SPITALUL MUNICIPAL
ODORHEIU SECUIESC

535600 Odorheiu Secuiesc, Str. Bethlen Gábor, Nr.72, jud. Harghita - România
telefon: 0040-266-212 186, fax: 0040-266-218 188
e-mail: office@spitalodorhei.ro, website: www.spitalodorhei.ro
Acreditat de Guvernul României, certificat seria ANMCS Nr. 2-158

Nr. de inregistrare la Autoritatea Contractanta 2786/19.03.2026

Aprob,
Manager
KOMOROCZY ZSOLT

CAIET DE SARCINI

pentru atribuirea serviciilor avand ca obiect

„Servicii informatice pentru managementul activitatii medicale, clasificare DRG, analiza statistica, medicala si securitate cibernetica,

Avand urmatoarele referinte:

Procedura de atribuire:

Cod CPV: *48180000-3 – Pachete software pentru uz medical (Rev.2); 72212730-5 – Servicii de dezvoltare de software de securitate (Rev.2); 72700000-7 – Servicii de retele informatice (Rev.2).*
Valoare estimata:

Pozitia in PAAP 2026: 4245259_2026_PAAPD1604986

Modalitatea de atribuire: Procedura simplificata

Numar loturi:3

PROCEDURA SIMPLIFICATA

Acord cadru: 12 luni.

Capitolul 1. Introducere

1) Aceasta sectiune a Documentatiei de Atribuire include ansamblul cerintelor pe baza carora fiecare Ofertant va elabora OFERTA (*Propunere Tehnica si Propunere Financiara*) pentru prestarea serviciilor care fac obiectul Contractului ce va rezulta din aceasta procedura.

2) In cadrul prezentei procedure, SPITALUL MUNICIPAL ODORHEIU SECUIESC indeplineste rolul de Autoritate Contractanta, respective Achizitor in cadrul Contractului.

3) Pentru scopul prezentei sectiuni a Documentatiei de Atribuire, orice activitate descrisa intr-un anumit capitol din Caietul de sarcini si nespecificata in alt capitol, trebuie interpretata ca fiind mentionata in toate capitolele unde se considera de catre Ofertant ca aceasta trebuie mentionata pentru asigurarea indeplinirii obiectului Contractului.

4) Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o lienta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta de produs si nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse, aceste specificatii vor fi considerate ca avand mentiunea de SAU ECHIVALENT.

Capitolul 2. Contextul initierii procedurii de achizitie. Date generale privind procedura.

1) Spitalul Municipal Odorheiu Secuiesc este amplasat în zona de sud-vest a județului Harghita și reprezintă o unitate sanitară publică ce asigură servicii medicale pentru populația din municipiu și din localitățile limitrofe.

Profilul de activitate al spitalului constă în furnizarea de **servicii de asistență medicală spitalicească continuă și de zi pentru pacienți cu afecțiuni acute**, precum și **servicii de asistență medicală ambulatorie**, în cadrul specialităților clinice și paraclinice existente în structură.

2) Procedura de achiziție inițiată în baza prezentului **Caiet de sarcini** este necesară pentru **susținerea și eficientizarea activităților medicale și administrative desfășurate în cadrul Spitalului Municipal Odorheiu Secuiesc**, contribuind la îmbunătățirea condițiilor de desfășurare a actului medical, la creșterea calității serviciilor oferite pacienților și la optimizarea managementului operațional al unității sanitare.

2.1. Informatii generale despre Autoritatea Contractanta

1) Spitalul Municipal Odorheiu Secuiesc

Adresa: Strada: Str. Bethlen Gabor, nr. 72, Tipul juridic al cumparatorului: Autoritate locală, Cod fiscal: 4245259, Cod postal: 535600, Cod NUTS: RO124 Harghita, Localitate: Odorheiu Secuiesc, Tara: Romania, E-mail: achizitii@spitalodorhei.ro, Telefon:+40 266210069, Fax:+40 266210069, Adresa Internet (URL):https://spitalodorhei.ro, Adresa profilului cumparatorului:https://www.e-licitatie.ro.

2) Sector de activitate: Sanatate.

2.2. Informatii despre contextual care a determinat initierea procedurii. Date privind procedura.

Spitalul Municipal Odorheiu Secuiesc desfășoară activități medicale complexe, ce presupun gestionarea unui volum ridicat de date medicale și administrative, precum și raportarea periodică a activității medicale către instituțiile competente, inclusiv către Casa Națională de Asigurări de Sănătate, în conformitate cu metodologia de finanțare a serviciilor spitalicești prin sistemul DRG.

În acest context, unitatea sanitară are necesitatea utilizării unor **instrumente informatice specializate pentru clasificarea și analiza cazurilor medicale**, care să permită codificarea corectă a diagnosticelor și procedurilor, calcularea indicatorilor specifici activității medicale și generarea statisticilor necesare managementului spitalului și raportărilor instituționale.

Conform documentației tehnice, aplicația informatică de tip WebGrouper *sau echivalent*, permite clasificarea rapidă a diagnosticelor și procedurilor aferente cazurilor tratate în spital, determinarea finanțării corespunzătoare fiecărui caz și generarea automată a unor statistici relevante privind activitatea medicală (ex. indicatori precum ICM, durata medie de spitalizare, cazuri chirurgicale etc.).

De asemenea, aplicația permite analiza bazei de date a spitalului pe diferite perioade și realizarea de statistici pe medici, secții sau tipuri de cazuri.

Totodată, pentru buna funcționare a sistemelor informatice ale spitalului și pentru protecția infrastructurii IT care susține activitatea medicală, este necesară implementarea unor servicii specializate de **securitate cibernetică**, având în vedere obligațiile legale aplicabile operatorilor de servicii esențiale din domeniul sănătății și riscurile asociate incidentelor informatice. Serviciile propuse includ managementul vulnerabilităților, monitorizarea incidentelor de securitate, consultanță privind conformarea la cerințele legislative, precum și intervenții pentru remedierea incidentelor de securitate informatică.

În acest context, pentru asigurarea continuității activităților medicale, a acurateței raportărilor și a securității infrastructurii informatice, Spitalul Municipal Odorheiu Secuiesc inițiază prezenta procedură de achiziție a serviciilor informatice necesare.

