

Románia egészségügyben alkalmazott kriptográfiai megoldásai

Cryptographic solutions used in Romania's healthcare sector

Dr. MÁRTON Gyöngyvér
adjunktus

EMTE-Sapientia Műszaki és Humán tudományok Kar, Marosvásárhely
540485 Corunca / Tg. Mureș, Calea Sighișoarei nr. 2
tel.: +40 265 208 170, fax.: +40 265 206211
mgyongyi@ms.sapientia.ro

Abstract

According to the latest research, the healthcare sector faces new challenges in the digital age. This article provides a comprehensive analysis of trends and challenges within the healthcare sector. We present cryptographic techniques used for privacy-preserving computation -- a topic situated at the intersection of two rapidly evolving fields: healthcare digitalization and applied cryptography, and finally we outline the solutions used in the Romanian healthcare sector.

Keywords: healthcare, cryptography, privacy-preserving computation, cryptographic solutions, Romania healthcare sector

Kivonat

Digitális korunkban a legújabb kutatások szerint az egészségügyi ágazat új kihívásokkal néz szembe. Jelen cikk átfogó elemzést nyújt az egészségügyi szektor trendjeiről és kihívásairól. Bemutatjuk az adatvédelmet biztosító számításokhoz alkalmazott kriptográfiai technikákat – egy olyan témakört, amely két gyorsan fejlődő terület, az egészségügyi digitalizáció és az alkalmazott kriptográfia metszéspontjában helyezkedik el –, végül pedig ismertetjük a romániai egészségügyi ágazatban alkalmazott megoldásokat.

Kulcsszavak: egészségügy, kriptográfia, adatvédelmi szempontok, Románia egészségügyi ágazata

1. BEVEZETŐ FOGALMAK

A digitális átalakulás korában az egészségügyi ágazat összetett kihívások és lehetőségek középpontjában áll. Egyre nagyobb az igény a pontos diagnózisok, a személyre szabott kezelések és a színvonalasabb betegellátás iránt. Ennek következtében az ágazat új kihívásokkal néz szembe. Megállapítható, hogy a mesterséges intelligencia, a kiberbiztonság és az egészségügyi szektor közötti ellentmondások és összefüggések átfomálják az orvosi beavatkozásokról és a betegellátásról alkotott elképzeléseket, sőt, újra értelmezik az orvosi paradigmákat is, lásd [1].

Az első tisztázandó fogalmak az egészségügyi információs rendszerekhez (Health Information Systems - HIS) kapcsolódnak. Ezek a rendszerek alkotják ugyanis a modern egészségügy digitális infrastruktúráját. Ezek közül három kulcsfontosságú rendszert emelünk ki, lásd [2].

Az első az elektronikus egészségügyi nyilvántartás (Electronic Health Record - EHR). Ezek olyan digitális platformok, amelyek lehetővé teszik a betegek kórtörténetének tárolását, feldolgozását és a különböző egészségügyi intézmények közötti megosztását. Az EHR-rendszerek valós időben összesítik a klinikai, diagnosztikai és adminisztratív adatokat, lehetővé téve, hogy a beteg kórtörténete a különböző szolgáltatók és ellátási környezetek között is követhető maradjon.

A második a Betegportál (Patient Portal - PP). Ez egy biztonságos, webalapú felület, amely közvetlen hozzáférést biztosít a betegek számára saját, védett egészségügyi adataikhoz (Protected Health Information - PHI). A Betegportálok nem csupán a nyilvántartások megtekintését teszik lehetővé, hanem közvetlen kommunikációt is biztosítanak az egészségügyi szolgáltatókkal – például időpontfoglalást, üzenetváltást vagy receptmegújítást is lehetővé tesznek.

A harmadik az orvostechnikai eszközök telemetriája (Medical Device Telemetry - MDT). Ez a biometrikus és működési adatok automatikus, folyamatos továbbítását jelenti a hálózatra kapcsolt orvostechnikai eszközökről – például viselhető eszközökről, beültethető implantátumokról vagy betegség melletti monitorokról – a megfigyelőrendszerek, klinikai műszerfalak vagy felhőalapú elemzőplatformok felé.

