Příloha č. 2

**Minimální technické požadavky - IS pro sdílení klinických postupů nad databázemi nádorových onemocnění**

**Zkratky:**

FNOL Fakultní nemocnice Olomouc

GDPR Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)

IS informační systém pro evidenci a zpracování výsledků vědy a výzkumu

SLA úroveň dohodnutých služeb (service level agreement)

VZ veřejná zakázka

**1. Obecné požadavky**

Zadavatel stanovuje dále uvedené minimální technické požadavky na IS včetně servisní podpory.

Řešení musí soustředit v jednom systému všechny požadované funkcionality IS s tím, že z hlediska účelnosti budou současně využívány i další IS zadavatele. Požadované integrační vazby budou součástí úvodní analýzy.

Servisní podpora se bude řídit dle jednotlivých SLA uvedených v návrhu servisní smlouvy jako její Příloha č. 2 – SLA.

**2. Podklady pro kalkulaci nákladů**

Zadavatel požaduje, aby součástí celkové nabídkové ceny bylo:

* všechny nezbytně potřebné licence pro provoz IS včetně neomezených uživatelských licencí;
* servisní podpora dle SLA na dobu trvání pilotního projektu, tedy 12 měsíců;
* prodloužená splatnost faktur 60 dnů.

**3. Požadavky na IS.**

Zadavatel požaduje poskytnutí služeb na cloudové řešení na principu software-as-a-service, které slučuje informace z různých zdrojů a poskytuje platformu k vizualizaci kontextuálních informací o pacientech do jedné aplikace za účelem pracovního odbavení specialistů z klinického týmu pacienta (například onkolog, patolog, radiolog, chirurg apod.), přičemž zahrnuje i aplikace podporující klinické rozhodování.

IS musí:

* využívat údaje o zdraví pacienta zahrnující zejména údaje ze systému elektronických zdravotnických záznamů („EMR“), radiologické snímky pacienta, digitální patologické snímky, patologické zprávy, genetické zprávy, průběžné zprávy a případně další jiné informace;
* poskytovat optimální a komplexní pohled na onkologického pacienta;
* pomocí strukturovaných dat aktivně pracovat s daty a připravovat je ke kolaborativnímu rozhodování u specifických terapií u onkologických pacientů. Tato rozhodnutí zachycovat ve strukturované formě;
* umožnit vybrat kategorii a přidat informaci, která se zobrazí zpět v pacientském elektronickém záznamu (EMR);
* umět napomoct zkompletovat úkoly jako vytvořit pacienta nebo příprava onkologické (histo-patologické) komise, a zjednodušit komunikaci mezi odděleními;
* umět informace obsažené v IS aktivně využít k prohledávání databází klinických studií a také publikací, které byly/jsou u podobného pacienta (pacientů) po celém světě publikované. V případě klinických studií minimálně z 21 různých registrů a v případě publikací min ze čtyř zdrojů;
* umožnit do něj implementovat lokální či vybrané pracovní postupy (guidelines), kterými se dané odbornosti řídí;
* umožnit efektivní a bezpečný přístup k datům pacienta zahrnující různé elektronické lékařské záznamy (EMR), obrázky z radiologie, výsledky z laboratoří, registry onemocnění, reporty z patologie a molekulární data, NGS reporty aj.;
* umožnit zobrazování patologických a histopatologických dat a využití digitální patologie v rozhodovacím procesu;
* data zabezpečit dle certifikací HIPAA a GDPR regulací: HITRUST a ISO 27001, ISO 27017 a ISO 27018;
* vytvořit časovou osu (time-line), ve které budou chronologicky řazená data a výsledky jednotlivých vyšetření;
* umět vytvořit multidisciplinární setkání včetně prezentace a připnutí nejdůležitějších bodů k diskusi;
* umět zajistit on-line připojení a přizvání kolegů;

Cílem pilotního testování systému poskytovatele ve FNOL bude po dobu jednoho roku (12 měsíců) s vybranými pracovníky FNOL monitorovat, připravovat a testovat tento systém, identifikovat přínosy a benefity pro FNOL, zejména pro zdravotnický personál. Zejména pak:

* zadavatel bude:
* manuálně vkládat omezený počet dat pacientů, zejména osobní data, rok narození, anamnézu;
* vkládat reporty jednotlivých vyšetření, data z laboratoří, molekulární a patologická data;
* poskytovatel:
* vytvoří časovou osu (time-line), ve které budou chronologicky řazena data a výsledky jednotlivých vyšetření;
* otestuje možnost automatizovat a natahovat data z digitální patologie;
* naučí pracovníky zadavatele zjednodušenou formou vytvořit multidisciplinární setkání včetně prezentace a připnutí nejdůležitějších bodů k diskusi;
* zajistí on-line připojení a přizvání kolegů;
* zmonitoruje všechny vstupy, které vedou během multidisciplinárního sezení k výslednému rozhodování, zjistí četnost vstupů a potenciál pro implementaci (automatické natahování);
* připraví analýzu implementace, zrychlení procesu, oficiální zpracování dokumentace, její uchování aj.;
* proškolí personál, zorganizuje potřebné semináře, kde ukáže benefity;
* zajistí bezplatné školení a podporu produktu

Zadavatel požaduje, aby nabízený IS:

* byl instalován a provozován na HW prostředcích a v **cloudovém prostředí poskytovatele** služby, případně jeho smluvního partnera;
* umožňoval přístup k aplikaci a datům odkudkoliv přes webový přístup (webová aplikace);
* měl webové řešení pro více subjektů;
* umožňoval přístup k aplikaci přes webový prohlížeč min.:
* MS Edge chromium 70 a novější;
* Google Chrome 70 a novější;
* Mozilla Firefox 70 a novější;
* Opera 60 a novější;
* Safari 10 a novější.
* a služba byla provozovatelná s garancí poskytovatele na aktualizace aplikace pro nové verze webových prohlížečů;
* splňoval všechny požadavky dle bodu **5. Požadavky na webové aplikace;**
* byl dimenzován pro min. 500 uživatelů z řad zaměstnanců a externích studentů a zahrnoval licenční oprávnění pro neomezený počet uživateů (serverová licence);
* ověřoval uživatele v MS Active Directory zadavatele (ADSF a SSO);
* archivoval logování spuštění a průběhů aplikace a online přístup administrátorů zadavatele k logům min. po dobu 18 měsíců. Logy musí obsahovat informace min. o činnostech:
* přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů;
* provedených administrátory;
* úspěšné i neúspěšné manipulace s účty, oprávněními a právy;
* neprovedení činností v důsledku nedostatku přístupových práv a oprávnění;
* uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému;
* byl celý v české lokalizaci, tedy nejen v českém jazyce ale i v souladu s platnou českou legislativou;
* umožnil nastavení práv přístupů určených uživatelů aplikace.

**4. Další požadavky**

Uchazeč musí být poskytovatelem/výrobcem nebo mít od něj souhlas k přístupu a změnám zdrojových kódů, datových struktur nabízeného IS a služby tak, aby mohl provádět úpravy dle požadavků zadavatele (tuto skutečnost doloží uchazeč potvrzením od poskytovatele / výrobce);

Nabízený IS:

 - musí splňovat požadavky GDPR a Zákona o kybernetické bezpečnosti uvedené v textu návrhu

 Smlouvy;

- integrační vazby dle bodu 6. prostřednictvím datových standardů;

- integraci bude řešit úvodní analýza. Uchazeč se zavazuje poskytnout součinnost při této

 integraci.

Datové úložiště a servery pro požadovanou službu musí být umístěny na území Evropské unie ideálně v České republice. Informace uvede uchazeč v Příloha č.4 – Čestné prohlášení. Zadavatel požaduje doložit úroveň bezpečnosti poskytovaných cloudových služeb alespoň jedním aktuálně platným z těchto dokumentů/certifikátů:

* ČSN ISO/IEC 27001;
* Auditní zprávu SOC 2 Type II (AT101);
* ISO 27017

Zadavatel požaduje šifrovanou komunikaci (TLS/VPN) přes internet.

Zadavatel ještě před podepsáním smlouvy vyzve vítězného uchazeče k okamžitému (nejpozději však do 14 dnů) provedení prezentace nabízeného IS za účelem prokázání splnění **všech** požadovaných funkcionalit dle této Přílohy č.2 zadávací dokumentace.

Součástí bude poskytnutí dokumentace – uživatelského a administrátorského manuálu v elektronickém formátu a jejich aktualizace s každou nově nasazenou verzí, která přinese změny v ovládání aplikace.

