

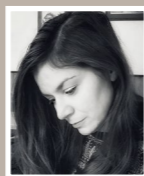


Jakkoliv je prognostický a prediktivní význam hladiny S-100B v rámci diagnostiky maligního melanomu diskutován, jedná se stále o jeden z nejčastěji používaných biomarkerů v diagnostice tohoto onemocnění a jeho monitorování je doporučeno zejména u pacientů s vysokým rizikem vzniku maligního melanomu,¹¹ což je v souladu s daty získanými ve FN Brno.

Přestože protein S-100B byl historicky objeven a popsán jako marker specifický pro neurální tkáň a využívaný pouze pro traumatické poranění hlavy, brzy vyšlo najevo, že jeho zvýšené hodnoty se vyskytují i u pacientů bez traumatu mozku, což značí, že k expresi proteinu dochází i v dalších tkáních.

Tím lze vysvětlit falešně pozitivní výsledky u pacientů bez poranění hlavy.^{4,5} Navíc se uvažuje o tom, že i extrakraniální tkáň musí nějakým způsobem přispívat ke zvýšení hodnot S-100B, protože zvýšené hladiny se vyskytují mimo jiné i u zdravých maratonských běžců.⁵ Stejně tak žlutá i červená kostní dřev, které obsahují velké množství adipocytů, mohou přispívat k vysoké hladině S-100B u pacientů se zlomeninami dlouhých kostí či hrudníku. Kromě toho každá zlomenina je neoddělitelně spojena s poškozením okolní měkké tkáně. To vše pravděpodobně ovlivňuje zvýšení hladin S-100B a vysvětluje tak asociaci s celkovou vážností traumatického zranění.⁵ Kromě toho by tento fakt vysvětloval i to, proč mnohé studie nalezly

zvýšené hladiny S-100B u pacientů s jinými traumatickými zraněními nepostihujícími oblast hlavy.⁴ Pokud jde o skutečnost, že v rámci FN Brno není toto vyšetření častěji indikováno na neurochirurgické klinice, vysvětluje nám to dostupnost zobrazovacích metod a velký počet dalších vyšetření. Použití markeru S-100B by v takovém případě neposkytlo ošetřujícím lékařům novou informaci o stavu pacienta. Lze předpokládat, že i v těchto případech by S-100B korelovalo s dalšími vyšetřovanými parametry a výsledkem by neovlivnil diagnostické a terapeutické postupy. Avšak na pracovištích, kde nejsou dostupné zobrazovací techniky, může S-100B představovat ideální marker schopný svou výpovědní hodnotou přispět ke správné diagnostice a léčbě.



Mgr. Alice Hoffmannová, Ph.D.
Kontakt: Hoffmannova.Alice@fnbrno.cz
Vystudovala bakalářské a magisterské studium na Fakultě chemicko-technologické Univerzity Pardubice se zaměřením na speciální chemicko-biologické obory. Následně navázala na doktorské studium biochemie na Masarykově univerzitě v Brně. V současné době pracuje na oddělení klinické biochemie ve FN Brno a předtím se několik let profesně věnovala biobankování na Masarykově onkologickém ústavu v Brně.

Ing. Tomáš Procházka
ROCHE s.r.o., Diagnostics Division

Úvod

Tradičně poskytovatelé zdravotních služeb a laboratoře zajišťují sběr většiny dat týkajících se zdraví populace. K nim se v poslední době připojují také údaje z výstupů genetických analyzátorů, specifických registrů a soukromé vlastních zařízení, která například monitorují tepovou frekvenci, zásobení organismu kyslíkem či krevní tlak atd. Množství záznamů klinických, laboratorních, genetických anebo vyvozování nových poznatků exponenciálně roste. S tímto se pojí zvýšený tlak na zpracování, zabezpečení a standardizaci dat. Poslední zmíněná soukromá zařízení se vyznačují ukládáním datových kolekcí na izolovaných platformách, které nejsou navzájem propojeny, a tím se celá situace komplikuje.

Dlouhodobým cílem pro zdravotnictví je digitální transformace, která by pomohla

Digitalizace zdravotnictví – výzvy a přínosy

Rychlý technologický pokrok zaznamenal v posledních letech každý z nás, nejen díky pandemii byl tento trend ještě urychlen. Jako klíčová se pro vyrovnání s tímto pokrokem jeví digitalizace jednotlivých sektorů.