Mindhárom rendszer rendkívül érzékeny betegadatokat állít elő, dolgoz fel és továbbít. Amellett, hogy komoly értéket teremtenek az egészségügyi ellátás és kutatás számára, jelentős adatvédelmi és biztonsági kihívásokat is felvetnek. Éppen itt válnak nélkülözhetetlenné a kriptográfiai megoldások, amelyek alkalmazása és implementálása a Romániai egészségügyi rendszerekben is számos problémát vet fel.

2. KRIPTOGRÁFIAI TECHNIKÁK

Az egészségügyben alkalmazott kriptográfiai technikák két párhuzamos igényt elégítenek ki. Az első az alapvető működési biztonság szavatolása. A tárolt adatok védelme klasszikus kriptográfiai primitívek – például titkosítás, hash-elés és digitális aláírás – révén biztosítható, míg az adatátvitel biztonságát kriptográfiai protokollok alkalmazása garantálja. Ezek az eljárások képezik az alapvető biztonsági követelményeket, lásd [3].

A tárolt adatok titkosítását az Advanced Encryption Standard (AES) látja el. Ezt a NIST SP 800-111 szabványnak megfelelően adatbázisok, orvosi képkéntő archívumok és eszközökön lévő helyi adattárak védelmére használják. Az SHA-256 és az SHA-3 kriptográfiai hash-elést biztosít az integritás megőrzése érdekében; ezek segítségével ellenőrizhető például, hogy az orvosi felvételeket vagy a klinikai vizsgálati adatokat nem módosították-e illetéktelenül. A nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI) és a digitális aláírások (Digital Signatures, DS) lehetővé teszik a hitelesítést és a letagadhatatlanságot; ezeket használják többek között elektronikus receptek aláírására, az egészségügyi szolgáltatók jogosultságainak ellenőrzésére, valamint a hálózatra kapcsolt orvosi eszközök firmware-frissítéseinek hitelesítésére.

Az olyan protokollok, mint a TLS 1.3 és az IPsec, az adatátvitel biztonságát szolgálják. Ezeket a NIST SP 800-52 szabvány előírásait követve telemetriai adatfolyamok, klinikák közötti API-kapcsolatok és betegportálok védelmére alkalmazzák.

A második igény, amely jelenleg is aktív kutatási lehetőségekkel bír az adatvédelmi szempontból biztonságos számítási technikák meghatározására, kiválasztására vonatkozik. Ezek olyan megoldások, amelyek lehetővé teszik az olyan szabályozási előírásoknak való megfelelést, mint az európai GDPR vagy az egyesült államokbeli HIPAA. Ezek a technikák új módszereket is magukba foglalnak, lehetővé téve az együttműködésen alapuló kutatást, a mesterségesintelligencia- (MI) modellek betanítását és a hozzáférés-szabályozást anélkül, hogy a nyers betegadatokat bármikor is felfednék.

Az alábbiakban áttekintjük az adatvédelmi szempontból biztonságos számítások alapvető technikáit.

Az első technika, a homomorf titkosítás (HE), amely lehetővé teszi, hogy a számításokat titkosított adatokon végezzük anélkül, hogy azokat előzetesen vissza kellene fejteni. A gyakorlatban ez lehetővé teszi az egészségügyi szolgáltatók számára, hogy elemzéseket és mesterségesintelligencia-modelleket futtassanak közvetlenül a titkosított betegadatokon – anélkül, hogy az információkat bármikor is visszafejtenék. Az adatok a teljes számítási folyamat során védettek maradnak, lásd [4].

A második technika, a nulla-ismeretű bizonyítás (Zero-Knowledge Proof, ZKP), tények ellenőrzésére összpontosít anélkül, hogy felfedné a mögöttes adatokat. A ZKP megoldást kínálja az egészségügy egyik alapvető kihívására: a megfelelés, a jogosultság vagy a személyazonosság ellenőrzésére anélkül, hogy védett egészségügyi adatokat kellene közzétenni, lásd [5].

