyta per 8 darbo valandas |
| Reagavimo į nekritinį incidentą laikas | Turi būti atsakyta per 16 darbo valandų |
| Kritinio incidento sprendimo laikas | Turi būti išspręsta per 2 darbo dienas |
| Nekritinio incidento sprendimo laikas | Turi būti išspręsta per 10 darbo dienų |

# Projekto tikslai ir rezultatai

1. Pagrindinis projekto tikslas – įvertinti, ar OpenEHR standartu pagrįsti HIS sprendimai yra perspektyvi alternatyva ir ar juos būtų galima apsvarstyti ateityje diegiant HIS. Projekto tikslai išdėstyti toliau pateiktoje lentelėje, išsamiai apibūdinant pagrindinius klausimus, kuriuos siekiama išspręsti šiuo projektu, ir numatomus rezultatus. Tikslų rezultatai skirstomi į 3 kategorijas:
   1. **Reikalavimų atitikties rezultatai**. Reikalavimų atitikties rezultatai siekia užtikrinti, kad pateiktas sprendimas atitiktų specifikacijoje nurodytus reikalavimus.
   2. **Galimybių studijos rezultatai**. Šiuose rezultatuose daugiausia dėmesio skiriama konsultacijų rezultatams, įskaitant dokumentus, o ne bandomosios techninės sistemos įgyvendinimui.
   3. **Bandomojo projekto informacinės sistemos rezultatai**. Šie rezultatai orientuoti į TEST aplinkos informacinės sistemos diegimą, siekiant techniškai patvirtinti konkrečius aspektus ir išspręsti pagrindinius projekto tiksluose išdėstytus klausimus.

