

ODOLNOST SLUŽEB eHEALTH



Petr Pavlinec
Kraj Vysočina – odbor IT
2. 2. 2026

1. Definice WHO

- eHealth je **přenos informací pomocí elektronických prostředků** za účelem podpory zdraví a zdravotní péče, včetně léčby, prevence, výzkumu, vzdělávání a správy.

2. ČR – Zákon č. 325/2021 Sb. o elektronizaci zdravotnictví:

- Elektronické zdravotnictví - poskytování a využívání služeb a informačních systémů Integrovaného datového rozhraní zdravotnictvía informačních systémů poskytovatelů zdravotních služeb nebo poskytovatelů sociálních služeb poskytujících zdravotní služby.... sloužících **k vedení nebo předávání zdravotnické dokumentace v elektronické podobě, včetně systémů umožňujících dálkový přístup pro pacienta, podle tohoto zákona.**

3. Prakticky:

- Zahrnuje **technologie, standardy, právní rámce a služby**, které umožňují **bezpečné, efektivní a interoperabilní nakládání se zdravotními informacemi napříč zdravotnickými subjekty** – ve prospěch pacienta i systému jako celku.

1. Pandemie COVID 19

- Předávání informací ve zdravotnictví bylo neefektivní, pomalé a ne vždy bezpečné
- Pochopení, že bez centralizace dat a služeb to dál nepůjde

2. Rostoucí potřeba sdílení dat mezi zdravotnickými subjekty

- Problém – každý má jiný IS, jiného zřizovatele, jiné priority
- Bez sdílení informací je efektivní návazná zdravotnická péče problematická.
- Už existují dobré praxe z jiných států

3. Papírová zdravotnická dokumentace nestačí

- Zdravotnictví se digitalizaci ZD dlouhodobě vyhýbalo, ale mnohé obory se digitalizují
- Papírová dokumentace – nosičem je pacient, pošta....
- Cílem je dostat správné informace o správné osobě správnému adresátovi bezpečně, standardizovaně a rychle

1. Elektronická zdravotnická dokumentace

- EHR – Electronic Health Record (propouštěcí zprávy, laboratorní výsledky, snímky, zprávy, žádanky...)

2. Telemedicína

- Měřicí přístroje, naměřené hodnoty, chytrá zařízení, dávkovače/pumpy (!!)

3. Elektronická preskripce (eRecept), ePoukaz.....

4. mHealth

- Povinnost poskytovat informace veřejnosti, online

5. Další související služby

- Zdravotnické registry (nově „kmenové“ – lékařů, poskytovatelů, pacientů...)
- Dočasné úložiště (DU), statistické služby (NZIS), eŽádanka, Sdílený zdravotní záznam
- Přenosové sítě – ePAC, eMedocs, NCPeH, eZpráva, ClickBox ...

1. Identifikace/autentizace/autorizace

- Pacienta – RID, kmenový registr pacientů
- Zdravotníka – identifikátor pracovníka, kmenový registr zdravotnických pracovníků

2. Zdroje dat

- Centralizace / decentralizace

3. Standardizované formáty a služby

- Aby si systémy rozuměly, musí mluvit stejným jazykem.
- HL7 CDA (L1, L3) – dokumentově orientovaný formát (XML)
- HL7 FHIR - resource(service)-based formát (JSON)
- DASTA – český specifický formát používaný v nemocničních IS

4. Bezpečnost a důvěra

- Každý bezpečnostní incident snižuje důvěru uživatelů.
- GDPR, ZOKB, NIS2, EHDS

Důvěryhodnost

- Jasný a důvěryhodný provozovatel/poskytovatel (i u mobilních aplikací)
- Funkční uživatelská (vícekanálová) podpora
- Správa citlivých osobních údajů = nutnost zpracování DPIA
- Jasné podmínky nakládání s osobními údaji
- Využívání důvěryhodných identitních nástrojů (NIA)