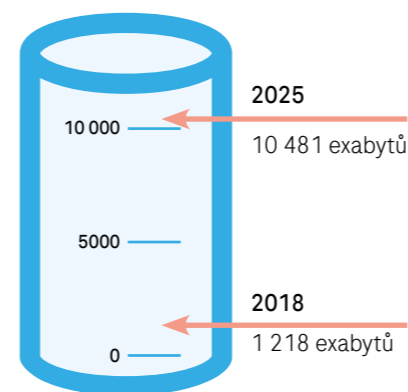
zabezpečení a sběru dat, analýze, parametrizaci a zejména interoperabilitě mezi poskytovateli zdravotní péče. Velkou výzvou se jeví standardizace výměny zdravotních záznamů a její nasazení v praxi. Tento problém by mohly řešit sdílené centrální služby, které by sloužily k propojování a poskytování dat z centrálních registrů ČR, kde jsou data v drtivé většině agregována a dále zpracovávána. Prozatím se ale jako více realistická jeví varianta, kde zdravotnická zařízení na vlastní náklady upgradují softwarové vybavení a tzv. NIS (nemocniční informační systémy), v nichž je drtivá většina dat uchovávána, jsou upgradovány na novější verze, které dokážou komunikovat v nadnárodně uznávaných messaging standardech, jako je například HL7 v.2 nebo FHIR. Samostatnou skupinou je messaging standard DASTA (<https://www.dastacr.cz>), který je českou specialitou a není mezinárodním standardem, čímž uživatele omezuje

v interoperabilitě. Z tohoto důvodu je řada českých poskytovatelů zdravotní péče nucena zřizovat komunikační a integrační platformy, které slouží k převodu dat mezi jednotlivými standardy.

Cíle digitalizace zdravotnictví a hlavní opatření jsou uvedeny ve Strategickém rámci rozvoje péče o zdraví v ČR do roku 2030, „Zdraví 2030“, schváleném vládou ČR.¹

Vůbec největší výzvou je zabezpečení exponenciálně rostoucího množství zdravotních dat. Státní úřady jsou si této hrozby vědomy, a proto stále více a více investují do pracovníků a nabírají nové zaměstnance. **Tabulka 1** popisující mzdové náklady Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), **uvedená níže**, mluví za vše.

Více dat bude zachyceno a ukládáno než kdy předtím



Zdravotnická data¹
exabytů zachyceno

- Počet sportovních a zdravotních mobilních zařízení třikrát zvýšil svůj objem z 26 mil. v 2014 na 87 mil. v 2017
- V USA se elektronické zdravotnické záznamy na onkologických klinikách zvýšily z ~10% na >95%²
- Poskytovatelé zdravotní péče agregují elektronické zdravotní záznamy z nemocničních informačních systémů (každý provozovatel v odhadovaném objemu 50 petabytů – zahrnutý obrázek a anotace³)

> Zdroj: a) IDC, "Data Age 2025: The Digitization of the World from Edge to Core," November 2018 using 2018 data volume and predicted 36% CAGR. b) <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>