| Projekto tikslas / spręstinas klausimas | Laukiami rezultatai |
| --- | --- |
| **Analizės, sistemos konfigūravimo ir mokymų etapas** | |
| **Projekto inicijavimo dokumentacija** | **Reikalavimų atitikties rezultatai:**   * Parengta projekto inicijavimo dokumentacija, detalizuojanti:   + Projekto tikslai, uždaviniai ir prioritetai,   + rezultatų aprašymas (etapų apimtis ir rezultatai),   + suinteresuotosios šalys (suinteresuotosios šalys)   + projekto komanda ir atsakomybė (sprendimų priėmimo proceso organizacinės struktūros detalizavimas)   + darbo grafikas (detaliai nurodant orientacines datas ir buferio laiką)   + rizika ir jos valdymo metodai,   + komunikacijos principai,   + tarpinių ir rezultatų priėmimo kriterijai,   + pakeitimų valdymo procedūros. |
| **Analizės ataskaita**  Tikslas – užtikrinti, kad pateikta priemonė atitiktų visus techninėje specifikacijoje nurodytus reikalavimus. | **Reikalavimų atitikties rezultatai:**   * Paslaugų teikėjas yra atsakingas už reikalavimų analizės ataskaitos parengimą, kurioje turi būti detaliai nurodyta, kaip kiekvienas reikalavimas bus įgyvendintas. Ataskaitoje turi būti pažymėta, ar reikalavimas bus įgyvendintas naudojant standartinę funkcionalumą, ar reikės atlikti pakeitimus. Jei reikia, paslaugų teikėjas turi inicijuoti susitikimą su Užsakovu, siekiant suderinti reikalavimų viziją. |
| **Testavimo scenarijai**  Tikslas – parengti naudotojų priėmimo testavimo (UAT) scenarijus. | **Reikalavimų atitikties rezultatai:**   * Paslaugų teikėjas parengs testavimo scenarijus, skirtus pateiktų reikalavimų patikrinimui. Užsakovas peržiūrės šiuos scenarijus ir, jei reikės, galės pateikti papildomus testavimo scenarijus. |
| **OpenEHR kompetencijos**  Kokias kompetencijas organizacija turėtų turėti, kad galėtų naudoti OpenEHR pagrįstą HIS programinę įrangą? | **Galimybių studijos rezultatai:**   * Nustatyti, kurie darbuotojai turėtų gauti specializuotus mokymus apie OpenEHR ir kokių kompetencijų turėtų turėti organizacija. Įvertinti, kiek mokymų reikėtų organizacijai, kad ji galėtų pilnai naudotis OpenEHR pagrindu veikiančia HIS sistema. Taip pat įvertinti esamą organizacijos brandos lygį ir pateikti rekomendacijas dėl reikalingų kompetencijų. * Šio galimybių studijos ir PoC projekto metu apmokyti iki **30 pagrindinių naudotojų** apie OpenEHR. Naudotojai turi gebėti dirbti su programine įranga TEST aplinkoje ir įvertinti jos galimybes. Kiekvienam naudotojui numatoma iki 20 mokymų valandų. Mokymai gali būti organizuojami grupėmis iki 5 dalyvių ir vykdomi nuotoliniu būdu. |
| **Duomenų migravimas**  Ar būtų įmanoma perkelti esamus HIS duomenis į OpenEHR standarto sprendimą ir kokio masto duomenų transformacijos tam būtų reikalingos? | **Galimybių studijos rezultatai**:   * Įvardinti pagrindines duomenų kategorijas, kurios gali kelti daugiausiai iššūkių duomenų perkėlimo iš esamų Kauno klinikų ir Šiaulių ligoninės informacinių sistemų metu, pavyzdžiui, kurioms duomenų kategorijoms reikėtų daugiausiai duomenų transformacijų. * Parengti galimą (aukštesnio lygmens) duomenų migracijos strategiją, atsižvelgiant į skirtingus metodus, tokius kaip „big-bang“ arba etapinis diegimas. * Nustatyti pagrindines rizikas ir išteklių poreikius, reikalingus sėkmingai duomenų migracijai, bei pateikti galimą įgyvendinimo grafiką.   **Bandomojo projekto rezultatai**:   * Turi būti įgyvendintas bandomasis klinikinių duomenų saugyklos, pagrįstos OpenEHR standartu, diegimas ir testavimas. Testinėje aplinkoje turi būti užtikrintas dalies esamos sistemos demografinių duomenų perkėlimas į saugyklą, numatant pradinį iki 10 000 pacientų demografinių įrašų perkėlimą. * Turi būti atliktas riboto masto bendrųjų klinikinių duomenų importas į klinikinių duomenų saugyklą, pagrįstą OpenEHR standartu. Tai apima pagrindinių bendrųjų klinikinių duomenų, tokių kaip ūgis, svoris, būklė, kraujospūdis ir kt., perkėlimą, kartu vertinant jų pritaikomumą OpenEHR standartui. Planuojama, kad bus perkelta apie 20 parametrų. * Turi būti atliktas riboto masto specializuotų klinikinių duomenų importas į klinikinių duomenų saugyklą, pagrįstą OpenEHR standartu. Tai apima specifinių paciento klinikinių duomenų, pavyzdžiui, kardiologinių duomenų pagal EuroHeart duomenų rinkinį, integravimą ir perkėlimą, siekiant įvertinti jų panaudojimo galimybes ir pritaikymą OpenEHR standartui. |
| **Duomenų integravimas**  Ar yra galimybė sukurti duomenų integracijas su vidinėmis ir išorinėmis sistemomis, ypač tais atvejais, kai yra reikalaujama naudoti nacionaliniu mastu taikomus FHIR pagrindu sukurtus standartus? | **Galimybių studijos rezultatai**:   * Nustatyti duomenų integravimo principus ir įvertinti kiekvieną esamą duomenų integraciją Kauno klinikose ir Šiaulių ligoninėje, pateikiant aukšto lygio jos sudėtingumo vertinimą. * Pateikti išsamų duomenų integracijos į centrinę ESPBI sistemą metodą, aiškiai apibrėžiant reikalingas duomenų transformacijas, galimas rizikas ir priemones, kurios padėtų užtikrinti sėkmingą integracijos įgyvendinimą. Nors nebūtina analizuoti visų duomenų, svarbu identifikuoti ir įvardyti daugumą galimų su šia integracija susijusių rizikų.   **Bandomojo projekto rezultatai**:   * "OpenEHR" pagrįsta platforma ir duomenų saugykla turi būti integruotos su tarptautiniais medicinos terminologijos standartais. Tikslas yra išbandyti ir integruoti naujai įdiegtą sistemą su tarptautiniais terminologijos klasifikatoriais (pvz., LOINC, SNOMED, ICD-10, OMOP). Duomenų šaltiniai, skirti šių klasifikatorių duomenims rinkti, analizės etape turėtų būti suderinti. * Esamos Kauno klinikų ir Šiaulių klinikų HIS sistemos turi REST technologija pagrįstą API. OpenEHR sprendimas turi gebėti per šį API gauti duomenis iš esamų sistemų, apsiribojant tik demografiniais duomenimis. |
| **Medicininių formų kūrimas**  Kaip sunku sukurti naujas medicinines formas, pagrįstas OpenEHR standartu? | **Bandomojo projekto rezultatai**:   * Medicininių formų kūrimas turi būti vykdomas naudojant OpenEHR klinikinių duomenų standartą ir jį palaikančią low-code/no-code platformą. Projektas turi apimti medicininių formų kūrimo proceso ir technologijos suprojektavimą ir testavimą pasirinktoje bandomojoje kardiologijos srityje. Paslaugų teikėjas, bendradarbiaudamas su Užsakovu, turi parengti iki 5 medicininių formų pagal Užsakovo pateiktus duomenis. Be to, Užsakovas projekto metu turi turėti galimybę savarankiškai sukurti iki 25 papildomų medicininių formų. |
| **Naudotojų priėmimo testavimo (UAT) ir galimybių studijos rezultatai** | |
| **Naudotojų priėmimo testavimo (UAT) ataskaita**  Tikslas – užtikrinti, kad sprendimas būtų ištestuotas pagal parengtus funkcinius ir nefunkcinius reikalavimus. | **Reikalavimų atitikties rezultatai:**   * Užsakovas testuos visus reikalavimus pagal apibrėžtus testavimo scenarijus. Paslaugų teikėjas privalo aktyviai dalyvauti testavimo etape – dalyvauti visose su tuo susijusiose susitikimuose ir teikti konsultacijas, kaip turi būti testuojamas kiekvienas reikalavimas. Nustačius klaidų, jos bus dokumentuojamos Užsakovo ir privalės būti pašalintos Paslaugų teikėjo. Pasibaigus testavimo etapui, Paslaugų teikėjas parengs UAT ataskaitą, kurioje nurodys, kokie scenarijai buvo testuoti, kokios klaidos identifikuotos ir koks yra jų statusas. |
| **Duomenų analizė**  Kokios galimybės užtikrinti duomenų analizę naudojant OpenEHR standartą? | **Galimybių studijos rezultatai:**   * Apibrėžti duomenų analizės galimybes, grindžiamas OpenEHR standartu, pateikti įžvalgas apie privalumus ir trūkumus, palyginti su šiuo metu Kauno klinikose ir Šiaulių ligoninėje taikomais metodais, bei nustatyti galimą naudą organizacijoms, jei būtų naudojamas OpenEHR standartas. Taip pat turi būti apibrėžti reikalingi įrankiai ir kompetencijos, būtinos duomenų analitikai užtikrinti. Reikia suformuluoti ir įvertinti 2–3 duomenų analizės scenarijus, analizuojant, kaip tokia analizė galėtų būti atliekama naudojant OpenEHR standartą, palyginti su dabartine sistema, ir pateikti įžvalgas.   **Bandomojo projekto rezultatai**:   * Atlikti duomenų analizę, pagrįstą OpenEHR klinikiniais duomenimis, pateikiant įžvalgas apie šio standarto panaudojimą, privalumus ir apribojimus. Suteikti duomenų analizės įrankius ir parengti iki 5 duomenų ataskaitų (prietaisų skydelių) pagal Užsakovo klinikinių duomenų saugyklą, taip pat užtikrinti, kad Užsakovas galėtų savarankiškai sukurti iki 10 papildomų švieslenčių. |
| **Diegimo strategija**  Kokia būtų tinkamiausia diegimo strategija diegiant naują OpenEHR pagrindu veikiančią HIS sistemą? Jei nebūtų pasirinkta „big-bang“ strategija, kaip veiktų nauja ir esama sistema lygiagrečiai, ir kokios su tuo susijusios rizikos galėtų būti identifikuotos? | **Galimybių studijos rezultatai:**   * Įvertinti bendrą organizacijos pasirengimą pereiti prie OpenEHR standarto. * Nustatyti ir įvertinti galimas OpenEHR alternatyvas, pavyzdžiui, FHIR ar kitus standartus, nurodant jų pranašumus ir trūkumus. * Išanalizuoti kiekvieną susijusią informacinę sistemą Kauno klinikose ir Šiaulių ligoninėje, įvertinant jų technines galimybes diegti OpenEHR bei nustatant diegimo scenarijus – ar reikalinga visiškai nauja aplikacija, ar pakanka pakeisti tik duomenų saugyklą, išlaikant esamas sąsajas ir funkcionalumą. * Apibrėžti OpenEHR programinės įrangos rinką ir įvertinti jos plėtros perspektyvas. Pateikti iki 3 ligoninių, kurios jau yra įdiegusios OpenEHR, suorganizuoti nuotolinius susitikimus su jų atstovais, kad būtų pasidalinta praktine patirtimi. * Identifikuoti atvirojo kodo sprendimus bei pagrindinius OpenEHR sprendimų tiekėjus rinkoje. * Įvertinti OpenEHR plėtros planą (angl. roadmap) ir planuojamus standartų ar technologinius pokyčius. * Parengti preliminarų OpenEHR diegimo planą tiek Kauno klinikoms, tiek Šiaulių ligoninei, įskaitant projekto etapų grafiką bei preliminarią biudžeto sąmatą. * Pasiūlyti ateities architektūrinį sprendimą Kauno klinikoms ir Šiaulių ligoninei. Jei projektas būtų įgyvendinamas etapais, turi būti numatyta ir laikinoji (pereinamoji) architektūra. Architektūrinis sprendimas turi apimti tiek funkcinius, tiek duomenų komponentus. * Įvertinti papildomus aspektus, tokius kaip debesijos (angl. cloud) ar vietinio (angl. on-premise) diegimo galimybės, saugumo rizikas bei kitus esminiai projekto įgyvendinimo aspektus. |