Prezenta procedură de achiziție are ca obiect **furnizarea de servicii informatice și servicii asociate necesare desfășurării activităților medicale și administrative din cadrul Spitalului Municipal Odorheiu Secuiesc.**

Serviciile ce fac obiectul achiziției includ, în principal:

- utilizarea unei aplicații informatice specializate pentru clasificarea cazurilor medicale și analiza indicatorilor DRG;
- servicii de suport și instruire pentru personalul medical privind utilizarea aplicației și codificarea medicală;
- servicii de analiză și verificare a datelor medicale raportate;
- servicii de securitate cibernetică pentru protecția infrastructurii informatice și gestionarea incidentelor de securitate.

Coduri CPV relevante pentru procedură:

48180000-3 – Pachete software pentru uz medical
72212730-5 – Servicii software de securitate
72700000-7 – Servicii rețea informatică.

Serviciile vor fi furnizate pe bază de abonament lunar, iar implementarea și utilizarea aplicațiilor informatice vor permite accesul utilizatorilor autorizați ai spitalului la funcționalitățile necesare pentru analiza și raportarea activității medicale, cu respectarea cerințelor privind protecția datelor și securitatea informațiilor.

2.3. Informatii despre beneficiile anticipate de autroitatea contractanta

Implementarea serviciilor și soluțiilor informatice care fac obiectul prezentei proceduri de achiziție va genera o serie de beneficii pentru Spitalul Municipal Odorheiu Secuiesc, contribuind la creșterea eficienței activităților medicale și administrative, precum și la îmbunătățirea calității serviciilor oferite pacienților.

Prin utilizarea aplicațiilor informatice dedicate clasificării și analizei cazurilor medicale, personalul medical și administrativ va putea realiza într-un mod rapid și eficient codificarea diagnosticelor și procedurilor, precum și analiza indicatorilor specifici sistemului de finanțare DRG, ceea ce va conduce la creșterea acurateței raportărilor și la optimizarea procesului de finanțare a serviciilor medicale furnizate de unitatea sanitară. Totodată, aplicațiile informatice vor permite generarea automată a unor statistici relevante privind activitatea spitalului, facilitând procesul decizional la nivel managerial și monitorizarea performanței secțiilor și a personalului medical.

De asemenea, implementarea serviciilor de securitate cibernetică va contribui la creșterea nivelului de protecție a infrastructurii informatice și a datelor gestionate de spital, inclusiv a datelor medicale cu caracter sensibil. Aceste servicii vor permite identificarea și gestionarea vulnerabilităților sistemelor informatice, monitorizarea incidentelor de securitate, precum și intervenția rapidă în cazul apariției unor incidente care ar putea afecta funcționarea sistemelor informatice sau continuitatea activității medicale.

În ansamblu, implementarea soluțiilor și serviciilor ce fac obiectul prezentei achiziții va conduce la:

- îmbunătățirea acurateței și eficienței procesului de raportare a activității medicale;
- creșterea capacității de analiză și monitorizare a indicatorilor de performanță ai spitalului;
- optimizarea procesului de finanțare a serviciilor medicale;
- creșterea nivelului de securitate a sistemelor informatice și a datelor medicale;
- asigurarea continuității și siguranței activităților medicale și administrative desfășurate în cadrul unității sanitare.

Prin urmare, realizarea prezentei achiziții contribuie la modernizarea infrastructurii informatice a spitalului și la creșterea calității serviciilor medicale furnizate comunității deservite de Spitalul Municipal Odorheiu Secuiesc.

Capitolul 3. Descrierea produselor solicitate. Conditii tehnico - economice

Serviciile solicitate sunt:

Denumire serviciu	Cerință tehnică
LOT 1 – Servicii informatice clasificare DRG	**Servicii informatice pentru clasificarea cazurilor medicale DRG (de tip WebGrouper sau echivalent);** **CPV:** 48180000-3 – Pachete software pentru uz medical **CPV:** 48220000-6 – Pachete software pentru internet; Autoritatea contractantă solicită furnizarea de **servicii informatice pentru clasificarea cazurilor medicale conform sistemului DRG**, prin intermediul unei aplicații informatice **de tip WebGrouper sau echivalent**. Menționarea denumirii „WebGrouper" are rol exclusiv orientativ pentru descrierea nivelului de funcționalitate și performanță dorit. Se vor accepta **orice soluții software echivalente** care îndeplinesc **cel puțin cerințele funcționale și tehnice minime specificate în prezentul caiet de sarcini**, în conformitate cu prevederile legislației privind achizițiile publice. Soluția ofertată trebuie să fie o aplicație informatică **online (web-based)**, accesibilă prin intermediul unui browser web, destinată personalului medical și responsabililor DRG din cadrul spitalului pentru clasificarea rapidă a cazurilor medicale și analiza indicatorilor de activitate spitalicească. **1. Funcționalități minime obligatorii** Aplicația informatică ofertată, de tip **WebGrouper sau echivalent**, trebuie să asigure cel puțin următoarele funcționalități: **1.1 Clasificarea automată a cazurilor medicale** • clasificarea automată a cazurilor medicale pe baza **diagnosticelor și procedurilor introduse**, conform metodologiei DRG aplicabile la nivel național; • generarea rezultatului clasificării într-un interval de timp foarte scurt (de ordinul secundelor); • afișarea rezultatului clasificării DRG și a **valorii estimate a finanțării aferente cazului**. **1.2 Clasificarea bazelor de date ale spitalului** • posibilitatea clasificării unei **baze de date cu cazurile tratate în spital**, atât înainte, cât și după raportarea către instituțiile competente;