Literatura

- LIU, Yidong; MYRVANG, Helene K.; DEKKER, Lodewijk V., A nxn A 2 complexes with S 100 proteins: structure, function and pharmacological manipulation. *British journal of pharmacology*, 2015, 172 (7), 1664-1676.
- GÜNGÖR, Olcay, et al., Evaluation of blood neuron specific enolase and S-100 beta protein levels in acute mercury toxicity. *Trace Elements and Electrolytes*, 2018, 35 (3), 131-135.
- SATO, Yasunori, et al., Clinicopathological significance of S 100 protein expression in cholangiocarcinoma. *Journal of gastroenterology and hepatology*, 2013, 28 (8), 1422-1429.
- PFORTMUELLER, Carmen Andrea, et al., S-100 B concentrations are a predictor of decreased survival in patients with major trauma, independently of head injury. *PLoS One*, 2016, 11 (3), e0152822.
- MÜLLER, Martin, et al., Increased S-100 B levels are associated with fractures and soft tissue injury in multiple trauma patients. *Injury*, 2020, 51 (4) 812-818.
- CHAPARRO-HUERTA, Verónica, et al., Proinflammatory cytokines, enolase and S-100 as early biochemical indicators of hypoxic-ischemic encephalopathy following perinatal asphyxia in newborns. *Pediatrics & Neonatology*, 2017, 58 (1), 70-76.
- CALIK, Mustafa, et al., Interictal serum S-100B protein levels in intractable epilepsy: a case-control study. *Neuroscience letters*, 2014, 558, 58-61.
- WOJTCZAK-SOSKA, K.; LELONEK, M., S-100B protein: An early prognostic marker after cardiac arrest. *Cardiology journal*, 2010, 17 (5), 532-536.
- HELÁNOVÁ, K., et al., S-100B protein elevation in patients with the acute coronary syndrome after resuscitation is a predictor of adverse neurological prognosis. *Vnitřní lékařství*, 2012, 58 (4), 266-272.
- MOCELLIN, S.; ZAVAGNO, G.; NITTI, D., The prognostic value of serum S100B in patients with cutaneous melanoma: A meta-analysis. *International journal of cancer*, 2008, 123 (10), 2370-2376.
- ERTEKIN, S. S., et al., Monthly changes in serum levels of S100B protein as a predictor of metastasis development in high-risk melanoma patients. *Journal of the European Academy of Dermatology and Venereology*, 2020, 34 (7), 1482-1488.
- MISSOTTEN, G. S., et al. S-100B protein and melanoma inhibitory activity protein in uveal melanoma screening. *Tumor Biology*, 2007, 28 (2), 63-69.





Mzdové náklady Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB)

	2018	2019	2020
Platy a podobné související náklady	141,66 mil. CZK	165,01 mil. CZK	191,75 mil. CZK

Tab. 1: Zdroj: <https://monitor.statnipokladna.cz/kapitola/378/prehled?obdobi=1812&rad=t>

Personální náklady Agentury Evropské unie pro kybernetickou bezpečnost (ENISA)

	2015	2016	2017
Personální náklady	5,9 mil. €	6 mil. €	6,4 mil. €

Tab. 2: Zdroj: https://www.enisa.europa.eu/about-enisa/accounting-finance/files/annual-budgets?b_start:int=20

Stejný trend lze pozorovat i za hranicemi a **tabulka 2**, která zachycuje personální náklady ENISA (Agentura Evropské unie pro kybernetickou bezpečnost), vykazuje také rostoucí tendenci.

V řechi čísel lze jasně a jednoduše demonstrovat, jaká důležitost je kladena nejvyššími orgány na kybernetickou bezpečnost. Není divu, když NÚKIB oznámil k datu 31. 12. 2019 celkem 78 řešených kybernetických bezpečnostních incidentů pouze za rok 2019. Přičemž nejvíce určených informačních systémů základní služby bylo ze sektoru zdravotnictví – v celkovém počtu 34 z 56 celkově možných. Pro srovnání: chemický průmysl měl celkem 4 určené informační systémy základní služby k datu 31. 12. 2019. Závěrem lze konstatovat, že sektor zdravotnictví je ze všech sektorů ten nejvíce zranitelný.

Minimální bezpečnostní standard

Nejen mzdové náklady NÚKIB, ale i *zákon o kybernetické bezpečnosti*², který vešel v platnost 1. ledna 2015, napovídá, že se prostor s informacemi mění. Vymezení působnosti zákona však není vůbec jednoduché a ne vždy je jasné, zda subjekt spadá pod tento zákon anebo nikoliv. Z tohoto důvodu NÚKIB ve spolupráci s NAKIT (Národní agentura pro komunikační a informační technologie) a Ministerstvem vnitra vydalo 17. července 2020 *Minimální bezpečnostní standard*³, což je podpůrný materiál pro subjekty, které nespádají pod zákon o kybernetické bezpečnosti.