# Funkciniai reikalavimai

# Sprendimas saugoti ir valdyti klinikinius duomenis pagal openEHR specifikacijas

### Klinikinių duomenų saugykla (CDR)

1. Sprendimas turi užtikrinti klinikinių duomenų ir dokumentų saugojimą. Jis turi palaikyti saugų duomenų įrašymą, atnaujinimą, paiešką, versijų valdymą ir prieigos kontrolę.
2. Teikiama klinikinių duomenų saugykla (CDR) turi palaikyti ir aptarnauti šias, bet neapsiribojant, funkcijas:
   1. openEHR EHR API
   2. openEHR Query API
   3. openEHR Definition API
   4. Audito ir stebėsenos funkcionalumas
   5. Masinio duomenų įrašymo ir užklausų galimybės, kurios nesukelia sisteminių užstrigimų ar laiko limitų viršijimo. Turi būti palaikomi keli duomenų formatai (pvz., XML, JSON)
   6. Diegimas ir konfigūravimas organizacijos infrastruktūroje (on-premises).
3. Nors duomenų bazių sistemos pasirinkimui nėra taikomi apribojimai, svarbu atkreipti dėmesį, kad bandomojo diegimo vietoje aplikacijos ir paslaugos yra talpinamos OpenShift platformoje. Todėl bet kuri pasirinkta ar naudojama duomenų bazių sistema turi užtikrinti OpenEHR programinės įrangos veikimą pagal keliamus našumo reikalavimus ir būti efektyviai veikianti kaip vietinis (on-premise) sprendimas.