	• posibilitatea clasificării datelor pentru **perioade configurabile**, stabilite în funcție de necesitățile spitalului; • posibilitatea procesării unor volume mari de date fără limitări lunare privind numărul de cazuri analizate. **1.3 Generarea de statistici și indicatori de activitate** Aplicația trebuie să calculeze automat indicatori statistici privind activitatea spitalului, inclusiv, dar fără a se limita la: • **ICM – Indicele de Complexitate a Cazurilor**; • **DMS – Durata Medie de Spitalizare**; • **CP – Cazuri ponderate**; • numărul de **cazuri chirurgicale**; • alte statistici relevante pentru analiza activității medicale. Statisticile trebuie să poată fi generate: • pe **medici**; • pe **secții**; • la nivelul **întregului spital**. **1.4 Clasificarea cazurilor de spitalizare de zi** Soluția trebuie să permită: • clasificarea cazurilor de **spitalizare de zi**; • generarea statisticilor aferente acestui tip de activitate medicală. **1.5 Analiza detaliată a cazurilor clasificate** Aplicația trebuie să permită: • afișarea valorii **CCL (Complication and Comorbidity Level)** pentru diagnosticele secundare; • analiza rezultatelor clasificării pentru **multiple combinații de diagnostice și proceduri**; • marcarea diagnosticelor și procedurilor cu **restricții la internare**; • afișarea **denumirii corespunzătoare codurilor de diagnostic și procedură**. **2. Cerințe privind accesul și utilizarea** • soluția trebuie să fie disponibilă **online**, accesibilă prin browser web; • accesul utilizatorilor trebuie realizat pe bază de **autentificare securizată**; • aplicația trebuie să permită **importul și prelucrarea datelor provenite din sistemele informatice ale spitalului**. **3. Suport pentru activitatea DRG** Soluția trebuie să ofere suport operațional pentru **responsabilii DRG din cadrul spitalului**, prin: • generarea automată de **rapoarte și statistici privind activitatea spitalului**; • facilitarea analizei performanței secțiilor și a medicilor; • suport pentru verificarea și optimizarea **raportărilor DRG**. **4. Servicii incluse** Furnizorul va asigura cel puțin următoarele servicii: • acces la aplicația software de tip **WebGrouper sau echivalent** pe perioada contractului; • actualizarea aplicației în funcție de modificările legislative și metodologice ale sistemului DRG; • suport tehnic pentru utilizatori.

	5. Condiții de echivalență Orice soluție software ofertată va fi considerată **echivalentă** dacă îndeplinește **toate cerințele funcționale și tehnice minime prevăzute în prezentul caiet de sarcini** și permite realizarea clasificării cazurilor medicale conform sistemului DRG utilizat în sistemul sanitar din România. 6. Furnizorul soluției informatice **de tip WebGrouper sau echivalent** va asigura, fără costuri suplimentare, următoarele servicii de suport și instruire pentru personalul spitalului: **6.1. Instruirea utilizatorilor** Furnizorul va organiza sesiuni de instruire pentru personalul medical și personalul implicat în activitatea de raportare DRG, care vor include: • instruire privind **utilizarea aplicației informatice pentru clasificarea cazurilor medicale**; • cursuri privind **codificarea medicală și raportarea cazurilor de spitalizare continuă (cazuri acute)**; • prezentarea și analiza unor **exemple practice din patologia specifică a spitalului**, în vederea îmbunătățirii acurateței codificării și raportării. Sesiunile de instruire vor putea fi organizate: • **în plen** sau **pe secții**, în funcție de necesitățile spitalului; • la solicitarea autorității contractante, cu o frecvență de **maximum o întâlnire la sediul spitalului pe lună**. **6.2. Suport tehnic și consultanță** Furnizorul va asigura **suport telefonic pentru personalul spitalului** în vederea clarificării problemelor legate de utilizarea aplicației și de raportarea medicală a cazurilor de spitalizare continuă. Suportul tehnic va fi disponibil: • în **zilele lucrătoare**; • în intervalul orar **08:00 – 16:00**. **6.3. Analiza codificării medicale** La solicitarea autorității contractante, furnizorul va realiza **analize ale datelor medicale raportate de spital**, în scopul identificării situațiilor de: • **subcodificare**; • **supracodificare**. Analizele vor fi efectuate pe baza **bazei de date a spitalului**, iar frecvența realizării acestora va fi stabilită **de comun acord între autoritatea contractantă și furnizor**. **6.4. Expertiză și consultanță de specialitate** Pentru realizarea activităților menționate, furnizorul va pune la dispoziția autorității contractante **personal specializat (analiști și consultanți în domeniul codificării medicale și al finanțării DRG)**, care va asigura suport metodologic și consultanță în vederea optimizării raportării cazurilor și a indicatorilor de activitate ai spitalului. Experții implicați trebuie să dețină **experiență relevantă în domeniul sistemului DRG, al managementului sanitar sau al codificării medicale**, precum și experiență în activități de instruire și analiză a datelor medicale la nivelul unităților sanitare. **Expertiză și consultanță de specialitate** Furnizorul va asigura, pe perioada derulării contractului, suport de specialitate prin intermediul unei **echipe multidisciplinare de**

	experți (medici, specialiști în management sanitar, analiști de date medicale sau specialiști în codificare medicală), cu experiență relevantă în domeniul **finanțării spitalelor prin sistemul DRG și al codificării medicale**. Experții implicați trebuie să îndeplinească cel puțin următoarele condiții: • experiență profesională relevantă în **codificarea medicală, management sanitar, statistică medicală sau finanțarea spitalelor prin sistemul DRG**; • participare la **proiecte, analize sau activități de consultanță** privind implementarea sau utilizarea sistemului DRG în unități sanitare; • experiență în **activități de instruire, analiză și verificare a datelor medicale raportate de spitale**. Echipa de experți va putea include specialiști care au participat la proiecte naționale sau internaționale privind: • dezvoltarea metodologiilor de finanțare a spitalelor prin sistemul DRG; • analize privind costurile la nivel de caz și recalcularea valorilor grupelor DRG; • activități de instruire și consultanță pentru unități sanitare în domeniul codificării medicale și al finanțării DRG. Experții furnizorului trebuie să aibă **experiență în colaborarea cu unități sanitare**, inclusiv spitale clinice, județene, municipale sau orășenești, pentru: • instruire în domeniul codificării medicale; • suport în raportarea cazurilor DRG; • verificări și analize privind acuratețea codificării; • analize privind subcodificarea sau supracodificarea cazurilor medicale. Ofertantul trebuie să dispună de o echipă de specialiști cu experiență relevantă în domeniul **codificării medicale, managementului sanitar, statisticii medicale sau finanțării spitalelor prin sistemul DRG**. În acest sens, ofertantul va prezenta: • **lista experților propuși pentru implementarea contractului**; • **curriculum vitae (CV)** pentru fiecare expert; **documente justificative privind studiile și calificările profesionale** (diplome de studii, certificate de absolvire, etc.). 7. **Cerințe privind funcționarea aplicației** Aplicația informatică de tip **WebGrouper sau echivalent** trebuie să îndeplinească următoarele cerințe: • să poată fi utilizată **24 de ore din 24, 7 zile din 7**, prin intermediul internetului; • să permită utilizarea simultană de pe **un număr nelimitat de calculatoare din cadrul spitalului**, conectate la internet; • furnizorul trebuie să asigure **actualizarea aplicației** în cazul modificării legislației sau a metodologiei privind sistemul de finanțare DRG, într-un termen rezonabil de la intrarea în vigoare a modificărilor. **8. Protecția datelor** Pentru protecția datelor cu caracter personal ale pacienților, soluția informatică trebuie să permită **anonimizarea datelor**

