**Technické podmínky: Interoperabilita e-Health**

**Cíle zadavatele**

Cílem této veřejné zakázky je zlepšení kvality poskytované péče při využívání informačních technologií a postupů v oblasti zdravotnictví, a to především zlepšením způsobu vedení zdravotnické dokumentace umožňující její interoperabilní výměnu, sdílení, bezpečné uložení a interpretaci, prostřednictvím modernizace informačních systémů nemocnic zřizovaných Krajem Vysočina.

Zdravotnická dokumentace bude v maximální možné míře vedena a přenášena v elektronické podobě tak, aby pacientům a oprávněným osobám byl umožněn on-line přístup k této zdravotnické dokumentaci, která bude odpovídat standardům interoperability dle specifikace MZ/NCEZ (národní standardy pro vnitrostátní předávání zdravotnické dokumentace - dále CZ) a také standardům dle specifikace MyHealth@EU (pro přeshraniční komunikaci - dále EU).

Součástí dodávky je také splnění povinností nemocnic ve smyslu využívání nově zaváděných centrálních systémů elektronického zdravotnictví a nových povinností vyplývajících z EU legislativy (nařízení EHDS).

Dalším cílem této veřejné zakázky je minimalizace závislosti zadavatelů na konkrétním výrobku případně dodavateli prostřednictvím zavedení otevřených interoperabilních řešení.

**Požadavky na řešení systému**

Dodané řešení musí splňovat následující funkční a technické požadavky:

1. Dodávka řešení umožňující vytváření, sdílení, příjem a zobrazení zdravotnické dokumentace v podobě standardizovaných elektronických zdravotních záznamů (dále EHR) prostřednictvím služeb a rozhraní provozovaných v souladu se standardy elektronického zdravotnictví a doporučeními IHE. Výstupem budou plně strukturovaná data.

Součástí dodávky je podpora scénářů (usecase) pro tyto jednotlivé standardy interoperability dle specifikace MZ/NCEZ (národní standardy pro vnitrostátní předávání zdravotnické dokumentace - dále CZ) a také dle specifikace MyHealth@EU (pro přeshraniční komunikaci - dále EU - viz <https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en>):

* Laboratorní zpráva (CZ, EU)
* Zpráva z obrazových vyšetření (CZ, EU)
* Obrazové vyšetření (CZ, EU)
* Propouštěcí zpráva (CZ, EU)
* Pacientský souhrn (CZ, EU)
* Originální klinický dokument (CZ, EU)
* Záznam o výjezdu (CZ)
* Žádanka laboratorního vyšetření (CZ)
* Žádanka obrazového vyšetření (CZ)

Součástí zadávací dokumentace jsou aktuální verze standardů dostupné zadavateli v době vyhlášení VZ.

Předmětem dodávky bude řešení respektující standardy platné v době předání díla a údržba informačního systému v rámci servisu tak, aby byl v souladu s platnou legislativou i standardy.

Předmětem dodávky je implementace standardů v plném rozsahu povinných i volitelných položek daného standardu. V případě nedostupnosti dat ze zdrojového systému bude využita metodika HL7 NullFlavor

<https://terminology.hl7.org/1.0.0/CodeSystem-v3-NullFlavor.html>

1. Dále musí být součástí dodávky úprava prostředí organizace tak, aby podporovalo a využívalo rozhraní (API) dle specifikace:

* profilu IHE MHD (zápis do registru, vyhledání záznamu, získání záznamu/dokumentu, uložení záznamu do repozitáře) v akreditované afinitní doméně
* centrálních systémů elektronického zdravotnictví
  + Kmenový registr pacientů
  + Kmenový registr poskytovatelů
  + Kmenový registr zdravotnických pracovníků
  + Dočasné úložiště
  + Národní kontaktní místo pro elektronické zdravotnictví (NCPeH)
  + Registr oprávnění
  + Centrální terminologický server
  + Napojení na Národní registry NZIS
  + Implementace systému eŽadanek
  + Žurnál činností
  + Notifikační služby