### FHIR pagrindu veikiantis pagrindinis pacientų registras (MPI)

1. Turi būti palaikomas pagrindinis pacientų registras (MPI), skirtas demografinių duomenų valdymui.
2. Nors MPI yra išorinė paslauga OpenEHR klinikinių duomenų saugyklai (CDR), būtina užtikrinti, kad CDR būtų kuriami teisingi EHR įrašai ir jie būtų tinkamai susieti su atitinkamais paciento duomenimis.
3. Tais atvejais, kai paciento identifikatorius neegzistuoja, CDR vis tiek turi turėti galimybę sukurti EHR įrašą pacientui ir užtikrinti, kad kiekvienas sukurtas EHR būtų unikalus ir susietas su vienu paciento identifikatoriumi.

### Duomenų integravimas

1. Papildomai, OpenEHR pagrindu veikiantis sprendimas turi turėti galimybę valdyti terminologijos duomenis, įskaitant, bet neapsiribojant SNOMED CT, LOINC, TLK-10 (ICD-10) ir kitomis aktualiomis klasifikacijomis.

### Turinio kūrimo ir valdymo sprendimas

1. Pateiktas sprendimas turi palaikyti openEHR artefaktų – įskaitant archetipus, šablonus ir kt. – kūrimą, modifikavimą, versijų valdymą, vertimą į lietuvių kalbą ir bendrą valdymą.
2. Sprendimas turi apimti low-code/no-code tipo įrankius formoms kurti pagal openEHR šablonus. Šie įrankiai turi užtikrinti struktūrizuotą duomenų suvedimą naudojant interaktyvius komponentus, tokius kaip pasirinkimo mygtukai (radio buttons), žymimieji langeliai (checkboxes) ir kiti naudotojo sąsajos (UI) elementai, kartu išlaikant atitiktį openEHR apribojimams.
3. Sprendime turi būti įtraukti specializuoti įrankiai ir SDK, skirti openEHR artefaktų modeliavimui, įskaitant archetipų ir šablonų kūrimą, redagavimą bei versijavimą. Šie įrankiai turi būti atskiri nuo formų kūrimo įrankių, siekiant užtikrinti lankstumą diegimo ir integravimo procesuose.
4. Versijų valdymas. Sprendimas turi turėti patikimus versijų valdymo mechanizmus, leidžiančius sekti pakeitimus ir atnaujinimus.
5. Vertimas. Sprendimas turi užtikrinti artefaktų vertimo į lietuvių kalbą galimybę.
6. Valdymas. Sprendimas turi užtikrinti efektyvų openEHR artefaktų, tokių kaip archetipai, šablonai ir kt., valdymą:
   1. Artefaktų struktūrizuotą ir prieinamą saugojimą bei klasifikavimą.
   2. Artefaktų grupavimą pagal naudojimo atvejį, klinikinę sritį ar projektą.
   3. Atnaujinimo, pasenusių artefaktų nutraukimo ar archyvavimo procesų palaikymą.
   4. Atitikties klinikiniams ir techniniams standartams užtikrinimą viso gyvavimo ciklo metu.
   5. Bendradarbiavimo galimybes, leidžiančias keliems naudotojams dirbti su artefaktais taikant prieigos kontrolę.
   6. Vartotojų vaidmenų ir teisių sistemą, reglamentuojančią kūrimą, redagavimą ar pakeitimų tvirtinimą.
   7. Pakeitimų stebėjimo įrankius, įskaitant detalius žurnalus apie tai, kas, kada ir ką keitė.
   8. Artefaktų versijų atsekamumo palaikymą.
   9. Paieškos funkcionalumą, leidžiantį naudotojams lengvai rasti reikiamus artefaktus pagal metaduomenis ar klinikinį kontekstą.
7. Formų modeliavimas. Sprendimas turi leisti kurti formas, skirtas archetipams generuoti.

# Kiti funkciniai reikalavimai

### Bendrieji kiti reikalavimai

1. Be pagrindinės openEHR pagrindu veikiančios programinės įrangos pateikimo, sėkmingam bandomajam diegimui reikės ir papildomų palaikymo paslaugų. Šios paslaugos apims openEHR platformos diegimą, instaliavimą ir konfigūravimą bandomojo diegimo aplinkoje. Tiekėjas taip pat turės teikti esminius atnaujinimus ir pagrindinius modifikavimus, reikalingus pilotinės versijos veikimui.

### Autorizacija ir praėjimo kontrolė

1. Turi būti pateiktas prieigos valdymo sprendimas, paremtas rolėmis grįstu prieigos valdymu (RBAC), siekiant užtikrinti duomenų saugumą ir privatumą. Kadangi tai tik koncepcijos įrodymo (PoC) etapas, integracija su pilotinės ligoninės esama tapatybės ir prieigos valdymo sistema nėra būtina. Vietoj to, openEHR sprendime turi būti įdiegta savarankiška prieigos valdymo sistema, kuri savarankiškai demonstruotų reikiamas saugumo ir privatumo funkcijas.

### Asmens duomenų tvarkymas.

1. Vadovaujantis BDAR (Bendruoju duomenų apsaugos reglamentu), pacientai turi teisę reikalauti savo asmens duomenų blokavimo ir susipažinimo su jais.

### Darbo eigos valdymas ir automatizavimas.

1. Sprendimas turi leisti valdyti darbo srautus (angl. workflows), įskaitant galimybę priskirti konkrečius darbo srautus medicininėms formoms. Sprendime turi būti užtikrinta low-code/no-code tipo naudotojo sąsaja.