	personale din baza de date utilizată pentru analize, inclusiv prin conversia sau eliminarea identificatorilor personali (de exemplu CNP), astfel încât datele utilizate pentru analiză să nu permită identificarea directă a pacienților. Pentru soluția software de tip **WebGrouper sau echivalent**, ofertantul va prezenta: • **Descrierea tehnică a aplicației informatice**, care să evidențieze modul în care sunt îndeplinite cerințele funcționale din caietul de sarcini; • **Documentație tehnică sau materiale de prezentare** ale aplicației; • **Declarație privind asigurarea actualizării aplicației** în cazul modificărilor legislative sau metodologice ale sistemului DRG; • **Declarație privind asigurarea suportului tehnic și a serviciilor de instruire** pentru utilizatorii din cadrul spitalului.
LOT 2 – Servicii statistică medicală	**Platformă de analiză statistică medicală pentru management spitalicesc** **1. Cerințe generale privind sistemul** Sistemul informatic trebuie să fie o **aplicație online (web-based)** destinată analizei și raportării statisticilor medicale la nivelul unităților sanitare. Platforma trebuie să permită **acces securizat prin internet**, fără instalarea de aplicații suplimentare pe stațiile utilizatorilor. Sistemul trebuie să funcționeze pe principalele browsere web: Google Chrome; Microsoft Edge; Mozilla Firefox; Safari; Opera. Soluția trebuie să fie compatibilă cu sisteme de operare **Windows, macOS sau alte sisteme care permit utilizarea browserelor web moderne**. Platforma trebuie să fie disponibilă **24/7**, cu mecanisme de backup și securitate a datelor. **2. Managementul utilizatorilor și controlul accesului** Sistemul trebuie să permită **gestionarea rolurilor și drepturilor de acces diferențiate**, cel puțin pentru următoarele categorii de utilizatori: managementul spitalului (manager, director medical, comitet director); șefi de secție / compartiment; personal statistică / informatică; administratori ai sistemului. Platforma trebuie să permită: acces la date **la nivel de spital** pentru managementul central; acces **restricționat la nivel de secție / compartiment** pentru șefii de secție. Sistemul trebuie să permită **autentificare securizată a utilizatorilor**. **3. Funcționalități de analiză statistică** Platforma trebuie să permită generarea și vizualizarea de **statistici medicale personalizate**, inclusiv: 1. Analize statistice la nivel: spital; secție / compartiment. 2. Analize comparative pe: luni; trimester; ani; perioade selectabile de utilizator. 3. Posibilitatea realizării de **analize comparative între perioade diferite**. 4. Posibilitatea configurării parametrilor statistici analizați. **4. Indicatori statistici medicali** Sistemul trebuie să permită analiza și raportarea cel puțin a

	următorilor indicatori: număr cazuri externate (acute / cronice); cazuri validate; cazuri invalidate; cazuri ponderate (CP); indice case-mix (ICM); durata medie de spitalizare (DMS) Soluția trebuie să permită **extinderea setului de indicatori**, în funcție de: modificări legislative; cerințe ale managementului spitalului; schimbări în sistemul de finanțare a serviciilor medicale. **5. Monitorizarea performanței manageriale** Sistemul trebuie să permită utilizarea indicatorilor statistici pentru: 1. monitorizarea **contractului de management al managerului spitalului** 2. monitorizarea **contractelor de administrare ale șefilor de secție** 3. analiza indicatorilor în raport cu: valorile contractate; valorile planificate; valorile realizate. **6. Vizualizare și raportare** Platforma trebuie să permită: 1. vizualizarea datelor statistice sub formă de: tabele; grafice; rapoarte sintetice. 2. exportul datelor în formate standard: **Microsoft Excel; PDF.** 3. generarea de rapoarte pentru: managementul spitalului; șefii de secție; compartimentul de statistică. **7. Gestionarea și încărcarea datelor** 1. Sistemul trebuie să permită **importul datelor statistice anonimizate**. 2. Încărcarea datelor trebuie să poată fi realizată: de către personalul spitalului; de către furnizorul soluției, dacă este cazul. 3. Platforma trebuie să permită **actualizarea periodică a bazei de date statistice**. **8. Securitatea și protecția datelor** 1. Sistemul trebuie să asigure **anonimizarea datelor medicale**. 2. Platforma trebuie să respecte cerințele privind **protecția datelor cu caracter personal (GDPR)**. 3. Sistemul trebuie să asigure: loguri de acces; protecție la acces neautorizat; backup periodic al datelor. **9. Documente ce trebuie prezentate de ofertanți** **1. Propunerea tehnică** Ofertantul va prezenta o **propunere tehnică detaliată**, care va include cel puțin: 1. Descrierea generală a soluției informatice ofertate. 2. Arhitectura sistemului și modul de funcționare al platformei. 3. Descrierea modulelor și funcționalităților sistemului. 4. Modul de gestionare a utilizatorilor și a drepturilor de acces. 5. Descrierea mecanismelor de analiză statistică și raportare. 6. Modalitatea de generare a rapoartelor și exportului de date. 7. Descrierea mecanismelor de securitate și protecție a datelor. 8. Modalitatea de actualizare și mentenanță a aplicației. Propunerea tehnică trebuie să demonstreze **conformitatea cu**