Implementace API pro výměnu a sdílení zdravotnické dokumentace dle Standardů EZ (Standard EZ - Dočasné úložiště), které umožní sdílení, předávání, vyhledávání a získávání EHR určené k výměně EHR s pacienty či jinými PZS v rámci zajištění kontinuity péče. Implementace bude provedena v souladu s výše jmenovaným Standardem. API je postaveno na následujících technických principech:

REST API rozhraní:

* API využívá standardní HTTP metody: GET, POST, PUT, DELETE dle definice FHIR pro příslušné transakce.
* Zdroje jsou identifikovány pomocí URI.
* Implementuje hypermediální odkazy (HATEOAS), které umožňují navigaci mezi zdroji.
* Možnost řízení oprávnění jednotlivých metod dle kritérií popsaných v úvodní analýze

1. Pro všechny výše popsané usecasy budou dodány nástroje na vyhledání, získání, poskytnutí, zobrazení a uložení EHR.
2. Zavedení systémů evidence jednoznačných identifikátorů příslušných vydaných a získaných dokumentů EHR (index dokumentů) a jejich úložišť (repozitářů).
3. Dodané Řešení bude respektovat tyto požadavky:
   1. podpora jednotného systému identifikace a přihlašování uživatelů (IDM, SSO) nebo pomocí Microsoft Active Directory/Entra ID. Aplikace nesmí lokálně ukládat žádná hesla a autentizace musí proběhnout prostřednictvím protokolu Kerberos/SAML/OIDC.
   2. Pokud je součástí aplikační software, který umožňuje diferencovat oprávnění v aplikaci (role), požadujeme, aby nastavení oprávnění v aplikaci bylo uděleno na základě členství ve skupině Microsoft Active Directory/Entra ID nebo prostřednictvím služeb IDM.
   3. Lokální účty jsou umožněny pouze jako systémové a fallback.
   4. S ohledem na skutečnost, že nemocnice jsou povinnou osobou dle Zákona č. 181/2014 Sb. požadujeme, aby veškeré logy ze všech aplikací a systémů byly ukládány do centrálního logovacího a vyhodnocovacího systému typu SIEM/SEM/logmanagement, a to prostřednictvím syslog protokolu dle RFC RFC 5424. Dále logy a auditní stopa musí splňovat tyto požadavky:
      1. Řešení musí zaznamenávat auditní záznamy a logy na všech existujících úrovních – tj. na úrovni:
         1. operačního systému aktiva,
         2. aplikačního serveru/modulu aktiva (např. web server, sql server, apod.)
         3. samostatné aplikace/informačního systému/služby informačního systému.
      2. Auditní záznamy a logy informačních aktiv musí obsahovat minimálně tyto informace:
         1. přihlášení a odhlášení všech uživatelů (včetně administrátorů či jiných privilegovaných účtů),
         2. činnosti provedené administrátory, např. (pokud danou funkcionalitu obsahují):
            1. přidělení/odebrání oprávnění,
            2. založení/smazání uživatele
            3. přidělení/odebrání role
            4. reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva)
            5. povýšení oprávnění administrátora, převzetí role konkrétního uživatele
            6. změna konfigurace logování událostí
            7. změna konfigurace informačního aktiva,
         3. činnosti prováděné uživateli,
         4. automatická informační, varovná a chybová hlášení provozního charakteru (tzv. aplikační logy)
      3. Auditní záznamy a logy musí obsahovat minimálně tyto parametry a metadata:
         1. identifikátor události,
         2. identifikátor zdroje událostí,
         3. přesné datum vzniku události,
         4. přesný čas vzniku události včetně specifikace časového pásma,
         5. typ/název události,
         6. případně popis události (pokud není zřejmé z typu/názvu),
         7. jednoznačnou identifikaci účtu, pod kterým byla událost provedena,
         8. jednoznačnou síťovou identifikaci zařízení původce a
         9. úspěšnost nebo neúspěšnost (včetně neprovedení činnosti v důsledku nedostatečných oprávnění) události.
      4. Formát (resp. standard) logů musí být v jedné z následujících možností:
         1. syslog (RFC 5424) + syslog over TLS,