A biztonságos többszereplős számítás (Secure Multi-Party Computation, SMPC) lehetővé teszi, hogy több egészségügyi intézmény közösen végezzen számításokat – vagy gépi tanulási modelleket tanítson be – összesített adatain úgy, hogy egyik fél sem látja, osztja meg vagy központosítja a tényleges betegadatokat. A technológia alapvető mechanizmusa a titokmegosztáson (secret sharing) alapul; ez egy olyan kriptográfiai eljárás, amely az adatokat több „részre” (share) osztja fel, és szétosztja azokat a résztvevők között. Az egészségügyi alkalmazásokban leggyakrabban Shamir titokmegosztási sémáját használják, lásd [6].

Az attribútum-alapú titkosítás (Attribute-Based Encryption, ABE) lehetővé teszi a betegek és az ellátók számára, hogy pontosan meghatározzák, ki mit tekinthet meg. A módszer olyan attribútumokon alapul, mint a szerepkör, az osztály vagy a kezelési kapcsolat, anélkül, hogy minden egyes egészségügyi szakember számára külön nyilvános kulcsra lenne szükség, lásd [7].

A szövetségi tanulás (Federated Learning, FL) technikája révén több eszköz vagy szerver működik együtt egy közös mesterségesintelligencia-modell betanításában anélkül, hogy a nyers adatokat egyetlen központi helyen egyesítenék. Az egyes kórházak helyben, saját adataik felhasználásával végzik a betanítást; csak a modellfrissítések – például a gradiensok vagy a súlyok – kerülnek megosztásra és összesítésre. Az FL-t gyakran kombinálják HE-vel vagy SMPC-vel a megosztott frissítések védelme érdekében, lásd [8].

A blokklánc – amely elsősorban megváltoztathatatlan, decentralizált főkönyvként funkcionál – hasznos eszköz a személyazonosság-kezelésben, a hozzájárulások nyomon követésében és az auditálási naplók vezetésében. Az egészségügyben engedélyköteles (permissioned) blokkláncokat használnak a hashek és a hozzáférési jogosultságok tárolására, miközben a nyers adatok a blokkláncon kívül maradnak, lásd [9].

Az orvosi dolgok internete (Internet of Medical Things, IoMT) olyan összekapcsolt orvosi eszközök, szoftveralkalmazások és egészségügyi rendszerek ökoszisztémáját jelenti, amelyek az interneten keresztül közvetlenül kapcsolják össze a betegadatokat az egészségügyi informatikai hálózatokkal. Speciális titkosítási módszereket alkalmaznak, mivel az olyan eszközök, mint a szívritmus-szabályozók, az infúziós pumpák és a viselhető monitorok, nem rendelkeznek a nagy teljesítményű titkosítási rendszerek futtatásához szükséges akkumulátor üzemidővel vagy számítási kapacitással. A könnyűsúlyú kriptográfiai (Lightweight Cryptography, LWC) algoritmusok – mint például a NIST által kiválasztott ASCON és a PRINCE – elfogadható szintű biztonságot nyújtanak minimális késleltetés és energiafogyasztás mellett. Ezek a rendszerek 128 bites kulcsokkal ellátott AES-t, a nyilvános kulcsú kriptográfia terén pedig ECC-t alkalmaznak, lásd [10].

A kvantum-ellenálló kriptográfia (Post-Quantum Cryptography PQC) megoldást kínál a „gyűjtsd most, fejtsd vissza később” (harvest now, decrypt later) fenyegetésre, amely ezen új megoldások fejlesztésének egyik fő mozgatórugója. Ez a fenyegetés azt jelenti, hogy a támadók már ma ellopják a titkosított egészségügyi adatokat azzal a szándékkal, hogy azokat akkor fejtsek vissza, amikor a kvantumszámítógépek elérik a megfelelő feldolgozási teljesítményt. A különböző szervezetek a kockázat mérséklése érdekében megpróbálnak áttérni a NIST által szabványosított PQC-re. Az egészségügyi rendszerek azonban jelenleg RSA- és ECC-alapúak; a PQC-re való átállás pedig nem egyszerű feladat, mivel hibrid megvalósításokat, a PKI-infrastruktúra korszerűsítését és a régebbi orvosi eszközök cseréjét igényli. Emellett időbeli korlát is fennáll, mivel a NIST az RSA-2048 és az ECC fokozatos kivezetését javasolja 2030-ig, valamint teljes körű betiltását 2035-ig, lásd [11].