	toate cerințele din caietul de sarcini. **2. Document privind specificațiile tehnice ale soluției** Ofertantul va prezenta documentația tehnică a aplicației, care trebuie să includă: • cerințele hardware și software necesare funcționării sistemului; • compatibilitatea cu sisteme de operare și browsere web; • modul de implementare a funcționalităților statistice; • indicatorii statistici medicali care pot fi analizați; • posibilitățile de configurare și personalizare a sistemului. **3. Document privind securitatea datelor** Ofertantul va prezenta un document care să descrie: • măsurile de securitate implementate în sistem; • mecanismele de protecție a datelor cu caracter personal; • conformitatea cu cerințele **Regulamentului (UE) 2016/679 (GDPR);** • procedurile de backup și recuperare a datelor. **4. Document privind implementarea soluției** Ofertantul va prezenta un **plan de implementare**, care trebuie să includă: • etapele implementării sistemului; • durata estimată pentru instalare și configurare; • activitățile de testare și punere în funcțiune; • activitățile de instruire a personalului utilizator. **5. Document privind suportul tehnic și mentenanța** Ofertantul va prezenta informații privind: • serviciile de suport tehnic oferite; • programul de suport (ex.: zile lucrătoare, interval orar); • modalitățile de contact pentru suport (telefon, email, platformă online); • timpul de răspuns pentru rezolvarea incidentelor; • serviciile de mentenanță și actualizare software. **6. Declarație privind dreptul de utilizare a soluției software** Ofertantul va prezenta o declarație pe propria răspundere privind: • dreptul legal de comercializare a soluției software ofertate; • drepturile de licențiere și utilizare ale aplicației; • faptul că soluția nu încalcă drepturi de proprietate intelectuală. **7. Materiale demonstrative ale soluției** Ofertantul va prezenta, după caz: • capturi de ecran ale aplicației; • broșuri sau documentații ale produsului; • acces demonstrativ la platformă sau prezentare demonstrativă. **8. Alte documente** Ofertantul poate prezenta, dacă este cazul: • manualul de utilizare al aplicației; • certificări relevante ale produsului sau companiei; • alte documente care demonstrează performanța soluției.
LOT 3 – Servicii securitate cibernetică	**Servicii de securitate cibernetică** **1. Cerințe generale privind serviciile** 1. Operatorul economic trebuie să furnizeze servicii specializate de securitate cibernetică destinate protejării sistemelor informatice care susțin activitatea medicală.

	2. Serviciile trebuie să fie furnizate în conformitate cu legislația rațională și europeană aplicabilă, inclusiv cerințele privind securitatea rețelelor și sistemelor informatice și obligațiile operatorilor de servicii esențiale. 3. Prestatorul trebuie să dispună de un **Centru de Operațiuni de Securitate Cibernetică (SOC)** operațional pentru monitorizarea și gestionarea incidentelor de securitate. 4. Serviciile trebuie să includă activități de identificare, analiză, monitorizare și remediere a vulnerabilităților sistemelor informatice. 5. Prestatorul trebuie să asigure suport pentru respectarea cerințelor legislative privind securitatea cibernetică și raportarea incidentelor către autoritățile competente. 6. Serviciile trebuie să fie furnizate de personal specializat în securitate cibernetică. **2. Servicii obligatorii** **2.1 Consultanță privind cadrul legislativ (NIS)** Prestatorul trebuie să asigure servicii de consultanță privind obligațiile legislative în domeniul securității cibernetice, care să includă cel puțin: 1. Consultanță privind cadrul legislativ și obligațiile rezultate din actele normative aplicabile securității rețelelor și sistemelor informatice. 2. Relaționarea cu autoritatea națională competentă în domeniul securității cibernetice. 3. Sprijin pentru notificarea incidentelor de securitate către autoritățile competente, conform legislației în vigoare. 4. Elaborarea de rapoarte semestriale sau anuale privind: managementul activelor IT, vulnerabilitățile identificate, incidentele de securitate. 5. Asistență în cazul evaluărilor efectuate de autoritățile competente. 6. Participarea unui expert al prestatorului la eventualele controale realizate de autorități, pentru demonstrarea respectării cerințelor legale. **Disponibilitate** • serviciul trebuie să fie disponibil permanent; • activitățile trebuie realizate la termenele prevăzute de legislația aplicabilă. **2.2 Managementul activelor IT și al sistemelor informatice** Prestatorul trebuie să furnizeze servicii de **inventory management** pentru infrastructura IT a beneficiarului, care să includă: 1. Identificarea și menținerea unui inventar actualizat al activelor IT. 2. Detectarea activelor IT operaționale și a sistemelor de operare instalate în rețea. 3. Identificarea și monitorizarea evoluției activelor informatice în timp. 4. Generarea de rapoarte periodice privind inventarul activelor informatice. 5. Furnizarea a cel puțin două rapoarte lunare generate de aplicația de scanare utilizată. **Disponibilitate**

	• realizarea inventarului inițial; • efectuarea a minimum **două scanări lunare**; • program de lucru: **luni – vineri, interval 09:00 – 17:00.** **2.3 Managementul vulnerabilităților** Prestatorul trebuie să asigure servicii de identificare și gestionare a vulnerabilităților sistemelor informatice, care să includă: 1. Scanarea periodică a vulnerabilităților sistemelor informatice. 2. Scanarea internă periodică a vulnerabilităților din rețeaua internă. 3. Scanarea vulnerabilităților pentru: adrese IP, aplicații web, sisteme informatice definite de beneficiar. 4. Realizarea scanărilor atât în mod autentificat, cât și neautentificat. 5. Clasificarea activelor din punct de vedere tehnic în: corespunzătoare, necorespunzătoare, pe baza unor reguli predefinite (liste albe, liste negre etc.). 6. Elaborarea de recomandări tehnice pentru remedierea vulnerabilităților identificate. 7. Transmiterea rezultatelor scanărilor sub forma unor rapoarte tehnice generate de soluțiile utilizate. 8. Includerea măsurilor de remediere în rapoartele lunare. 9. Notificarea urgentă a beneficiarului în cazul identificării unor vulnerabilități critice care pot afecta funcționarea sistemelor informatice. **Program de furnizare** • luni – vineri, 09:00 – 17:00; • inventar inițial și minimum două scanări lunare. **2.4 Servicii de coordonare a răspunsului la incidente (SOC – nivel L2)** Prestatorul trebuie să furnizeze servicii de monitorizare și răspuns la incidente de securitate cibernetică, care să includă: 1. Colectarea și agregarea evenimentelor de securitate provenite de la echipamente și aplicații informatice. 2. Corelarea și analiza evenimentelor pentru identificarea incidentelor de securitate. 3. Alertarea beneficiarului în cazul detectării incidentelor de securitate. 4. Deschiderea de tichete în platforma de management al incidentelor. 5. Păstrarea arhivei corespondenței și documentației aferente fiecărui incident. 6. Coordonarea activităților de răspuns la incidentele detectate. 7. Elaborarea de recomandări pentru îmbunătățirea procedurilor de prevenire a incidentelor. 8. Analiza cauzei rădăcină (root cause analysis) pentru incidentele identificate. 9. Păstrarea logurilor pe termen lung, în format prelucrat. 10. Elaborarea unui raport lunar privind evoluția alertelor și incidentelor de securitate. **Disponibilitate** • luni – vineri, interval **09:00 – 17:00.** **Volum minim** • gestionarea a până la **150 incidente de securitate pe lună.**