         2. MS Windows Event Log (případně vlastní umístění XPath pro informační aktivum),
         3. W3C (pro MS IIS Web server),
         4. Standardní apache/nginx web server logy,
         5. SQL view,
         6. MS SQL audit logy,
         7. jiné (pouze na základě domluvy a po předchozím schválení), např.:
            1. json,
            2. plain-text line-oriented logy,
            3. xml,
            4. atd.
   5. Požadujeme plnou funkcionalitu všech dodávaných řešení minimálně na protokolech IPv4.
   6. Verze OS – v rámci instalace a dodávky nových HW a SW řešení je podporován pouze OS ve verzi, který má aktuálně podporu od výrobce daného OS a to s výhledem minimálně dvou let dopředu.
   7. Nemocnice v Kraji Vysočina využívají pro ochranu operačních systémů na koncových stanicích i serverové infrastruktuře vlastní bezpečnostní řešení Je nutné počítat s jejich nasazením i pro dodávané řešení viz tabulka systémy k integraci.
   8. Aplikační servery/moduly/komponenty (např. web server, DB server, apod.) nesmí vyžadovat pro své spuštění privilegovaná oprávnění operačního systému (např. typu root, Administrator, NT Authority\System, apod.).
   9. Požadavky na použité kryptografické funkce, algoritmy, mechanismy a zařízení jsou samostatně definovány ve smlouvě o dílo a servisní smlouvě.
   10. V případě, že bude v řešení použit webový server, musí být nakonfigurovaný tak, aby splňoval požadavky na bezpečnostní HTTP hlavičky dle dobré bezpečnostní praxe, která je definována prostřednictvím OWASP CheatSheet projektu, konkrétně dle doporučení HTTP Security Response Headers Cheat Sheet (<https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html>)
4. Řešení musí poskytovat auditní logy dle doporučení IHE profilů ATNA nebo BALP, které lze kombinovat s požadavky na logování viz bod 6.
5. Funkce rozlišení zdroje zdravotnické dokumentace - cílem je umožnit evidenci, ale zároveň zamezit předávání dokumentů, u kterých není autorem organizace (daná nemocnice). Např. zpráva o výjezdu ZZS nebo vnesená dokumentace pacienta.
6. Řešení musí podporovat elektronickou tvorbu, správu a výměnu (poskytnutí, získání, zobrazení a uložení) dokumentů definovaných v rámci vyhlášky č. 444/2024 Sb. o zdravotnické dokumentaci a to jak pro účel EMERGENCY a TREATMENT (žádost ošetřujícího lékaře) tak pro účel PATIENT (pacient žádá o svůj EHR) a to s rozlišením cíle předávaných dat (vnitrostátní vs. přeshraniční).
7. Veškeré získané externí EHR ve všech usecasech s příjmem dat budou automaticky založeny do zdravotnické dokumentace daného pacienta u systému, které tyto metody umožňují - bude upřesněno v rámci úvodní analýzy.
8. Dodané řešení musí být schopno na základě služeb klientského konektoru NCPeH (role B) nabídnout integrované klientské prostředí (UI) pro identifikaci pacientů v rámci infrastruktury MyHealth@EU (konfigurační služby), jejich vyhledání, získání a jeho zobrazení a uložení ve zdravotnické dokumentaci včetně správných identifikátorů pacienta-cizince s to jak ve formě L1 tak ve formě L3 pro všechny EHR podporované na úrovni NCPeH pro ČR.
9. Součástí dodávky je provedení funkčních testů jednotlivých scénářů a EHR vůči testovací platformě MZ/NCEZ a vůči prostředí NCPeH v souladu s metodikami testování platnými v době předání díla a zapracování případných výhrad a nálezů z testů. Součástí dokumentace díla bude zpráva o provedení testu s výsledkem bez blokujících výhrad.
10. Rozhraní pro příjem a předávání EHR bude obsahovat funkci validátoru předávaných dat vůči specifikaci EHR včetně možnosti konfigurace možných akcí v případě nesouladu (blokace, varování).
11. Součástí dodávky je implementační analýza pro každou organizaci, obsahující:
    1. návrh detailní architektury řešení včetně popisu integrace stávajících systémů organizace. Architektura se skládá minimálně z těchto částí:
       1. Komunikační vrstva (sítě, výměnné protokoly, porty)
       2. Infrastrukturní vrstva (servery, úložiště)
       3. Aplikační vrstva
       4. Bussines vrstva (logický model a datové toky)
    2. způsob řešení standardizovaných EHR včetně popisu zdrojů dat, datového modelu a návrhu interní metodiky vedení zdravotnické dokumentace
    3. specifikace API až do úrovně jednotlivých metod, oprávnění a podporovaných scénářů a IHE profilů
    4. specifikace nezbytné součinnosti ze strany zadavatele při integraci systému třetích stran
    5. zohlednění metod identifikace pacientů v organizaci (GS1)
    6. harmonogram implementace zohledňující stav standardizace a stav implementace integrovaných systémů a v souladu s požadavky SoD
    7. popis datových toků zdravotnické dokumentace včetně metod zpracování, zpřístupnění, míst uložení, klasifikace a její identifikace
    8. návrh mechanismů zpřístupnění a případné integrace dříve vytvořených (nestandardizovaných) částí zdravotnické dokumentace do systému výměny dat (např. zpřístupnění jen v L1 formě)
    9. návrh způsobu údržby dokumentace a záznamů o change managementu včetně návrhu formátu a prostředí
12. Veškerá aplikační rozhraní (API) dodaného řešení budou dokumentována pomocí strojově čitelné dokumentace dle OpenAPI specifikace (např. Swagger)
13. Řešení provádí řádnou identifikaci pacientů i cizinců, jejich ztotožnění vůči Kmenovému registru pacientů, identifikaci uživatelů žádajících o data včetně ztotožnění vůči Kmenovému registru zdravotnických pracovníků a identifikaci zařízení vůči registru poskytovatelů zdravotních služeb. Součástí řešení bude i získání dat o registrujících lékařích a zdravotní pojišťovně pacienta. Tyto funkce jsou realizovány formou otevřeného řešení využitelného i jinými IS organizace, např. MPI.
14. Dodané řešení nebude licenčně omezeno ve smyslu času (perpetuální), počtu transakcí, uživatelů ani počtu integrovaných systémů.
15. Za rozumnou a vhodnou se považuje využití open source řešení celé dodávky (včetně produkčního prostředí).
16. Dodané řešení musí být ve smyslu komunikace s centrálními službami elektronického zdravotnictví provozovatelné v rámci sítě CMS2 a to i v ostrovním režimu bez dostupnosti veřejného internetu. Musí být implementován mechanismus automatického směrování komunikace na aktuálně dostupné rozhraní dané služby (internet vs. CMS2, primární vs. sekundární rozhraní, apod.)
17. Dodané řešení musí integrovat systém správy souhlasů a mechanismus zastupování v návaznosti na Registr oprávnění a REZA.
18. Implementace povinných mechanismů zápisu údajů do Žurnálu činností minimálně v rozsahu komunikace s externími systémy.
19. Dodané řešení umožňuje oprávněným a zaškoleným administrátorům zadavatele samostatně konfigurovat integrační vazby a nástroje včetně definice datových zdrojů (např. nová API NIS, LIS, PACS), definovat pravidla čerpání dat, jejich transformace (mapování DASTA, HL7 CDA/FHIR, mapování nomenklatury, validace) a směrování dat (např. publikace jiným API, předání dat do dalších systémů typu NZIS, portál pacienta atd) bez zásahu dodavatele. Konfigurace musí být možná prostřednictvím přehledného webového rozhraní, nástroje typu grafický orchestrátor případně skriptovací jazyk.
20. Integrace Notifikačních služeb jako centrální služby elektronického zdravotnictví minimálně pro úlohy: avíza pacientům a lékařům v okamžiku vytvoření zprávy z laboratorního vyšetření a zprávy z obrazového vyšetření.
21. Součástí dodávky řešení musí být bezpečnostně provozní dokumentace v tomto rozsahu:
    1. Analýza rizik
       1. součástí dodávky bude podrobné a komplexní provedení analýzy rizik informační bezpečnosti v souvislosti jak s nasazením řešení (informačního aktiva), tak i s jeho provozem. Analýza rizik informační bezpečnosti musí být zpracována před nasazením do provozního režimu. Zhotovitel/dodavatel vypracuje a předá objednateli:
          1. zdokumentovaný postup provedení analýzy rizik (metodiku, jak postupoval),
          2. zprávu z analýzy rizik obsahující vydefinovaná a klasifikovaná rizika, která jsou určena na základě míry dopadu, pravděpodobnosti výskytu zranitelnosti a pravděpodobnosti naplnění hrozby, a popis těchto rizik,
          3. plán zvládání rizik s návrhy opatření na snížení míry případných rizik včetně popisu způsobu jejich nasazení.
       2. Objednatel bude schvalovat výstupy z provedené analýzy rizik před nasazením řešení (informačního aktiva) do provozního režimu formou akceptačního protokolu.
    2. Bezpečnostní specifikace systému
       1. Cíl dokumentu: popsat a zdokumentovat veškeré bezpečnostní mechanizmy a opatření za účelem identifikace toho, jaká data jsou jakým způsobem chráněna.
       2. Forma dokumentu: textový popis
       3. Minimální rozsah:
          1. Soupis a popis všech funkcí prosazujících bezpečnost pro:
             1. zajištění integrity dat při jejich přenosu a uložení,
             2. zajištění důvěrnosti dat při jejich přenosu a uložení,
             3. zajištění autentizace a session managementu,
             4. zajištění ošetření, filtrování a prověřování veškerých vstupních dat,
             5. zajištění auditní stopy a logování,
             6. externí rozhraní – jak uživatelská, tak pro komunikaci s externími systémy.
          2. Popis těchto oblastí:
             1. použité kryptografické funkce a algoritmy,
             2. autentizační a autorizační model a mechanizmus,
             3. řízení uživatelských a privilegovaných rolí a oprávnění
             4. detailní popis úrovně všech přístupových oprávnění/aplikačních rolí,
             5. způsob zajištění dostupnosti, důvěrnosti a integrity dat ve stavech jejich uložení/uchování, zpracování a přenosu,
             6. bezpečnostní architektura infrastruktury.
    3. Instalace systému
       1. Cíl dokumentu: popsat a zdokumentovat postupy, kroky a činnosti vedoucí k instalaci těch částí systému, které jsou instalované on-premise.
    4. Základní konfigurace
       1. Cíl dokumentu: popsat a zdokumentovat postupy, které vedou k nastavení systému do takového stavu, aby bylo možné systém po instalaci provozovat na základní úrovni.
    5. Záloha, obnova, restart
       1. Cíl dokumentu: popsat a zdokumentovat strategii zálohování systému, resp. návrh strategie zálohování od dodavatele, způsoby obnovy systému po havárii nebo ze zálohy, postupy a konkrétní kroky, které povedou k bezpečnému restartu systému.
       2. Zálohování
          1. Strategie zálohování systému navržená dodavatelem
       3. Obnova
          1. Posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému nebo jeho části či dat ze zálohy do jeho plně funkčního stavu
          2. Zpracovaný disaster recovery plán, tedy posloupnost kroků (co a jak udělat), které je třeba provést pro obnovu systému po jeho selhání do jeho plně funkčního stavu
          3. Včetně potřebných zdrojů, jako je např. SW, HW, přístupové údaje, data, parametry disaster recovery prostředí, apod.
       4. Restart
          1. Posloupnost kroků (co a jak udělat), které je třeba provést pro bezpečné restartování systému tak, aby naběhl do původního stavu
    6. Monitoring
       1. Cíl dokumentu: popsat a zdokumentovat mechanizmus monitorování a zaznamenávání bezpečnostních a provozních logů a auditních událostí.
       2. Popis logů informačního aktiva, jejich formát, umístění včetně cest, přístupnost a možnosti integrace na jiné systémy (SIEM, logmanagement, apod. )
       3. Popis možností provozního monitoringu (např. SNMP, síťový monitoring, aplikační monitoring) a návrh monitorovaných parametrů/metrik za účelem bezpečného provozování řešení
    7. Popis klíčových komponent
       1. Cíl dokumentu: popsat a zdokumentovat účel, význam, úlohu a způsob použití klíčových komponent systému