A továbbiakban két táblázatot mutatunk be, amelyek felsorolják az egészségügyi problémákat és a hozzájuk tartozó kriptográfiai megoldásokat, ahol mindkét esetben az utolsó oszlop rövid leírást tartalmaz a megoldások működéséről. Az 1. táblázat klasszikusnak mondható eseteket, míg a 2. táblázat összetettebb egészségügyi problémákat és komplexebb megoldásokat mutat be.

Egészségügyi problémák és kriptográfiai megoldások

1. táblázat

egészségügyi probléma	kriptográfiai megoldás	működési elv	benchmark
betegadatokat tartalmazó laptop vagy USB-meghajtó ellopása	lemeztitkosítás (AES-256)	A teljes tárolóegység titkosítása AES-256 algoritmussal. Ez minden klinikai eszközön szabványos megoldás.	Az AES-256 hardveres gyorsítással ellátott modern processzorokon 2–5 GB/s sebességet ér el.
laboreredmények továbbítása szakorvosnak	TLS + PKI	Biztonságos, titkosított csatornát hoz létre a küldő és a fogadó szerver között. A megbízható tanúsítvány-kibocsátó (CA) által kiállított digitális tanúsítványok (X.509) igazolják a fogadó szerver hitelességét, megakadályozva ezzel a közbeékelődéses (man-in-the-middle) támadásokat.	TLS 1.3 teljes kézfogás (handshake): ~8–9 ms szerveroldalon, ~8–9 ms kliensoldalon; adatmennyiség-többlet (overhead): ~983 bájt;

recept hamisítatlanságának igazolása	Digitális aláírás (RSA / ECDSA)	Az orvos a saját privát kulcsával írja alá az elektronikus receptet. A gyógyszerért az orvos publikus kulcsával ellenőrzi az aláírást. A recept bármilyen módosítása érvényteleníti az aláírást, így biztosítva az adatok sértetlenségét és a letagadhatatlanságot.	RSA aláírás-ellenőrzés: 0,1–10 s közötti időtartam a legrosszabb esetekben; az ECDSA lényegesen gyorsabb (modern hardveren ezredmásodperc alatti időigény)
jogosulatlan hozzáférés betegadatokhoz alkalmazott által	Szerepkör-alapú hozzáférés-szabályozás (RBAC) + ABE	Az adatok titkosítása olyan szabályok alapján történik, amelyek magába a titkosított szövegbe vannak ágyazva (pl. „csak kardiológusok fejthetik vissza”, „ápoló nem fejtheti vissza a pszichiáter feljegyzéseit”)	ABE titkosítási idő: ~0,019 s (HCKP-ABE) vs. 0,048 s (KP-ABE); ABE kulcsméret: 512 bit
orvosi képalkotó felvételek (röntgen, MRI) felhőalapú tárolása	kliensoldali vagy proxy alapú újratitkosítás	Az adatok titkosítása még azelőtt megtörténik, hogy elhagynák a kórház biztonságos környezetét. A felhőszolgáltató csak titkosított szöveget tárol, és soha nem látja a sima szöveges képeket.	Hibrid titkosítás ajánlott: az aszimmetrikus műveletek 240-szer drágábbak, mint a szimmetrikus műveletek; a munkamenetkulcs újrafelhasználása önkényesen csökkentheti a terhelést.

Összetettebb problémák és komplexebb kriptográfiai megoldások

2. táblázat

egészségügyi probléma	kriptográfiai megoldás	működési elv	benchmark
érzékeny adatokon végzett MI-következtetés a felhőben	HE (Homomorf titkosítás)	A betegadatokat titkosítják, mielőtt a felhőbe küldenék őket. A felhőben futó MI-modell közvetlenül a titkosított adatokon végez számításokat, és titkosított eredményt ad vissza.	FHE-számítási időigény: kulcsgenerálás 15 ms, titkosítás 20 ms, kiértékelés 45 ms, visszafejtés 10 ms (összesen 100 ms); CKKS rejtjelezett szöveg méretnövekedése: ~130 KB 512 bájtnyi nyílt szöveg esetén (~260-szoros növekedés).
beteg jogosultságának ellenőrzése személyazonosság felfedése nélkül	ZKP (nulla-ismeretű bizonyítás)	A beteg (bizonyító fél) kriptográfiai bizonyítékot generál arról, hogy megfelel bizonyos kritériumoknak (pl. „X betegséggel diagnosztizáltak”). A kutató (ellenőrző fél) ellenőrzi a bizonyítékot, és csak annyit tud meg, hogy a kritériumok teljesülnek.	ZKP-bizonyíték generálása: összetett áramkörök esetén másodperces nagyságrend; ellenőrzés: másodpercnél rövidebb idő alatt