### Vartotojo užduočių valdymas ir vidiniai pranešimai.

1. Sprendimas turi turėti užduočių valdymo funkcionalumą, leidžiantį naudotojams peržiūrėti jiems priskirtas užduotis, jas kategorizuoti ir stebėti jų vykdymo eigą.
2. Be to, sprendime turi būti įdiegta pranešimų sistema, kuri siųstų priminimus naudotojams, neatsakiusiems į užduotis per nustatytą laiką, taip užtikrinant savalaikį jų įvykdymą ir atsakomybę.

### Pritaikyti nefunkciniai reikalavimai

1. Nefunkciniai reikalavimai turi būti pritaikyti pagal pilotinio projekto apimtį, daugiausia dėmesio skiriant praktiniam įgyvendinamumui. Duomenų įvedimo lietuvių kalba palaikymui turi būti naudojama Unicode UTF-8 koduotė. Nors ilgalaikėje perspektyvoje yra numatyti tikslai, tokie kaip paslaugomis grįstos architektūros (SOA) laikymasis ir sistemos plečiamumas, pilotinio projekto metu turi būti pasitelkiami esami komponentai ir maksimaliai sumažintas specifinis programavimas. Toks požiūris leis patikrinti pagrindines funkcijas ir surinkti įžvalgas tolimesniam vertinimui.
2. Pilotinis projektas turi pateikti supaprastintą sprendimą, skirtą įvertinti OpenEHR sprendimo tinkamumą ir veikimo efektyvumą, sutelkiant dėmesį į esmines funkcijas, tokias kaip duomenų saugojimas ir užklausų vykdymas. Turi būti panaudotos AQL galimybės, tokios kaip „EXISTS“, leidžiančios atlikti svarbiausias duomenų paieškas ir analizes. Paprasti naudojimo rodikliai, pavyzdžiui, dažniausiai naudojamų archetipų stebėjimas, turi padėti optimizuoti sprendimą be papildomo sudėtingumo.

### Stebėsena ir atitiktis

1. Turi būti sukurti priežiūros mechanizmai, skirti vertinti darbo srautų efektyvumą, užduočių įvykdymo rodiklius ir priminimų laikymosi lygį.

# Nefunkciniai reikalavimai

# Patikimumo reikalavimai

1. Sprendime turi būti nustatyti mechanizmai, užtikrinantys, kad sistemos gedimo atveju duomenys nebūtų prarasti.
2. Sprendimas turi įgyvendinti veiklos tęstinumo procesą, leidžiantį sistemai tęsti veiklą gedimo atveju, veikti reikiamu pajėgumu ir per nustatytą laikotarpį apdoroti susikaupusį darbų kiekį.
3. Sprendimas turi gebėti atkurti nepakitusius duomenis iš atsarginių kopijų iki tinkamo lygmens, atnaujinti apdorojimo procesus neprarandant ir nedubliuojant gaunamų ar siunčiamų pranešimų.
4. Sprendimas turi gebėti aptikti pranešimų, perduodamų į jį ar iš jo, praradimą ar dubliavimą ir turėti mechanizmus šiems netikslumams ištaisyti.
5. Sprendimas turi būti nuoseklus – užtikrinti, kad ta pati užklausa dėl gaunamo pranešimo visada duotų tą patį rezultatą, nepriklausomai nuo to, kiek kartų ji vykdoma.
6. Sprendimas turi užtikrinti atsarginių duomenų kopijų sudarymą, jų atkūrimą ir sisteminį veiklos atstatymą.