Dostupnost

- Vysoká dostupnost (HA) ... i v době rostoucích DDoS a geoblokace
- Přehlednost - využívání státního design systému (bootstrap)
- Dlouhodobá dostupnost dat – elektronická archivace, skartace

Technická bezpečnost

- Kvalitní pen-testování (nejen vnější) a zátěžové testování (včetně autentizace)
- Využívání neveřejných sítí pro backoffice komunikaci
- Využívání post-kvantových šifer

<https://api.csez.gov.cz/krp/>

Cipher Suites			
# TLS 1.3 (suites in server-preferred order)			[-]
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
# TLS 1.2 (suites in server-preferred order)			[-]
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits	FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xccaa)	DH 2048 bits	FS	256
TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)	DH 2048 bits	FS	256
TLS_ECDHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc061)	ECDH x25519 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_ARIA_256_GCM_SHA384 (0xc053)	DH 2048 bits	FS	256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits	FS	128
TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)	DH 2048 bits	FS	128
TLS_ECDHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc060)	ECDH x25519 (eq. 3072 bits RSA)	FS	128
TLS_DHE_RSA_WITH_ARIA_128_GCM_SHA256 (0xc052)	DH 2048 bits	FS	128
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)	ECDH x25519 (eq. 3072 bits RSA)	FS WEAK	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0xc023)	DH 2048 bits	FS	256
TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384 (0xc09d)	ECDH x25519 (eq. 3072 bits RSA)	FS	256

[cisa.gov/resources-tools/resources/product-categories-tech...](#)

[Home](#) / [Resources & Tools](#) / [Resources](#) / Product Categories for Technologies That Use Post-Qu...

Product Categories for Technologies That Use Post-Quantum Cryptography Standards

Publish Date: January 23, 2026

RELATED TOPICS: [CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE](#), [RISK MANAGEMENT](#)

[Scan Security](#)

- api.csez.gov.cz - Quantum-Vulnerable
- Currently vulnerable - quantum-safe migration needed

TLS Version: Unknown

Cipher Suite: Unknown

Key Exchange: Classical only

Certificate: Certificate details unavailable

No post-quantum handshake

The server rejected every ML-KEM offer and completed TLS with a classical key exchange (unknown). Recorded traffic could be decrypted later once sufficiently powerful quantum computers exist.

Kudy komunikujeme?

<https://api.csez.gov.cz/>

% Information related to '193.16.104.0/24AS12767'

route: 193.16.104.0/24
descr: KSRZIS
origin: AS12767
mnt-by: AS12767-MNT
created: 2014-06-27T13:13:16
last-modified: 2014-06-27T13:13:16
source: RIPE