V technické části tohoto dokumentu se lze dočíst minimální technické požadavky, které by měl subjekt splňovat:

1. Fyzická bezpečnost (kamerový systém, chráněné servery, klimatizace prostor, nezávislý zdroj napájení atd.)
2. Řízení přístupů
 - > registrace, autentizace a identifikace uživatelů
 - > politika hesel pro uživatelské a privilegované účty
3. Požadavky v oblasti ochrany před škodlivým kódem
4. Kybernetické bezpečnostní události a incidenty (log systém)
5. Požadavky v oblasti aplikační bezpečnosti
6. Kryptografické prostředky
 - > šifrování disků a externích USB disků (mezi preferované patří AES, Camellia a Serpent – v uvedeném pořadí – a velikost klíče 256 bitů)
 - > ukládání hesel (nejlépe použitím k tomu určenému hašovacímu

algoritmu spolu s náhodně vygenerovanou „solí“)

- Argon2 (nejlépe ve verzi „id“)
- Scrypt
- Bcrypt
- Pbkdf2 (s použitím schváleného hašovacího algoritmu)

7. Požadavky v oblasti zajišťování úrovně dostupnosti informací
 - > řešení vysoké dostupnosti (určeno dle SLA, které vychází z jednotlivých hodnot RPO a RTO)
 - > SPOF (Single Point of Failure) – to znamená, že porucha jedné komponenty nezpůsobí výpadek celého informačního nebo komunikačního systému
 - > zálohování
8. Požadavky v oblasti cloudových služeb
 - > deklarace místa uložení zákaznických dat v rámci jurisdikce EU
 - > deklarace úrovně bezpečnosti poskytovaných cloudových služeb (doporučíme doložení certifikátu ČSN ISO/IEC 27001 nebo Auditní zprávu SOC 2 Type II (AT 101), případně zajištění auditu na místě)
 - > šifrovaná komunikace (TLS/VPN) přes internet s využitím kryptografických algoritmů publikovaných v doporučení NÚKIB
 - > smlouva s provozovatelem cloudových služeb obsahující vymezení provozních podmínek (SLA) a tzv. exit strategii (exit plán) včetně předání dat
 - > smluvní podmínky s provozovatelem cloudových služeb, které jsou v souladu s požadavky na zpracovatele dle čl. 28 obecného nařízení GDPR (v případě zpracování osobních údajů v informačním nebo komunikačním systému)
 - > smlouva s provozovatelem cloudových služeb obsahující povinnost informovat o bezpečnostních incidentech týkajících se daného zákazníka a spolupracovat při jejich zvládnutí
 - > další požadavky (například ochrana před SQL injection útoky atd.)⁴

Iniciativa ministerstva zdravotnictví

Další, kdo nabídl pomocnou ruku zdravotnickým zařízením, je Ministerstvo zdravotnictví, které 2. 8. 2017 zpracovalo *Metodický*

*pokyn poskytovatelům zdravotních služeb k problematice kybernetické bezpečnosti*⁵. Nás bude zajímat jeho poslední verze 2.0 z 12. 6. 2019 a konkrétně sekce „Bezpečnostní opatření – Technická opatření“.

Obsahuje tyto body:

1. fyzická bezpečnost
2. nástroj pro ochranu integrity komunikačních sítí
3. nástroj pro ověřování identity uživatelů
4. nástroj pro řízení přístupových oprávnění
5. nástroj pro ochranu před škodlivým kódem
6. nástroj pro zaznamenávání činnosti informačních systémů, jejich uživatelů a administrátorů
7. nástroj pro detekci kybernetických bezpečnostních událostí
8. nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
9. aplikační bezpečnost
10. kryptografické prostředky
11. nástroj pro zajišťování úrovně dostupnosti informací
12. bezpečnost průmyslových a řídicích systémů⁶

Hackerské útoky

Na chvíli opustíme teorii a zaměříme se na praxi. Nyní by se mohlo zdát, že zdravotnické záznamy jsou jedny z nejvíce zabezpečených dat. Nicméně stále se objevují nové a nové zprávy o úspěšném napadení nemocničních systémů hackery. Například společnost IBM (<https://www.ibm.com/us-en/>) a její tým „IBM Security research“ narazil na online prodej balíku skenů dokumentů z lékařské dokumentace, včetně informací o zdravotním pojištění nebo platebních kartách. To celé pouze za 69,99 USD. **Obrázek 1** ukazuje reklamu na prodej skenů.

V posledních letech pandemie COVID-19 dopadá na zdravotnická zařízení po celém světě a kritická infrastruktura čelí další výzvě – zvyšujícímu se počtu kybernetických útoků během pandemie. Interpol vydal zprávu na začátku pandemie, v níž oznámil významný nárůst kybernetických útoků. Více zde: <https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19>. Interpol se také nechal slyšet,

Reklama společnosti IBM na prodej skenů



Figure 1 shows an ad for such a combination, asking USD69.99 for full payment card data—“Fullz” in fraudster jargon—for an impressive package of document scans including medical

and health insurance information. Spear phishing, financial fraud and medical identity theft are just a few of the ways attackers can use such data for monetary gain.