3. Cerințe privind implementarea serviciilor

1. Implementarea și configurarea soluțiilor de securitate cibernetică trebuie realizată exclusiv de personal specializat al prestatorului sau de parteneri autorizați.
2. Implementarea se va realiza în conformitate cu procedurile de securitate stabilite împreună cu beneficiarul.

4. Cerințe privind accesul și colaborarea

Beneficiarul trebuie să permită prestatorului:

1. accesul personalului autorizat la infrastructura IT;
2. accesul la sistemele informatice proprii sau operate de alți furnizori IT;
3. accesul la sursele de date relevante pentru securitate.

Sursele de date trebuie să includă cel puțin:

- Active Directory;
- firewall;
- servere proxy;
- sisteme antivirus / endpoint;
- sisteme DLP;
- sisteme IDS/IPS;
- alte echipamente sau aplicații relevante pentru securitate.

5. Cerințe privind conectivitatea

Beneficiarul trebuie să asigure:

1. conectivitatea necesară pentru accesul la distanță al prestatorului;
2. conturi de acces pentru sistemele și aplicațiile incluse în contract;
3. acces la echipamentele și aplicațiile gestionate de alți furnizori IT.

6. Cerințe privind suportul tehnic

Prestatorul trebuie să asigure suport tehnic prin următoarele canale: suport telefonic; suport prin email; suport prin platformă de analiză și alertare; suport on-site, la solicitarea beneficiarului.
Call center-ul trebuie să reprezinte punctul unic de contact între utilizatorii beneficiarului și prestator.

7. Clasificarea incidentelor de securitate

Prestatorul trebuie să clasifice incidentele în funcție de gravitate:
incident major - incident care împiedică funcționarea corespunzătoare a sistemului informatic (ex.: atac ransomware).
incident mediu - incident care permite funcționarea sistemului, dar afectează parțial serviciile.
incident minor - incident care nu afectează major funcționarea sistemului, dar poate genera dificultăți de exploatare.

8. Timpi de răspuns

Prestatorul trebuie să respecte următorii timpi de răspuns:
pentru preluarea incidentelor

- incident major: **1 oră**
- incident mediu: **4 ore**
- incident minor: **24 ore**

pentru diagnosticare și coordonarea răspunsului

- incident major: **5 ore**
- incident mediu: **10 ore**
- incident minor: **48 ore**
- alte probleme: **ASAP**

9. Tipuri de intervenție

Prestatorul trebuie să poată realiza intervenții:

	• **remote (off-site)** • **la locația beneficiarului (on-site)** Tipul intervenției va fi stabilit în funcție de gravitatea și complexitatea incidentului. În vederea demonstrării îndeplinirii cerințelor tehnice prevăzute în prezentul caiet de sarcini, ofertanții vor prezenta în cadrul propunerii tehnice documente justificative relevante, care să permită verificarea conformității soluției ofertate. În acest sens, ofertanții vor prezenta cel puțin următoarele: • **broșuri, fișe tehnice (datasheet-uri), manuale de utilizare, documentații tehnice ale producătorilor sau alte documente oficiale** din care să rezulte caracteristicile tehnice ale soluțiilor utilizate pentru furnizarea serviciilor; • **descrieri tehnice detaliate ale serviciilor ofertate**, din care să rezulte modul de îndeplinire a fiecărei cerințe tehnice prevăzute în caietul de sarcini; • **metodologii și proceduri de lucru** utilizate pentru furnizarea serviciilor de securitate cibernetică (ex.: managementul vulnerabilităților, monitorizarea evenimentelor de securitate, gestionarea incidentelor); • **modele sau exemple de rapoarte tehnice** care vor fi furnizate beneficiarului pe parcursul derulării contractului; • **documente privind infrastructura tehnică utilizată**, inclusiv descrierea platformelor și instrumentelor utilizate pentru monitorizarea și analiza incidentelor de securitate. **Documente privind personalul de specialitate** Pentru demonstrarea capacității de furnizare a serviciilor, ofertanții vor prezenta documente privind personalul de specialitate propus pentru implementarea contractului, respectiv: • **CV-urile experților propuși**; • **copii ale diplomelor de studii** care atestă pregătirea în domenii relevante (IT, securitate informatică, automatică, electronică sau domenii conexe); • **certificate sau certificări profesionale relevante** în domeniul securității cibernetice sau al administrării sistemelor informatice. **Cerințe privind documentele prezentate** Documentele tehnice prezentate trebuie să permită **identificarea clară a corespondenței dintre cerințele caietului de sarcini și caracteristicile soluției ofertate**. Autoritatea contractantă își rezervă dreptul de a solicita clarificări sau documente suplimentare pentru verificarea conformității tehnice. În cazul în care documentele prezentate nu demonstrează în mod clar îndeplinirea cerințelor tehnice, **oferta poate fi considerată neconformă**.