**Přehled systémů, jejichž integrace je předmětem dodávky:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **IS** | **NemJI** | **NemHB** | **NemPE** | **NemTR** | **NemNM** | **Komunikační formát** | **Datové rozhraní** |
| **NIS** | FONS FE (STAPRO s. r. o.) | FONS FE  Stapro s.r.o | FONS FE Stapro s.r.o | FONS FE Stapro s.r.o | FONS FE Stapro s.r.o | Dasta 3, Dasta 4, HL7 CDA | [Dokumentace FONS FE](https://stapro.atlassian.net/wiki/spaces/FE/overview)  [Rozcestník centrálního FEApi](https://stapro.atlassian.net/wiki/spaces/FE/pages/202834084/Rozcestn+k+centr+ln+ho+FEApi+k+jednotliv+m+controller+m) |
| **LIS** | Envis (DS Soft Olomouc, spol. s r.o.) | Amadeus Orpheus  Steiner | OpenLims  Stapro s.r.o | Amadeus Orpheus  Steiner | OpenLims  Stapro s.r.o | Dasta 3 | Výměna dat prostřednictvím filesystému |
| **PACS** | JiveX (VISUS Health IT GmbH) | Marie PACS ORCZ | Marie PACS ORCZ | Marie PACS ORCZ | JiveX (VISUS Health IT GmbH) | HL7, DICOM | webové služby  pro JiveX  OR CZ  viz příloha |
| **Archiv EZD[[1]](#footnote-1)** | DESA (ICZ a.s.) | DESA  ICZ | DESA | DESA | DESA | Dle typu uloženého dokumentu (typicky pdf, HL7, Dasta, atd) | IHE XDS.b ITI43 |
| **Výměnná síť** | eMeDocS (ICZ a.s.) | eMeDocS | eMeDocS | eMeDocS | eMeDocS | Dasta 3 | Viz příloha |
| **Antivir** | Microsoft Defender for Endpoint | Eset  protect | Trend Vision One Endpoint security | Eset  protect | Trend Vision One Endpoint security | Nerelevantní | Nerelevantní |
| **Centrální systémy EZ** | * + Kmenový registr poskytovatelů   + Kmenový registr zdravotnických pracovníků   + Dočasné úložiště   + Národní kontaktní místo pro elektronické zdravotnictví (NCPeH)   + Registr oprávnění   + Centrální terminologický server   + Napojení na Národní registry NZIS   + Implementace systému eŽadanek   + Žurnál činností   + Notifikační služby | | | | | Viz příloha | Viz příloha |

**Pro realizaci požadavků zadavatele je možné využít stávající rozhraní a podporované formáty informačních systémů provozovaných organizací (nemocnicí). Součinnost třetí osoby zajistí na své náklady zadavatel – nemocnice na základě úvodní analýzy.**

1. Archiv není primárním zdrojem strukturovaných dat, ale disponuje finální zdr. dokumentací typicky podepsanou nebo opečetěnou. Požadavek na integraci vychází ze situace, že veškerá finální zdravotnické dokumentace bude uložena v archivu, včetně podpisu či pečetě. [↑](#footnote-ref-1)