Figure 1. Screenshot of record for sale on the dark web. Source: IBM Security research.

Obr. 1: Zdroj: <https://www.ibm.com/downloads/cas/PLWZ76MM>





že hackeři využívají výhody probíhající pandemie zvláště u zdravotnických zařízení.

Bohužel nemusíme chodit do zahraničí, abychom se dočetli o hackerských útocích. Na počátku pandemie české nemocnice čelily řadě útoků. Jejich úspěšné odrazení se povedlo krajské nemocnici v Olomouci, v Karlových Varech, Nemocnici Pardubického kraje a Fakultní nemocnici v Ostravě. Bohužel útok v benešovské nemocnici nebo Fakultní nemocnici v Brně byl pro hackery úspěšný.

Dne 11. prosince 2019 došlo k útoku na Nemocnici Benešov, kde ransomware, počítačový vir, který šifruje data na serverech a PC, ochromil chod nemocnice. Omezené byly zejména lékařské výkony a transfúzní stanice. Pachatele se ani po půl roce nepovedlo odhalit. Nakonec vyšetřovatelé rozkryli pachatele až začátkem roku 2021.

Dne 13. března 2020 byla napadena jedna z největších nemocnic, a to Fakultní nemocnice v Brně. Jednalo se o stejný typ útoku. „Podle odborníků bylo v loňském roce napadena podobným způsobem devatenáct procent nemocničních a zdravotnických počítačů či zařízení. „Ransomwarevé útoky na nemocnice se v poslední době objevují poměrně často, což poukazuje na fakt, že nejde jen o slabou ochranu zdravotnických zařízení. Tento problém je dalekosáhlejší, protože celá IT infrastruktura moderních nemocnic není řádně organizována

a chráněna, s čímž mají problém organizace po celém světě. Například řada těchto zařízení běží na systému Windows XP a má stovky starých, nijak nezaplátovaných zranitelností, které by mohly vést k úplnému prolomení vzdáleného systému. V některých případech mají navíc tato zařízení nezměnná výchozí hesla, která lze snadno zjistit pomocí manuálů dostupných na internetu,“ okomentoval za firmu Kaspersky Miroslav Kořen.⁷

Hlavní překážkou zajištění kybernetické bezpečnosti v nemocnicích je nízký rozpočet dedikovaný na tuto oblast. Kybernetická bezpečnost je v nemocnicích podfinancována a nestačí na zakoupení potřebných technologií. Zde se nabízí řešení v podobě SaaS (software as a service), kdy nemocnice nemusí řešit náklady na například provozování serverů, jejich pravidelnou obměnu a personál, který je obsluhuje. Mnohem zajímavější je možnost delegovat tuto odpovědnost na dodavatele služeb, kteří jsou profesionálové v oboru a mají potřebné finance plynoucí z výnosů z rozsahu, které nemocnice z podstaty věci nemůže mít. Její soustředění se tak může zpět obracet k pacientům a ne k zabezpečení systémů.

Komerční řešení

Příkladem může být skupina produktů NAVIFY® od firmy Roche, divize RIS (Roche Information Solutions). NAVIFY® produkty jsou nadstavba nad NIS a dokážou

díky standardizované komunikaci v HL7 v.2, FHIR anebo DICOM (Digital Imaging and Communications in Medicine, <https://www.dicomstandard.org>) přijímat datové sady a pomocí machine learning a vyhledávacích algoritmů je „pročesávat“ a pomáhat lékařům při jejich rozhodování v mnoha oborech, jako je virologie, onkologie nebo patologie.

První dostupný produkt NAVIFY® Tumor Board byl spuštěn v roce 2017 a jedná se o softwarové řešení na základě cloudového úložiště, které zásadně mění způsoby, jak týmy onkologů připravují, provádějí a dokumentují klinická rozhodnutí o ošetřování. Produkt dokáže zpracovávat velmi komplexní onkologická data z různých zdrojů, od elektronického lékařského záznamu, údajů a reportů z laboratoře či patologie přes obrázky různých druhů a formátů až po DICOM snímky z CT nebo magnetické rezonance. Produkt se průběžně aktualizuje a rozšiřuje o další řešení pro podporu klinického rozhodování.