Capitolul 4. Servicii de suport tehnic pe durata contractului

Pe toată durata contractului, prestatorul va asigura suport tehnic pentru soluțiile informatice furnizate (aplicația pentru clasificarea cazurilor DRG, platforma de analiză statistică medicală și serviciile de securitate cibernetică), în vederea asigurării funcționării continue și corespunzătoare a sistemelor informatice utilizate în cadrul spitalului.

Suportul tehnic va acoperi atât aspectele legate de funcționarea aplicațiilor informatice, cât și asistența

acordată utilizatorilor pentru utilizarea corectă a acestora și pentru gestionarea incidentelor de securitate cibernetică.

4.1. Punct de contact pentru suport tehnic

Prestatorul va asigura un punct unic de contact (help-desk / call-center) dedicat personalului autorizat al Autorității Contractante, prin intermediul căruia pot fi semnalate incidente, solicitări de suport sau probleme privind funcționarea aplicațiilor informatice.

Suportul tehnic va fi disponibil:

- în zilele lucrătoare, de luni până vineri;
- în intervalul orar **08:00 – 16:00** pentru suport privind utilizarea aplicațiilor informatice și raportarea DRG;
- în intervalul **09:00 – 17:00** pentru activitățile aferente securității cibernetice și monitorizării infrastructurii IT.

Solicitările de suport vor putea fi transmise prin:

- telefon;
- e-mail;
- platformă online / sistem de ticketing;
- alte mijloace de comunicare stabilite între părți.

Prestatorul va înregistra toate solicitările primite și va urmări soluționarea acestora până la rezolvarea finală.

4.2. Clasificarea incidentelor

Incidentele raportate vor fi clasificate în funcție de impactul asupra funcționării sistemelor informatice și asupra activității spitalului.

Nivelurile de prioritate sunt:

Incident major - Incident care împiedică funcționarea corespunzătoare a aplicațiilor informatice sau a sistemelor informatice ale spitalului (ex.: indisponibilitatea aplicației DRG, atac cibernetic, blocarea sistemului informatic).

Incident mediu - Incident care permite funcționarea sistemului, dar afectează parțial anumite funcționalități sau servicii.

Incident minor - Incident cu impact redus asupra funcționării sistemului informatic sau al aplicațiilor utilizate.

Clasificarea incidentelor se va realiza în cadrul sistemului de management al incidentelor utilizat de prestator.

4.3. Timpi de răspuns pentru incidente

Prestatorul trebuie să respecte următorii timpi maximi de răspuns:

Pentru preluarea incidentelor

Nivel incident	Timp de răspuns
Incident major	maximum 1 oră
Incident mediu	maximum 4 ore
Incident minor	maximum 24 ore

Pentru diagnosticare și coordonarea răspunsului

Nivel incident	Timp de diagnosticare
Incident major	maximum 5 ore
Incident mediu	maximum 10 ore
Incident minor	maximum 48 ore

Prin timp de răspuns se înțelege intervalul dintre momentul raportării incidentului de către beneficiar și confirmarea preluării acestuia de către prestator.

4. 4. Activități incluse în suportul tehnic

Serviciile de suport tehnic trebuie să includă cel puțin următoarele activități:

- asistență pentru utilizarea aplicației de clasificare a cazurilor medicale DRG;
- suport pentru utilizarea platformei de analiză statistică medicală;
- suport pentru importul și analiza datelor medicale;
- suport pentru utilizarea indicatorilor statistici medicali și generarea rapoartelor;
- suport tehnic pentru personalul spitalului privind raportarea DRG;
- intervenții pentru remedierea incidentelor tehnice;
- suport pentru gestionarea incidentelor de securitate cibernetică;
- actualizarea aplicațiilor informatice în cazul modificărilor legislative sau metodologice aplicabile sistemului DRG;
- consultanță tehnică pentru optimizarea funcționării sistemelor informatice.

4.5. Modalități de intervenție

Prestatorul trebuie să asigure intervenții pentru rezolvarea incidentelor prin:

- intervenții **remote (off-site)**;
- intervenții **on-site**, la sediul beneficiarului, atunci când natura incidentului impune acest lucru.

Tipul intervenției va fi stabilit în funcție de gravitatea și complexitatea incidentului.

4.6. Raportarea activităților de suport

Prestatorul va transmite periodic beneficiarului rapoarte privind activitatea de suport tehnic, care vor include cel puțin:

- numărul incidentelor înregistrate;
- tipul și nivelul de severitate al incidentelor;
- timpul de răspuns și timpul de rezolvare;
- măsurile de remediere aplicate;
- recomandări pentru prevenirea incidentelor viitoare.

4.7. Continuitatea funcționării sistemelor

Prestatorul va asigura suport tehnic astfel încât:

- aplicațiile informatice să fie disponibile permanent pentru utilizatorii autorizați ai spitalului;
- eventualele incidente să fie remediate într-un termen rezonabil;
- securitatea și integritatea datelor medicale să fie menținute.

4.8. Garanția serviciilor și a aplicațiilor informatice

- Prestatorul garantează funcționarea corespunzătoare a aplicațiilor informatice și a serviciilor

furnizate pe întreaga durată de derulare a contractului.

- În perioada contractuală, prestatorul are obligația de a remedia, fără costuri suplimentare pentru Autoritatea Contractantă, orice erori de funcționare, deficiențe tehnice sau vulnerabilități ale aplicațiilor informatice furnizate, care sunt imputabile soluției software sau serviciilor prestate.
- Remedierea erorilor și a incidentelor tehnice se va realiza cu respectarea timpilor de răspuns și de intervenție prevăzuți în prezentul caiet de sarcini.
- Actualizările software necesare pentru corectarea erorilor, îmbunătățirea funcționalităților sau conformarea cu modificările legislative aplicabile vor fi realizate de prestator fără costuri suplimentare pe durata contractului.

4.9. Calendar de implementare a serviciilor

Implementarea serviciilor aferente fiecărui lot se va realiza în baza unui **ordin de începere emis de Autoritatea Contractantă**, în termenele prevăzute mai jos.

Prestatorul va asigura toate activitățile necesare configurării, testării și punerii în funcțiune a soluțiilor informatice, astfel încât acestea să poată fi utilizate în condiții operaționale de către personalul spitalului.