# Saugumo reikalavimai

### Duomenų apsaugos ir informacijos saugumo valdymo reikalavimai

1. Duomenų saugumas turi būti užtikrintas vadovaujantis Sistemos duomenų saugumo nuostatomis, o asmens duomenų apsauga – remiantis Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymu ir 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
2. Teikėjas privalo užtikrinti atitiktį Lietuvos Respublikos informacinių išteklių valdymo įstatymui, Lietuvos Respublikos kibernetinio saugumo įstatymui, , Saugumo dokumentų turinio gairių aprašui T-29, kibernetinio saugumo reikalavimų aprašui patvirtintam Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir kitiems susijusiems teisės aktams, įskaitant Vyriausybės nutarimus dėl elektroninės informacijos saugumo.
3. Užbaigus Sistemos pirkimo veiklas, Sistemoje saugomi duomenys turi būti apsaugoti nuo neteisėtos prieigos, naudojimo, pakeitimo, atskleidimo, sunaikinimo ar praradimo.
4. Asmens duomenys, perduodami viešaisiais duomenų perdavimo kanalais, turi būti šifruojami.
5. Draudžiama viešai skelbti asmens kodus.
6. Sistema turi užtikrinti tinkamą avarinių situacijų, kylančių dėl neteisingų naudotojų veiksmų ar kitų informacinės sistemos problemų, valdymą. Apie tokią situaciją turi būti informuojami naudotojai ar sistemos, taip pat pateikiami galimi tolimesni veiksmai.
7. Turi būti įdiegtos priemonės, leidžiančios sekti naudotojų veiksmus per Sistemos sąsają, o audituotinų duomenų specifiką reikia suderinti su Užsakovu analizės etape.
8. Siekiant išvengti perteklinio audito informacijos kaupimo, audito įrašų fiksavimo momentai turi būti nustatyti išsamios analizės metu bendradarbiaujant su Užsakovu.
9. Sistemos gedimo atveju naudotojams turi būti pateikiami atitinkami pranešimai.
10. Rengiant Sistemos modifikacijas, Teikėjas privalo suderinti su Užsakovu dėl konkrečių funkcijų apsaugos nuo įvairių grėsmių:
    1. Turi būti pašalintos saugumo spragos, tokios kaip neautentifikuota prieiga ir programinės įrangos pažeidžiamumai;
    2. Užkirstas kelias neteisėtam naudotojų seansų perėmimui;
    3. Užtikrintas duomenų perėmimo ar įterpimo prevencijos mechanizmas;
    4. Užkirstas kelias kenksmingo kodo įterpimui, įskaitant injekcijos atakas ir kelių svetainių scenarijų (XSS) atvejus;
    5. Užtikrintas apsisaugojimas nuo kitų saugumo pažeidimų, nurodytų atvirojo tinklo programos saugumo pirkimo (SSP) dokumentuose ir Open Web Application Security Project (OWASP) gairėse (www.owasp.org).
11. Programinės įrangos kūrimo metu turi būti laikomasi saugaus programavimo praktikų ir standartų, tokių kaip OWASP, užtikrinant apsaugą nuo neteisėtos prieigos prie duomenų ir kitų saugumo pažeidimų.
12. Saugumo patikros (grėsmių modeliavimas, programinio kodo peržiūros ir kt.), numatytos saugaus programavimo standartuose ir gerojoje praktikoje, turi būti atliekamos kiekviename programinės įrangos kūrimo etape vadovaujantis Elektroninių paslaugų plėtros metodika, patvirtinta Lietuvos Respublikos susisiekimo ministro 2015 m. spalio 7 d. įsakymu. Nustatytus atsparumo įsibrovimui testavimus turi atlikti nepriklausomas paslaugų teikėjas. Saugumo patikros turi būti pagrįstos visuotinai pripažintomis metodikomis: OWASP ASVS, OWASP Testing Guide, PTES, OSSTMM, ISSAF, SANS, NIST SP 800-30 arba lygiavertėmis.
13. Sistemos teikiamų web paslaugų saugumas turi atitikti WS-S (Web Services Security) standartus.
14. Teikėjas privalo naudoti Užsakovo pateiktus sertifikatus žiniatinklio paslaugų apsaugai.
15. Teikėjas privalo nedelsdamas informuoti apie informacijos saugumo incidentus, pastebėtus Užsakovo IT infrastruktūroje vykdant sutartį, neveikiančias ar netinkamai veikiančias saugumo priemones, informacijos saugumo reikalavimų nesilaikymą, galimus nusikalstamos veiklos požymius, sistemos pažeidžiamumus ir kitus svarbius saugumo įvykius. Suderinus su Užsakovu, turi būti imamasi atitinkamų priemonių nustatyti incidento priežastį ir užkirsti kelią susijusiai rizikai.
16. Vykdydamas paslaugas pagal Sutartyje numatytus reikalavimus, Teikėjas privalo įgyvendinti tinkamas organizacines ir technines priemones, skirtas apsaugoti informaciją nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo bei bet kokio kito neteisėto tvarkymo.

### Saugumą reglamentuojančių teisės aktų taikymo reikalavimai

1. Pagrindiniai saugumo (tiek programinės įrangos, tiek duomenų) teisės aktai, kurių turi būti laikomasi kuriant Sistemą, yra šie:
   1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas – BDAR), saugumo valdymo standartas LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių taikymo taisyklės“ ir ISO/IEC 27701:2019 „Saugumo metodai – ISO/IEC 27001 ir ISO/IEC 27002 priedas dėl privatumo valdymo – reikalavimai ir gairės“;
   2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
   3. Lietuvos Respublikos kibernetinio saugumo įstatymas;
   4. Kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;
   5. Informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;
   6. Duomenų teikimo formatų ir standartų rekomendacijos, patvirtintos Lietuvos Respublikos susisiekimo ministerijos Informacinės visuomenės plėtros komiteto direktoriaus 2013 m. kovo 25 d. įsakymu Nr. T-36 „Dėl duomenų teikimo formatų ir standartų rekomendacijų patvirtinimo“.
2. Teikėjas privalės atlikti Sistemos atitikties vertinimą pagal aukščiau nurodytus teisės aktus ir pateikti šio vertinimo ataskaitą, kuri turi būti suderinta su RC. Atitikties vertinimas turi būti atliktas ne vėliau kaip iki bandomosios Sistemos eksploatacijos pradžios.