biztonságos adatmegosztás intézmények között (kutatási konzorciumok)	SMPC	A betegadatokat kriptográfiai „részekre” (shares) bontják, és több kórház között osztják el. Minden kórház a saját részein végez számításokat. Az eredmény úgy áll elő, hogy egyetlen kórház sem látja a többi kórház nyers betegadatait.	Rész-összesítési késleltetés: ~4–4,2 s (10–16-os mélység esetén), lineáris skálázódás a részek számával
annak ellenőrzése (auditálása), hogy ki, mihez és mikor fért hozzá	kriptográfiai auditnaplók (pl. KSI blokklánc)	Minden hozzáférési eseményt (ki, mi, mikor) kriptográfiailag aláírnak és időbélyeggel látnak el, majd láncba fűznek.	Hyperledger Fabric (engedélyköteles blokklánc): tranzakciós késleltetés ~245 ms; okosszerződés-végrehajtás ~157 ms
álnevesített jelentéskészítés kutatási célokra	álnevesítés hash-eléssel és „salt” (véletlenszerű kiegészítő adat) használatával	A betegazonosítókat (pl. név, személyi azonosító, kórházi betegazonosító) egy egyedi, titkos „salt” értékkel fűzik össze, majd egy egyirányú kriptográfiai hash-függvényt (pl. SHA-256) alkalmaznak. Az eredeti azonosító és az álnév közötti megfeleltetést külön, szigorú hozzáférésszabályozás mellett tárolják.	SHA-256 átbocsátóképesség: 2,3 GB/s (egyszálú); az SHA-3-256 kb. 10-szer lassabb

3. ROMÁNIA EGÉSZSÉGÜGYBEN ALKALMAZOTT KRIPTOGRÁFIAI MEGOLDÁSAI

Románia egészségügyi rendszere fokozatos átalakuláson megy keresztül. A kriptográfia nyújtotta lehetőségeket vizsgálja aktívan olyan jelentős kihívások kezelésére, mint a kibertámadások, az interoperabilitás hiánya vagy a központosított adatrendszerek sebezhetősége. A Romániai rendszer aktívan elmozdult a sérülékeny, központosított egészségügyi informatikai megoldásoktól a kriptográfiailag védett, decentralizált modellek irányába, lásd [12].

Románia egészségügyi rendszere azonban jelentős strukturális kihívásokkal néz szembe, amelyek közvetlen hatással vannak kiberbiztonsági helyzetére. A fő problémás területek a következők, lásd [13]:

- Töredezett és kórházközpontú rendszer: A rendszer továbbra is erősen a kórházi ellátásra összpontosít, miközben az alapellátásra fordított kiadások jelentősen elmaradnak az OECD-átlagtól. Ez a központosítás összetett, nagy értékű célpontokat kínál a támadók számára.
- Munkaerő- és erőforráshiány: Kritikus mértékű az egészségügyi szakemberek hiánya; különösen a magasan képzett informatikai szakemberek hiányoznak az egészségügyi intézményekből, ami a biztonsági védelemhez szükséges humántőke hiányát eredményezi.
- Elavult infrastruktúra: Az egészségügyi ágazatban a technológiai fejlődés üteme meghaladta a támogató infrastruktúra fejlesztését, így számos rendszer sebezhetővé vált, biztonságuk szavatolása pedig nehézségekbe ütközik.