Uchazeč, jako poskytovatel, bude mít povinnost informovat určené pracovníky zadavatele o nasazení/změně aktuální verze systému.

**5. Požadavky na webové aplikace**

Zadavatel požaduje, aby uchazečem nabízené webové aplikace obsahovaly řešení potlačující rizika dle doporučení OWASP z roku 2017 min. v rozsahu T10 (A1-A10):

**A1 – injektování -** ke zranitelnostem injektováním, např. injektováním SQL, OS a LDAP, dochází,

 když se jako součást příkazu nebo dotazu odesílají do interpretu nedůvěryhodná data.

 Útočníkova nepřátelská data mohou lstí přimět interpret k provedení nezamýšlených příkazů

 nebo k umožnění přístupu k datům bez řádné autorizace.

**A2 – Chybná autentizace a správa relace -** funkce aplikací, které se vztahují k ověřování a správě

 relace, často nejsou provedeny správně, což útočníkům umožňuje kompromitovat hesla, klíče

 nebo tokeny relací anebo zneužít jiné slabiny v implementaci k tomu, aby převzali identitu

 jiných uživatelů.

**A3 – Expozice citlivých dat -** mnoho webových aplikací a rozhraní API nechrání náležitě citlivá data,

 jakými jsou např. finanční, zdravotní a PII. Tato slabě chráněná data útočníci mohou krást či

 modifikovat, aby mohli provádět podvody s kreditními kartami, krádeže identity nebo jiné

 trestné činy. Citlivá data si zaslouží zvláštní ochranu, např. šifrování dat v klidu nebo v

 na cestě, stejně tak i zvláštní bezpečnostní opatření pro data v prohlížeči.

**A4 – XML externí subjekty (XXE) -** mnoho starších nebo špatně nakonfigurovaných procesorů

 XML vyhodnocuje odkazy na externí entity v rámci XML dokumentů. Externí entity lze použít k

 odhalení interních souborů pomocí obslužné rutiny identifikátoru URI souboru, interní sdílení

 souborů, interní skenování portů, vzdálené spuštění kódu a útoky odmítnutí služby.

**A5 – Nedostatečné řízení přístupů -** omezení toho, co mají povoleno ověřovaní uživatelé, často

 nejsou řádně vynucována. Útočníci mohou tyto nedostatky využít k přístupu k neoprávněným

 funkcím a / nebo datům, jako je přístup k účtům jiných uživatelů, prohlížení citlivých souborů,

 úprava dat ostatních uživatelů, změna přístupových práv atd.

**A6 – Ne-zabezpečená konfigurace -** dobré zabezpečení vyžaduje mít definováno a nasazeno

 bezpečné nastavení aplikace, frameworků, aplikačního serveru, webového serveru, databázového

 serveru, platformy, cloudového úložiště, záhlaví HTTP a podrobných chybových zpráv

 obsahujících citlivé informace. Bezpečnostní nastavení by měla být definována, prováděna a

 udržována, protože výchozí hodnoty jsou často riskantní. Všechny operační systémy, rámce,

 knihovny a aplikace musí být bezpečně nakonfigurovány a včas opraveny a upgradovány.

**A7 – Cross-Site Scripting (XSS**) - chyby typu XSS nastávají tehdy, když aplikace přijme

 nedůvěryhodná data a odešle je webovému prohlížeči bez řádného ověření nebo escapování.

 XSS útočníkům umožňuje spouštět skripty v prohlížeči oběti, které mohou unést uživatelské

 relace, přetvořit webové stránky nebo přesměrovat uživatele na škodlivé stránky.

**A8 – Nezabezpečená deserializace -** často vede ke vzdálenému spuštění kódu. I když nedostatky

 deserializace nemají za následek vzdálené spuštění kódu, mohou být použity k provádění útoků,

 včetně jejich opakování, injekčních útoků a útoků na eskalaci privilegií.

**A9 – Použití známých zranitelných komponent -** komponenty, např. knihovny, frameworky a další

 softwarové moduly, téměř vždy běží s nejvyššími oprávněními. Jestliže je zranitelná

 komponenta zneužita, útok může usnadnit závažnou ztrátu dat nebo ovládnutí serveru. Aplikace

 používající komponenty se známými zranitelnostmi mohou zmařit ochranu aplikací a umožnit

 řadu útoků a dopadů.