### Duomenų saugumo reikalavimai teikiant paslaugas

1. Informacinių išteklių kūrimo ir priežiūros saugumas (saugus programavimas ir kt.) turi būti užtikrintas vadovaujantis Lietuvos standartais LST EN ISO/IEC 27001 ir LST EN ISO/IEC 27002.
2. Taip pat turi būti laikomasi saugumo reikalavimų, nustatytų Kliento valdomų registrų ir informacinių sistemų duomenų saugumo nuostatuose, saugumo politiką įgyvendinančiuose dokumentuose, kibernetinio ir elektroninės informacijos saugos incidentų valdymo tvarkos apraše bei kituose teisės aktuose (taip pat ir tuo atveju, kai šie reikalavimai pasikeičia arba atsiranda po viešojo pirkimo–pardavimo sutarties pasirašymo).
3. Duomenų saugumas turi būti užtikrinamas:
   1. Užtikrinant duomenų vientisumą, prieinamumą ir konfidencialumą.
   2. Registruojant sistemos naudotojų atliekamus veiksmus su duomenimis, įskaitant paiešką ir peržiūrą (tam tikrai sistemos naudotojų grupei turi būti reikalaujama nurodyti veiksmų atlikimo pagrindą ir/ar teisinį pagrindą).
   3. Sukuriant priemones, leidžiančias Sistemos administratoriui tikrinti naudotojų veiksmus.
   4. Sistemos naudotojai, dirbantys su tam tikrais komponentais, turi būti suskirstyti į grupes pagal duomenų tvarkymo pobūdį, kai kuriems jų suteikiant specialias teises (roles) atlikti tam tikrus veiksmus. Sistemos naudotojų grupių ir rolių aprašymai turi būti parengti analizės etape.
   5. Sistemoje saugoma informacija negali būti ištrinama jokiu kitu būdu ir jokiomis aplinkybėmis, išskyrus tas, kurios buvo nustatytos analizės metu.
   6. Teikėjas turi suderinti su Užsakovu failų formatus, kurie leidžiami įkelti į Sistemą (pvz., negali būti leidžiama prisegti potencialiai nesaugius failus, kurie gali būti paleidžiami automatiškai, pvz., savarankiškai pasileidžiančius failus (angl. self-executive files)).

### Naudotojų valdymo saugumo reikalavimai

1. Sistema turi automatiškai nutraukti naudotojo darbo sesiją po nustatyto neaktyvumo laikotarpio, kuris apibrėžiamas parametruose, ir pateikti naudotojui pranešimą su atsijungimo priežastimi. Sistemos administratorius turi turėti galimybę keisti šio neaktyvumo laikotarpio reikšmę.
2. Sistemos naudotojų vardai, slaptažodžiai ir kiti asmens duomenys, kuriems taikoma duomenų apsauga, turi būti saugomi užtikrinant tinkamą prieigos kontrolę ir informacijos šifravimą.
3. Sistema turi turėti galimybę naudotojus suskirstyti į atskiras roles su skirtingomis prieigos teisėmis prie konkrečių sistemos funkcijų. Naudotojas gali matyti ir redaguoti tik tą informaciją bei naudotis tik tomis funkcijomis, kurios jam yra priskirtos pagal jo prieigos teises.
4. Pagal naudotojo pateiktas užklausas turi būti atvaizduojami tik tie duomenys, kuriuos jis turi teisę matyti.

### Audito reikalavimai

1. Toliau pateikiami audito reikalavimai yra suskirstyti į dvi kategorijas: techninio lygmens auditą, orientuotą į duomenų ir sistemos technines operacijas, ir veiklos lygmens auditą, orientuotą į veiklos procesus ir veiklos logikos žingsnius. Šios kategorijos turi būti aiškiai atskirtos ir suderintos analizės bei projektavimo etapuose.
2. Visi sistemos komponentų (naudotojų veiksmų) naudojimo atvejai ir jų vykdomos operacijos turi būti audituojami.
3. Techninio lygmens audito reikalavimai apima sistemos lygmens įvykių, duomenų keitimo veiksmų, konfigūracijos pakeitimų ir su saugumu susijusių operacijų auditavimą. Techninis auditas užtikrina galimybę atkurti duomenų apdorojimo istoriją, tirti saugumo incidentus, identifikuoti neteisėtus veiksmus ir analizuoti sistemos problemas.
   1. Bendroji techninio audito apimtis:
      1. Naudotojų autentifikavimo įvykiai (pvz., prisijungimas, atsijungimas);
      2. Sistemos parametrų ar nustatymų pakeitimai;
      3. Su duomenimis susijusios veiklos duomenų bazėje: įrašymas, atnaujinimas, trynimas, peržiūra;
      4. Atliktos paieškos, įskaitant naudotas paieškos frazes;
      5. Integracijos įvykiai su vidinėmis ir išorinėmis sistemomis (duomenų siuntimas / gavimas, šaltinio / paskirties sistemos).
   2. Techninio lygmens audito duomenų saugojimo reikalavimai:
      1. Kas atliko veiksmą (naudotojas);
      2. Kada veiksmas buvo atliktas (data ir laikas);
      3. Kokie duomenų objektai buvo peržiūrėti, įterpti, atnaujinti ar ištrinti;
      4. Kokios paieškos frazės buvo naudotos;
      5. Naudotojo IP adresas;
      6. Kita papildoma techninė informacija, nustatyta analizės ir projektavimo etapuose.
4. Veiklos lygmens audito reikalavimai orientuoti į žingsnių, sprendimų ir veiksmų fiksavimą veiklos perspektyvoje. Veiklos veiksmų auditas padeda sekti veiklos procesų eigą, suprasti, kokie procesai buvo vykdomi, kas dalyvavo ir kaip keitėsi būsenos ar konfigūracijos logikos kontekste.
   1. Bendroji veiklos audito apimtis:
      1. Veiksmai, atlikti veiklos procesų metu (pvz., paciento registracijos žingsniai IPR, vizitų planavimas / atšaukimas);
      2. Būsenų pokyčiai procesuose (pvz., statuso pasikeitimas, atsakomybių perdavimas, veiklos parametrų pakeitimai);
      3. Sprendimų priėmimo žingsnių dokumentavimas veiklos procesuose.
   2. Veiklos lygmens audito duomenų saugojimo reikalavimai:
      1. Koks naudotojas ar rolė atliko konkrečius veiksmus;
      2. Atitinkamas veiklos kontekstas (pvz., paciento ID, vizito ID ar kiti srities identifikatoriai);
      3. Veiklos proceso įvykių data ir laikas;
      4. Pokyčiai objektuose ar darbo srautuose;
      5. Kita veiklos informacija, nustatyta analizės ir projektavimo etapuose.