Ezek a rendszerszintű hiányosságok nem kerültek el a rosszindulatú szereplők figyelmét sem. 2024 februárjában egy nagyszabású zsarolóvírus-támadás (ransomware) blokkolta 20 kórház adatbázisát, napokra megbénítva az orvosi szolgáltatásokkal kapcsolatos adatszolgáltatást és az elszámolási folyamatokat. Ez az incidens kritikus tesztként szolgált: feltárta a valós sebezhetőségeket, és rávilágított a nem megfelelő védelemből

eredő súlyos működési és pénzügyi kockázatokra. Válaszul a kormány az alábbi intézkedéseket indította el, lásd [14]:

- A Nemzeti Digitális Egészségügyi Stratégia kidolgozása 2026 és 2030 közötti időszakra, amelynek célja egy átjárható elektronikus egészségügyi nyilvántartási rendszer (EHD) létrehozása 2028–2030-ig. Ez lehetővé tenné a szolgáltatók közötti biztonságos adathozzáférést.
- Jelentős beruházások megvalósítása a nemzeti helyreállítási és rezilienciaépítési terv (PNRR) keretében, beleértve a romániai egészségügyi adatplatform fejlesztését és a kiberbiztonság megerősítését az uniós NIS2 irányelvvel összhangban.
- A PIAS/eHealth platform korszerűsítése, amely növeli a kiberfenyegetésekkel szembeni ellenállóképességet.
- Új irányítási struktúrák létrehozása, például egy egészségügyi digitalizációs igazgatóság felállítása a szakpolitika támogatására, valamint egy egészségügyi digitalizációs egység létrehozása a digitális átállás előmozdítására.
- Humántőke-fejlesztés: a tervek szerint szabályozott szakmává emelik az egészségügyi informatikát, amely hidat képezne az egészségügy és az IT-biztonság között.
- Kritikus egészségügyi adatok biztonságos mentése a GDPR előírásainak megfelelően, lehetőleg uniós adatközpontokban történő tárolással.

Emellett számos magánvállalat és kutatóintézet is alkalmaz fejlett kriptográfiai megoldásokat.

- A SETRIO SOFT SRL által fejlesztett PatientDataChain egy uniós finanszírozású kísérleti projekt, amely blokklánc-technológiát használ annak érdekében, hogy a betegek maguk rendelkezhessenek egészségügyi adataik felett. Lehetővé teszi az adatok biztonságos, a beteg jóváhagyásával történő megosztását az egészségügyi szolgáltatókkal. A rendszer a beteg autonómiájának elvén alapul: az egyén dönt arról, ki tekintheti meg adatainak egyes részeit.
- A Logika-X által fejlesztett FitChain egy kereskedelmi forgalomban elérhető, decentralizált platform, ahol a felhasználók kezelhetik saját fitness- és egészségügyi adataikat – sőt, akár pénzzé is tehetik azokat. A rendszer személyes vagyontárgyként kezeli az egészségügyi adatokat, és az egyén döntheti el, hogy megosztja vagy értékesíti-e azokat.
- A PharmaLedger – amelyben az Institute for Analytical Instrumentation is részt vett – egy 2019 és 2022 között zajló EU Horizon 2020 projekt volt; egy olyan európai konzorcium része, amely blokklánc-technológiát alkalmazott a hamisított gyógyszerek elleni küzdelemben és a gyógyszerellátási lánc biztonságának garantálásában. A projekt egy kritikus betegbiztonsági kérdést kezel: annak biztosítását, hogy a gyógyszerek eredetiek és hamisítatlanok legyenek.
- A SmartClover SRL – a Ratio platform fejlesztője – egy mesterséges intelligenciára épülő román egészségügyi technológiai vállalat, amely létrehozta a CerviGuard rendszert a méhnyakrák-szűréshez. Ez a kereskedelmi termék titkosítást és módosíthatatlan blokklánc-naplózást alkalmaz annak biztosítására, hogy a betegadatok ne hagyják el a klinikai környezetet; a tervezés során kulcsfontosságú szempont volt a GDPR-megfelelés és a teljes körű ellenőrizhetőség biztosítása.

E reformok egyik fő mozgatórugója az uniós tagság. A GDPR-nek való megfelelés, az Európai Egészségügyi Adattérhez (European Health Data Space) való igazodás, valamint a kórházak számára készült uniós kiberbiztonsági cselekvési terv egyaránt biztosítja a szabályozási keretet és a pénzügyi ösztönzést Románia átállásához. A kihívások tehát nagyok, de megvan a valós támogatói háttér is, amely előre remélhetőleg előre viszi Romániát. Mint láthattuk, ennek érdekében mind a magánszektor, mind a kormányzat több síkon is reagált.