První aplikace, které byly zveřejněny, jsou:

1. Clinical Trial Search App – hledání klinických studií pomocí vyhledávacích algoritmů běžících na enginu od společnosti MolecularMatch
2. Guidelines App – hledání v databázi NCCN nebo vytváření vlastních léčebných postupů
3. Publication Search App – hledání publikací pomocí vyhledávacích algoritmů

Nabídka je od roku 2019 rozšiřována o další inteligentní aplikace, aby ulehčila lékařům výběr toho nejlepšího ošetření pro jednotlivého pacienta.

Interoperabilita a standardizace formátů není jedinou výzvou, které digitální produkty obecně čelí. Firma Roche zpracovává po více než 120 let lékařská data pacientů a je si vědoma, že bezpečnost informací a ochrana dat je stěžejní. Společnost Roche proto zavedla četné kontroly, aby mohla spravovat data pacientů bezpečně a v souladu s mezinárodními a národními zákony, a zajišťuje, aby byly tyto kontroly pravidelně ověřovány externími stranami.

Infrastruktura NAVIFY® pracuje s IaaS (Infrastructure as a service), spravovanou přes Amazon Cloud Web Service (pro evropský trh úložiště ve Frankfurtu), aby mohla dodržet četné aspekty bezpečnosti a ochrany. Infrastruktura podstupuje časté kontroly, aby zajistila bezpečný přístup ke službám a zpracování citlivých dat:

1. oblast ochrany dat (kódování na více úrovních, popsáno níže)
2. kontrola přístupu (fyzická kontrola serverů, kontrola přístupu do platformy na základě udělení práv, možnost dvoufaktorového ověření atd.)
3. kybernetická ochrana (zabezpečení sítě na více úrovních, popsáno níže, pravidelné kontroly zranitelnosti systému a patch management, ročně jsou prováděny interní a externí penetrační testy, které prověřují vše, od síťového systému přes kontrolní systém až po procesy použití)
4. Change a Incident management (metodou „follow the sun“ neboli 24/7)



Infrastruktura NAVIFY® disponuje certifikací podle ISO 27001, 27701, 27017, 27018. V Prohlášení k použitelnosti jsou popsány kontrolované oblasti: management bezpečnosti informací identifikovatelných dat pacientů v rámci informačních řešení, vývoje softwaru, globálních řešení problémů a kontrolních procesů, jakož i globálních podpůrných procesů RIS včetně produktů, podpůrných procesů a IT, dálkové údržby, personalistiky a facility managementu.

NAVIFY® Tumor Board splňuje certifikační kritéria HITRUST CSF v8.1. HITRUST CSF vychází z celosvětově známých standardů, jako jsou ISO, NIST, EU GDPR, HIPAA a CCPA. Zaměstnanci Roche RIS nikdy nemají přístup k žádným datům. Průběžně je zajišťováno enkryptování dat. Kompetentní pracovníci zákazníka jsou jako jediní schopni zpracovávat data o uživateli nebo třídě integrace (připojovat, číst,

měnit nebo mazat). Pouze v případě výrobně-technických problémů může být do dat pacientů nahlédnuto, pokud se na tom shodne zákazník a firma Roche, a to jen po omezené časové období.