**A10 – Nedostatečné protokolování a monitorování -** spojené s chybějící nebo neúčinnou odezvou

 na incident, umožňuje útočníkům další vytrvalé útoky, rozšiřovat na více systémů, manipulovat,

 extrahovat nebo zničit data. Většina studií porušení ukazuje, že jsou obvykle detekovány

 externími stranami, nikoli interními procesy nebo monitorováním.

**6. Integrační vazby**

Zadavatel požaduje nabízený IS integrovat na jeho interní systémy:

* uživatelů (LDAP/MS Active Directory) pomocí SSO, konkrétně napojení na ADFS;
* test možnosti integrace na systém digitální patologie;

**7. Požadavky na provedení implementace**

Implementace bude zahrnovat poskytnutí veškerých potřebných licencí k dodanému IS, které jsou již zahrnuty v ceně nabídky.

Implementace bude zahrnovat integraci dle bodu 6. (bude předmětem úvodní analýzy).

Zadavatel požaduje provedení implementace takovým způsobem, aby výsledkem implementace byly poskytovatelem služby splněny následující body:

* vytvoření úvodní analýzy popisující detailně cílové řešení. Na základě této analýzy bude provedena implementace/nasazení IS. Dokument s procesní analýzou slouží zejména ke vzájemnému pochopení a vyjasnění všech aktivit, kterých se následná implementace IS dotkne. Výstupem bude dokument „Implementační analýza“, který projde schvalovacím procesem zadavatele.
* provedení komplexní integrace na systémy a jiné datové zdroje zadavatele provozované v prostředí zadavatele a nutné k integraci daného řešení;
* řádné otestování všech instalovaných součástí nabízeného IS v testovacím prostředí a následně i v ostrém provozu;
* školení správců IS v takovém rozsahu, aby byli schopni řešit funkčnost systému v rámci FNOL, byli schopni poskytovat uživatelskou podporu pracovištím zadavatele, spravovat systém po stránce nastavování jednotlivých funkcionalit, nastavování přístupových oprávnění, uměli poskytovat podporu klíčovým uživatelům, uměli popsat požadavky jednotlivých pracovišť směrem k poskytovateli služby…;
* školení klíčových uživatelů jednotlivých pracovišť zadavatele, v rámci kterého si osvojí všechny úkony spojené s použitím základních funkcí IS, aby uměli poskytovat podporu uživatelům, uměli popsat požadavky pracoviště směrem k administrátorovi systému, a to formou teoretické průpravy i praktického zaškolení na takové úrovni, aby byli schopni školit další uživatele IS na svých pracovištích ve FNOL;
* u všech školení dodání zápisu s jmenovitým seznamem proškolených osob a obsahem školení;
* předání uživatelského a administrátorského manuálu v elektronické podobě v českém jazyce;
* ověření, zda poskytované webové aplikace splňují řešení potlačující rizika v oblasti bezpečnosti webových aplikací dle doporučení OWASP z roku 2017 (viz Příloha č.5) min. v rozsahu T10 (A1-A10);
* aktivní dohled v průběhu testování, popřípadě na výzvu zadavatele provést úkony v rozsahu dle potřeby, ale min. v délce jednoho měsíce;
* rozběh ostrého provozu.

O provedené implementaci a jejím splnění bude sepsán akceptační protokol, který bude obsahovat popis případných nedostatků. Implementace bude považována za dokončenou až v okamžiku, kdy bude IS řádně bez závad a nedodělků fungovat v ostrém provozu a bude oběma stranami akceptována podpisem protokolu o provedení implementace.

Poskytovatel zahájí plnění předmětu zakázky do 7 pracovních dnů po oboustranném podpisu smlouvy (analýza) a implementuje IS v **plné** míře výše uvedených požadavků a funkcionalit nejpozději do 3 měsíců od zahájení plnění.

**8. Servisní podpora**

Servisní podpora bude součástí poskytovaných služeb a měsíčního paušálu. Požadavky na servisní podporu jsou popsány v Příloze č. 3 – Návrh Smlouvy o poskytování služeb technické podpory a servisu a v SLA jako příloha č.2 uvedené smlouvy.