Nyilvánvaló tehát, hogy Románia nem elszigetelten fejlődik. Arra törekszik, hogy a helyi sajátosságokhoz igazodó európai jövőképet valósítson meg. A megtett intézkedések azt mutatják, hogy Románia komolyan veszi az egészségügyi kiberbiztonságot – ám a megvalósítás még hátra van és igazából ez jelenti majd az igazi próbát. A stratégia természetesen ambiciózus, a kihívást pedig a kivitelezés jelenti.

Összegzőként megállapíthatjuk, hogy Románia nem csupán követi az előírásokat, hanem aktívan törekszik innovatív fejlesztések megvalósítására is – az uniós finanszírozású kísérleti projektektől kezdve egészen a kereskedelmi forgalomba kerülő termékekig.

IRODALMI HIVATKOZÁSOK

- [1] Rashmi Agrawal and Pramod Singh Rathore and Ganesh Gopal Devarajan and Rajiva Ranjan Divivedi, *Artificial Intelligence and Cybersecurity in Healthcare*, Hoboken, Wiley, 2025.
- [2] Alomar D, Almashmoum M, Eleftheriou I, Whelan P, Ainsworth J. *The Impact of Patient Access to Electronic Health Records on Health Care Engagement: Systematic Review*. J Med Internet Res. 2024 Nov 20;26:e56473. doi: 10.2196/56473. PMID: 39566058; PMCID: PMC11618012.
- [3] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Pearson Education, 8th edition, 2023.
- [4] Acar, Abbas and Aksu, Hidayet and Uluagac, A. Selcuk and Conti, Mauro. *A Survey on Homomorphic Encryption Schemes: Theory and Implementation*, ACM Comput. Surv., Association for Computing Machinery. New York, NY, USA, 2018, doi = "10.1145/3214303
- [5] Oded Goldreich, Silvio Micali, Avi Wigderson, *How to Prove All NP-Statements in Zero-Knowledge / Proofs that Yield Nothing But their Validity*. Journal of the ACM (JACM). 1991.
- [6] Yehuda Lindell. *Secure Multiparty Computation*, Cryptology ePrint Archive, 2020, doi: 10.1145/3387108
- [7] Vipul Goyal and Omkant Pandey and Amit Sahai and Brent Waters. *Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data*. Cryptology ePrint Archive, 2006.
- [8] Bonawitz, K., Eichner, H., Grieskamp, W., Huba, D., Ingerman, A., Ivanov, V., and McMahan, H. B. *Towards Federated Learning at Scale: System Design*. arXiv:1902.01046. 2019.
- [9] *Blockchains*. Editors: Sushmita Ruj, Salil S. Kanhere, Mauro Conti. Springer Cham. Advances in Information Security. A Handbook on Fundamentals, Platforms and Applications. 2024. <https://doi.org/10.1007/978-3-031-32146-7>.
- [10] Chenxi Huang and Jian Wang and Shuihua Wang and Yudong Zhang. *Internet of medical things: A systematic review*. Neurocomputing. vol 557. 2023. <https://doi.org/10.1016/j.neucom.2023.126719>.
- [11] Wu S-P, Wu S-D, Lu K-C and Wu C-C. *Post-quantum cryptography for healthcare: securing medical data, connected devices, and digital health infrastructure*. Front. Health Serv. 6:1901282. 2026. doi: 10.3389/frhs.2026.1901282.
- [12] Frăţilă, A. E. *Crearea unei noi platforme pias în sănătate şi implementarea directivei europene NIS 2*, 2025. <https://scred.eu/index.php/spr/article/view/597>.
- [13] Iulian V. Nastasa and Florentina Ligia Furtunescu and Dana Galieta Mincă. *Challenges and Progress in General Data Protection Regulation Implementation in Romanian Public Healthcare*. Cureus. Vol.17. 2025.
- [14] OECD Publishing. *ECD Reviews of Health Systems: Romania 2025*, OECD Reviews of Health Systems. 2025. 10.1787/f52e4a98-en