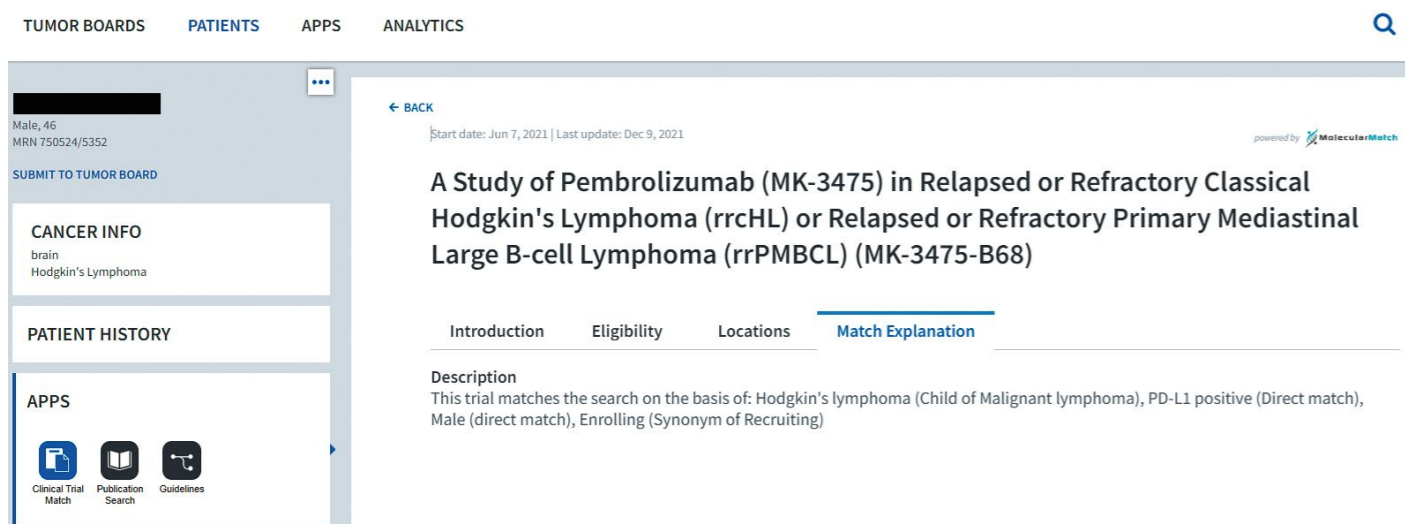
Všechna data jsou ve všech fázích zakódována pomocí AES nebo TLS se silou 256bitového klíče:

- > TLS pro datový přenos (256 bitů)
- > S3-Buckets jsou zakódovány
- > RDS zakódování
- > zakódování diskové jednotky
- > zakódování virtuálního stroje

O ochranu sítě se stará firewall se třemi úrovněmi ochrany:

- > DNS – Domain Network Service
- > VPC – Virtual Private Cloud
- > NACL – Network Access List

Všechny porty jsou na všech úrovních blokovány.



> Obr. 2: Náhled do aplikace Clinical Trial Match, software NAVIFY Tumor Board (vlastní zdroj)

HL7 v.2 – Health Level Seven version two; FHIR – Fast Healthcare Interoperability Resources; Petabyt – přibližně 1000 terabytů je petabyt (měrná jednotka uložených dat); Exabyt – přibližně 1000 petabytů je exabyt (měrná jednotka uložených dat); Hašovací algoritmus spolu s náhodně vygenerovanou „solí“ – šifrovací algoritmus určený k bezpečnému ukládání hesel, sůl v IT: používá se pro ukládání zakódovaného tvaru hesla, protože díky této „solí“ bude mít stejné heslo různý zakódovaný tvar a nebude z něj možné získat pomocí slovníkového útoku zpětně původní heslo (další stupeň ochrany nad kódování hesel, přidává zakódovanému tvaru speciální charakter, aby se nemohla stejná hesla opakovat a nešla rozluštit) – sůl zná pouze autor kódování; SLA – service-level agreement (servisní smlouva); RPO – Recovery Point Objective (jak moc dozadu lze obnovit data při útoku/ztrátě); RTO – Recovery Time Objective (za jak dlouho lze dostupná data obnovit při útoku/ztrátě); SQL injection – je to druh útoku na databázi programu, spočívá ve vsunutí škodlivého kódu do SQL (Structured Query Language – programovací jazyk) příkazu; Ransomwarevé útoky – druh kyberútku, při kterém jde o znemožnění přístupu k přístroji nebo datům (pozmění PIN nebo vypne monitor atd.).



Referenční centra a publikované výsledky

Software NAVIFY® Tumor Board, určený na podporu rozhodování, byl nejprve spuštěn a testován na západ od nás.