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Centrální místo služeb

Otevřené aplikace

Řízené aplikace

DNS záznamy

DNS zóny

Odebírané řízené aplikace

Vyhledat text

uzis

OFICIÁLNÍ NÁZEV
APLIKACE



SPRÁVCE APLIKACE

URL ADRESA

Rozhraní API ÚZIS ČR

Ústav zdravotnických informací a
statistiky ČR

<https://api.uzis.cms2.cz>

Zobraz záznamů

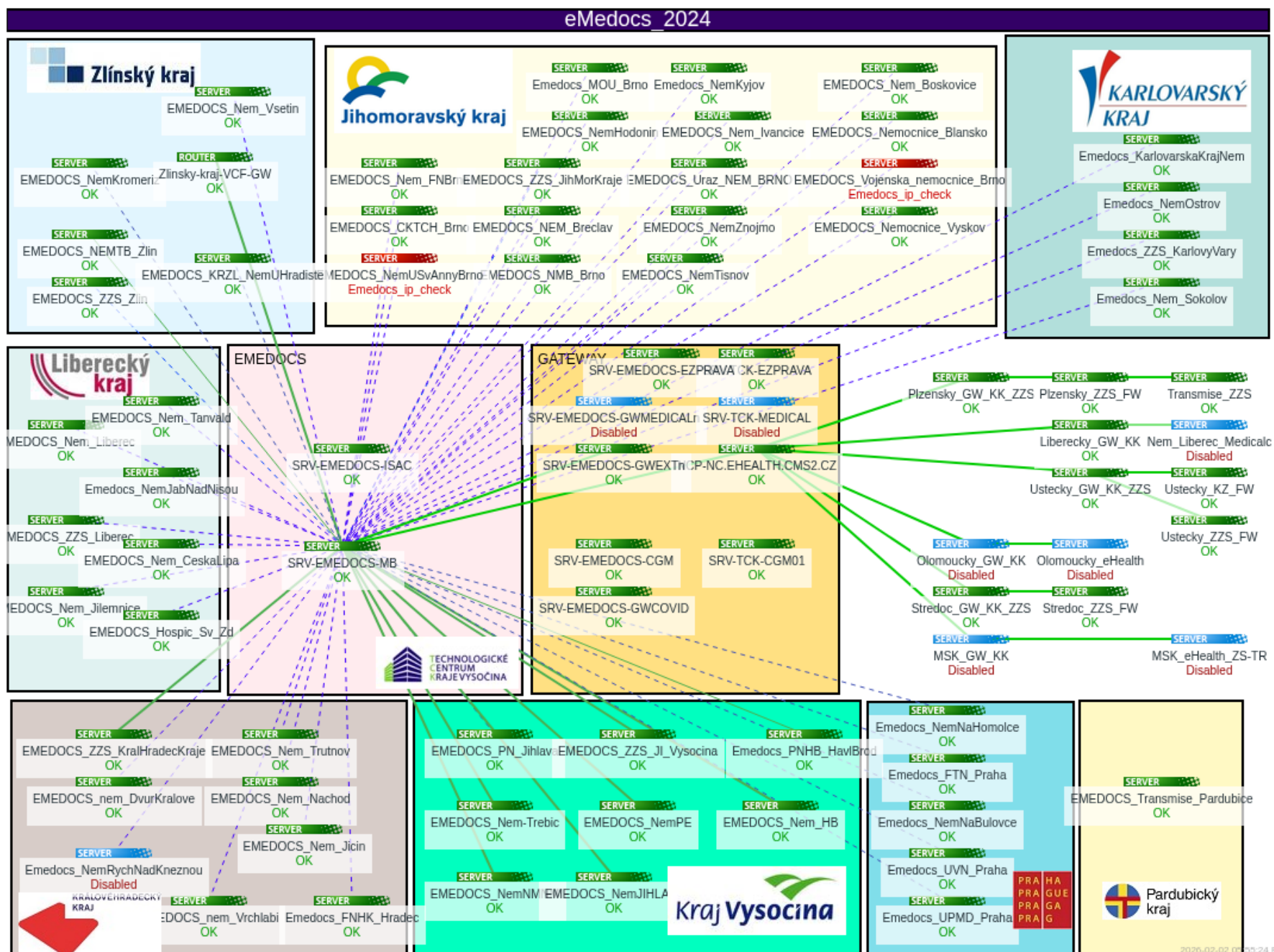
10 ▼

<

1

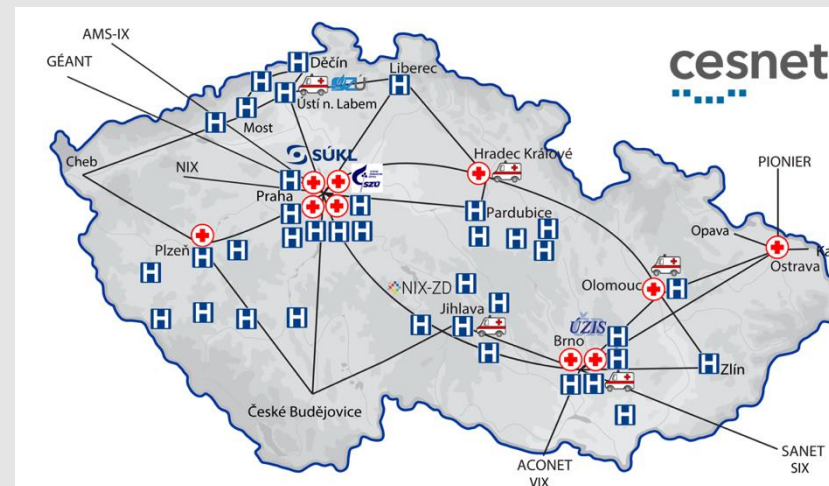
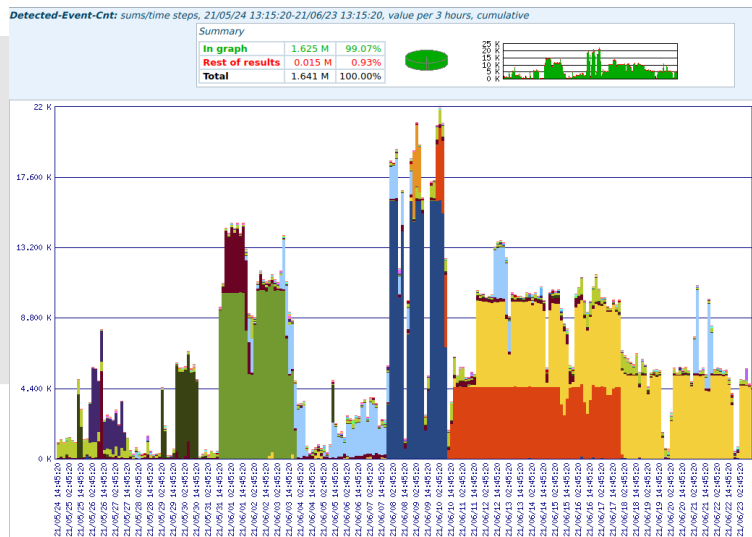
>

Kudy komunikujeme?



2020-02-02 15:55:24 PM

- V současnosti denně cca 80 – 90 tis. detekovaných a automaticky mitigovaných hrozeb na perimetru sítě**



Nutné kroky k bezpečnému zdravotníctví - X dní po kyberútociach na nemocnice ... II.časť