LOT 1 – Servicii informatice pentru clasificarea cazurilor medicale DRG
Durata estimată de implementare: **maximum 10 zile lucrătoare de la data ordinului de începere.**
Etapele implementării
Etapa 1 – Inițierea proiectului și analiza cerințelor (Zilele 1–2)
- organizarea întâlnirii de lansare a proiectului;
- stabilirea persoanelor de contact și a fluxului de comunicare;
- analiza modului de preluare a datelor din sistemele informatice ale spitalului.

Etapa 2 – Configurarea aplicației (Zilele 3–6)
- configurarea aplicației informatice pentru clasificarea DRG;
- configurarea conturilor de utilizator și a drepturilor de acces;
- configurarea parametrilor de analiză și clasificare.

Etapa 3 – Testarea funcționalităților (Zilele 7–8)
- testarea clasificării cazurilor medicale;
- verificarea generării indicatorilor statistici;
- remedierea eventualelor neconformități.

Etapa 4 – Instruirea utilizatorilor și punerea în funcțiune (Zilele 9–10)
- instruirea personalului medical și a responsabililor DRG;
- punerea în funcțiune a aplicației și validarea funcționării acesteia.

LOT 2 – Platformă de analiză statistică medicală
Durata estimată de implementare: **maximum 10 zile lucrătoare de la data ordinului de începere.**
Etapele implementării
Etapa 1 – Analiza cerințelor și planificarea implementării (Zilele 1–2)
- întâlnirea de lansare a proiectului;
- stabilirea indicatorilor statistici și a surselor de date.

Etapa 2 – Configurarea platformei (Zilele 3–6)
- configurarea platformei informatice;
- configurarea rolurilor și drepturilor de acces;
- configurarea indicatorilor statistici și a mecanismelor de analiză.

Etapa 3 – Testarea sistemului (Zilele 7–8)
- testarea generării rapoartelor și a indicatorilor statistici;
- verificarea exportului de date și a funcționării sistemului.

Etapa 4 – Instruirea utilizatorilor și punerea în funcțiune (Zilele 9–10)
- instruirea personalului din management și din compartimentul de statistică;
- punerea în funcțiune a platformei.

LOT 3 – Servicii de securitate cibernetică
Durata estimată de implementare: **maximum 15 zile lucrătoare de la data ordinului de începere.**
Etapele implementării
Etapa 1 – Evaluarea infrastructurii IT (Zilele 1–4)
- inventarierea infrastructurii IT;
- identificarea sistemelor și aplicațiilor relevante pentru securitate.

Etapa 2 – Configurarea serviciilor de securitate (Zilele 5–10)
- configurarea sistemelor de monitorizare și analiză a evenimentelor;
- integrarea surselor de loguri și a echipamentelor IT.

Etapa 3 – Testarea mecanismelor de securitate (Zilele 11–13)
- testarea detectării incidentelor;
- testarea scanărilor de vulnerabilități și a mecanismelor de alertare.

Etapa 4 – Operaționalizarea serviciilor (Zilele 14–15)
- activarea serviciilor de monitorizare;
- predarea documentației tehnice și prezentarea procedurilor de intervenție.

Capitolul 5. Receptia serviciilor

Recepția serviciilor prestate în cadrul contractului se va realiza de către Autoritatea Contractantă pe baza verificării îndeplinirii obligațiilor asumate de prestator și a documentelor justificative prezentate de acesta.

5.1. Modalitatea de recepție

Recepția serviciilor se va realiza periodic, de regulă lunar, pe baza raportului de activitate transmis de prestator și a verificării serviciilor efectiv prestate.

Raportul de activitate va fi transmis Autorității Contractante până cel târziu la data de 5 a lunii următoare perioadei pentru care au fost prestate serviciile.

Raportul va include cel puțin următoarele informații:

- descrierea serviciilor prestate în perioada de raportare;
- activitățile de suport tehnic realizate;
- incidentele tehnice sau de securitate gestionate;
- timpii de răspuns și de remediere a incidentelor;
- actualizările software implementate;
- activitățile de analiză, monitorizare și consultanță efectuate;
- rapoartele tehnice generate de aplicațiile utilizate, după caz.

Autoritatea Contractantă va verifica conformitatea serviciilor prestate cu cerințele prevăzute în caietul de sarcini și cu prevederile contractuale.

5.2. Verificarea serviciilor

Recepția serviciilor va avea în vedere, fără a se limita la acestea, următoarele elemente:

- funcționarea corespunzătoare a aplicației informatice pentru clasificarea cazurilor medicale DRG;
- funcționarea platformei de analiză statistică medicală și generarea indicatorilor statistici solicitați;
- realizarea activităților de suport tehnic pentru utilizatori;
- efectuarea analizelor și verificărilor privind codificarea medicală și raportarea DRG;
- realizarea activităților de monitorizare și gestionare a incidentelor de securitate cibernetică;
- transmiterea rapoartelor tehnice și a recomandărilor privind securitatea sistemelor informatice.

În cazul în care serviciile prestate corespund cerințelor stabilite, Autoritatea Contractantă va emite documentul de recepție a serviciilor pentru perioada respectivă.

5.3. Neconformități

În cazul în care, în urma verificării, se constată neconformități în prestarea serviciilor, Autoritatea Contractantă va notifica prestatorul în scris.

Prestatorul are obligația de a remedia neconformitățile constatate într-un termen rezonabil stabilit de comun acord cu Autoritatea Contractantă.

Recepția serviciilor se va realiza numai după remedierea neconformităților identificate.

5.4. Documente aferente recepției

Recepția serviciilor se va realiza pe baza următoarelor documente:

- raportul de activitate transmis de prestator;
- rapoartele tehnice generate de sistemele informatice sau de platformele de monitorizare;
- documente justificative privind intervențiile efectuate (ticket-uri, rapoarte de incident, rapoarte de analiză);
- procesul-verbal de recepție a serviciilor.

5.5. Facturarea serviciilor

Prestatorul va emite factura aferentă serviciilor prestate după aprobarea raportului de activitate și efectuarea recepției serviciilor de către Autoritatea Contractantă.

Factura va fi însoțită de raportul de activitate și de documentele justificative aferente serviciilor prestate în perioada respectivă.

Intocmit,

Lukács Zoltan – Sef serviciu Runos - în calitate de membru

Tifán László -inginer de sisitem - în calitate de membru