### Rizikos, grėsmių ir pažeidžiamumo valdymo reikalavimai

1. Sistema turi apimti rizikų, grėsmių ir pažeidžiamumų valdymo mechanizmus:
   1. Teikėjas privalo vadovautis pripažintomis saugaus programinės įrangos kūrimo metodikomis, tokiomis kaip ISO/IEC 27034-1 arba lygiavertėmis;
   2. Teikėjas privalo užtikrinti, kad visi su programinės įrangos kūrimu susiję darbuotojai būtų susipažinę su saugaus programavimo metodikomis;
   3. Teikėjas privalo atlikti patikrinimus, siekiant nustatyti pagrindines saugumo rizikas ir pažeidžiamumus, vadovaudamasis CWE/SANS Top 25 pavojingiausių programinės įrangos klaidų sąrašu ir OWASP Top 10 svarbiausių žiniatinklio programų saugumo rizikų sąrašu, bei pašalinti visus nustatytus trūkumus. Atlikęs patikrą ir pašalinęs pažeidžiamumus, teikėjas turi pateikti deklaraciją, kad po kūrimo darbų užbaigimo sprendime neliko pažeidžiamumų, išvardytų CWE/SANS Top 25 ir OWASP Top 10 sąrašuose;
   4. Teikėjas privalo pateikti visų sprendime naudojamų trečiųjų šalių komponentų sąrašą;
   5. Teikėjas turi imtis atitinkamų veiksmų (t. y. pagrįstų pastangų), kad užtikrintų trečiųjų šalių komponentų atitiktį kliento saugumo reikalavimams.
2. Priėmimo testavimo, pilotinio projekto ar kitu su Užsakovu suderintu laikotarpiu teikėjas turi sudaryti visas būtinas sąlygas Užsakovo atstovams atlikti sprendimo įsiskverbimo (angl. penetration) testavimą. Jei reikės, teikėjas privalo atlikti reikiamus konfigūracijos ar programavimo darbus, kad būtų galima testuoti sprendimo saugumą įvairiuose naudojimo scenarijuose. Teikėjas neprivalo pateikti jokios programinės ar techninės įrangos šiems testams vykdyti.
3. Teikėjas privalo atlikti visus reikiamus programavimo ir (ar) konfigūracijos darbus, atsižvelgdamas į Užsakovo atstovų atlikto įsiskverbimo (angl. penetration) testavimo rezultatus, ir pašalinti visus nustatytus reikšmingus saugumo pažeidžiamumus prieš pradedant sprendimo eksploatavimą.

### Su nacionaliniu saugumu susiję reikalavimai

1. Teikėjas privalo užtikrinti, kad teikiamos paslaugos atitiktų reikalavimus, nustatytus „Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše“, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.
2. Teikėjas privalo pasirašyti asmens duomenų tvarkymo sutartį, kaip nustatyta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 (Bendrasis duomenų apsaugos reglamentas) 28 straipsnio 3 dalyje. Šioje sutartyje turi būti nustatytas tvarkymo dalykas ir trukmė, duomenų tvarkymo pobūdis ir tikslas, asmens duomenų rūšys ir duomenų subjektų kategorijos, taip pat Užsakovo pareigos ir teisės.
3. Teikėjas yra atsakingas už tai, kad būtų laikomasi Lietuvos Respublikoje galiojančių darbuotojų saugos ir sveikatos teisės aktų bei kitų darbuotojų saugą ir sveikatą reglamentuojančių dokumentų.

### Kiti saugumo reikalavimai

1. Saugumo pataisymų ir atnaujinimų valdymas:
   1. Teikėjas privalo naudoti naujausias stabilias programinės įrangos versijas bei jų pataisas (angl. patches)/koregavimus, kuriant Sprendimą.
2. Neleistinos prieigos prevencija:
   1. Bet kokia neautorizuota arba nedokumentuota nuotolinė ar vietinė prieiga / paskyros, taip pat bet kokia slapta (nedokumentuota) funkcija, galinti kelti grėsmę Sistemos saugumui, yra draudžiama.
3. Saugaus konfigūravimo reikalavimai:
   1. Teikėjas privalo pateikti išsamias Sistemos ir platformos (operacinės sistemos, duomenų bazių valdymo sistemos, tarpinės programinės įrangos) saugaus konfigūravimo instrukcijas.
   2. Teikėjas privalo pateikti platformos komponentų, sisteminių paslaugų ir prievadų (portų), būtinų Sistemos veikimui, sąrašą. Visi komponentai, kurie nėra būtini Sprendimo funkcionalumui, turi būti išjungti prieš Sprendimo paleidimą.
   3. Tinklo architektūra:
      1. Duomenų srautai tarp skirtingų lygmenų turi būti dokumentuoti, nurodant komunikacijai reikalingus prievadus ir protokolus, o jų srautai turi būti ribojami ugniasienėmis.
      2. Sistemos išorinis portalas turi būti įdiegtas atskirame tinklo segmente, atskirtame nuo vidinių Sistemos posistemių.