European Health Data Space / Evropský prostor pro zdravotní údaje

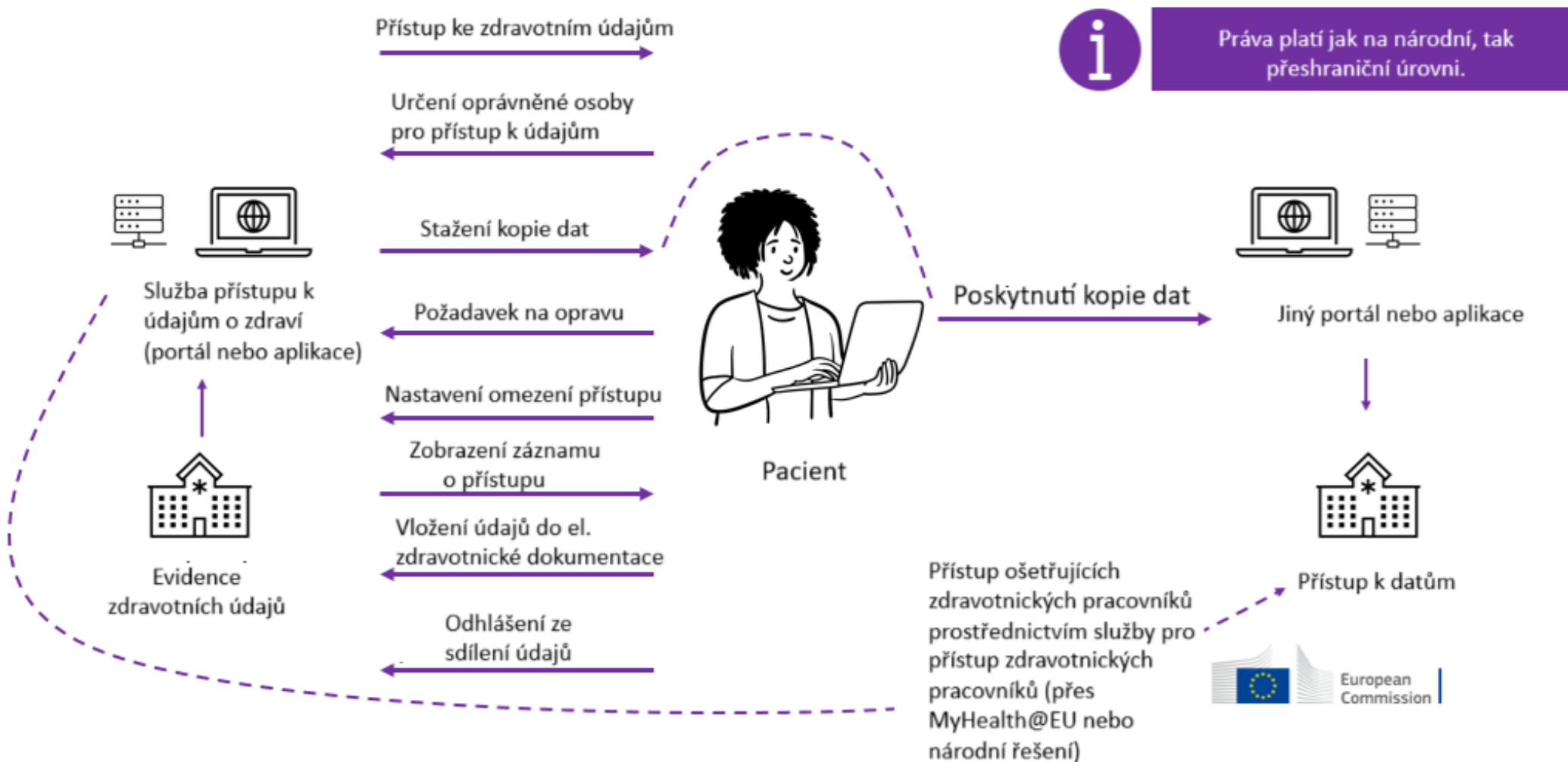
- Prijato: únor 2025 – klíčový legislativní milník pro digitální zdravotnictví v EU
- Nařízení – přímo platné a účinné

Přístup pacientů k jejich zdravotním údajům

Zdravotní údaje už nebudou uvězněné v jednom systému. Pacient je jejich vlastníkem.

- ✓ Každý občan EU má právo na bezplatný, přímý a okamžitý přístup ke svým vybraným zdravotním údajům v elektronické podobě.
- ✓ Musí být dostupné v interoperabilním, strojově čitelném formátu – např. CDA/FHIR.
- ✓ Týká se klíčových typů dokumentů: patientský souhrn, propouštěcí zprávy, laboratorní výsledky, zobrazovací zprávy, eRecepty atd.
- ✓ Přístup i přeshraničně: data musí být čitelná a použitelná v jiné zemi EU v systému MyHealth@EU

Důraz na práva pacientů



Povinné standardy a certifikace systémů EHR

- Systémy pro elektronické zdravotní záznamy (EHR – Electronic Health Record) budou podléhat certifikaci, pokud chtějí být používány v EU.
- Certifikace zajišťuje:
 - interoperabilitu (např. formáty jako HL7 FHIR, CDA; integrační profily)
 - bezpečnost (např. řízení přístupů, **auditní stopy – IHE profil ATNA případně BALP**)

Sekundární využití zdravotnických dat – pro vědu, výzkum, politiku

DĚKUJI ZA POZORNOST!

**Krajský úřad Kraje Vysočina
Odbor informatiky
Žižkova 57, Jihlava 587 33**

Petr Pavlinec

Pavlinec.p@kr-vysocina.cz