Referenční nemocnice:

- > Hospital Del Mar (Španělsko)
- > University Hospital of Missouri (USA)
- > Summit Cancer Centers (USA)
- > AKH Vienna (Rakousko)
- > Medical University of Graz (Rakousko)
- > Marien-Hospital Wesel (Německo)
- > MITO (Itálie)
- > Fondazione GSTU (Itálie)
- > Fakultní nemocnice Olomouc (ČR)

Důkazem užitečnosti software v klinické praxi je například studie, provedená na jednom z uvedených pracovišť, Univerzitní nemocnici státu Missouri. Ta prokázala významné

úspory času přípravy multidisciplinárních komisí napříč uživateli u 4 kategorií nádorových onemocnění, což odráží generalizovatelnost Navify Tumor Boardu. Přijetí takového řešení by mohlo zlepšit efektivitu a mít přímý ekonomický dopad na nemocnice.⁸

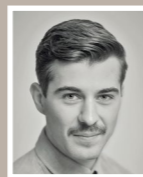
K dnešnímu dni se NAVIFY® Tumor Board testuje v několika vybraných onkologických centrech v České republice s cílem nejen zjistit, jak taková platforma funguje, ale také poskytnout zpětnou vazbu pro další vývoj.

Cíl digitalizace zdravotnictví

Cílem by mělo být zlepšení:

1. kyberochrany
2. interoperability vlivem standardizace datových formátů a komunikace
3. přesnější a větší zachycení dat nejen díky parametrizaci a jejich další vytěžování („data mining“)

Závěrem lze říct, že v minulém století byla snaha digitalizovat data zejména pro snadný přenos a sdílení. Nyní je s digitalizací spojeno motto „good for something“, za kterým se skrývá „data mining“ proces, jenž pomocí AI (Artificial Intelligence) neboli „machine learning“ a vyhledávacích algoritmů přináší přidanou hodnotu pro konkrétní pacienty v podobě lépe cílené léčby, zkrácení doby k získání definitivního výsledku, zvětšení kapacity diagnostických úseků nebo možnosti zapojit se do klinických studií.



Ing. Tomáš Procházka

ROCHE s.r.o., Diagnostics Division
Kontakt: tomas.prochazka@roche.com
Své zkušenosti přinesl z partnerské společnosti Microsoft Corporation, kde pracoval na cloudových produktech a vývoji uživatelských aplikací. Do Roche vstoupil v květnu 2020 a nyní působí na pozici Cloud Platform Specialist. Věnuje se digitálním produktům v oblasti onkologie ze skupiny „Clinical Decision Support“, od uvedení produktů na trh až po nasazení integrovaného řešení u zákazníka. Volný čas věnuje rodině, sportu, zálibě v automobilech a akvaristice.



Literatura

1. Ministerstvo zdravotnictví České republiky, Národní plán obnovy (duben 2021 – eHealth).
2. <https://www.nukib.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>.
3. https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf.
4. https://archi.gov.cz/_media/dokumenty:2020-07-17_minimalni-bezpecnostni-standard_v1.0.pdf.
5. <https://ncez.mzcr.cz/cs/dokumenty/metodicky-pokyn-poskytovatelum-zdravotnich-sluzeb-k-problematice-kyberneticke-bezpecnosti>.
6. <https://ncez.mzcr.cz/cs/dokumenty/metodicky-pokyn-poskytovatelum-zdravotnich-sluzeb-k-problematice-kyberneticke-bezpecnosti>.
7. https://brnensky.denik.cz/zpravy_region/brno-nemocnice-hacker-bohunic.html.
8. (Hammer, R. D., et al., 2020. JCO Clinical Cancer Informatics, 4, pp.757-768. Zdroj: <https://pubmed.ncbi.nlm.nih.gov/32816529/>).



NAVIFY Tumor Board je zdravotnický prostředek v podobě softwaru. Představuje cloudové řešení pracovních procesů pro onkologické týmy, které bezpečně integruje a zobrazuje relevantní agregovaná data do jediného uceleného přehledu tak, aby komise mohly posoudit, sladit a rozhodnout o optimální léčbě pacienta. Více na <https://www.navify.com/>

Mgr. Petra Trachtulcová, Ph.D.
ROCHE s.r.o., Diagnostics Division

„RBSS je, když...“

Transfuzní lékařství představuje v celé řadě klinických oborů neoddělitelnou součást komplexní léčebné péče o nemocné pacienty.

Podávání krevních přípravků a krevních derivátů je mnohdy laickou veřejností považováno za bezproblémový výkon, nicméně je nutné si uvědomit, že jakákoliv krevní transfuze či podání krevních derivátů s sebou nesou celou řadu rizik. Tato rizika a jejich velikost je možné díky soustavnému rozvoji diagnostických a technologických postupů při zpracování a skladování krve minimalizovat, nicméně je nelze nikdy zcela vyloučit.

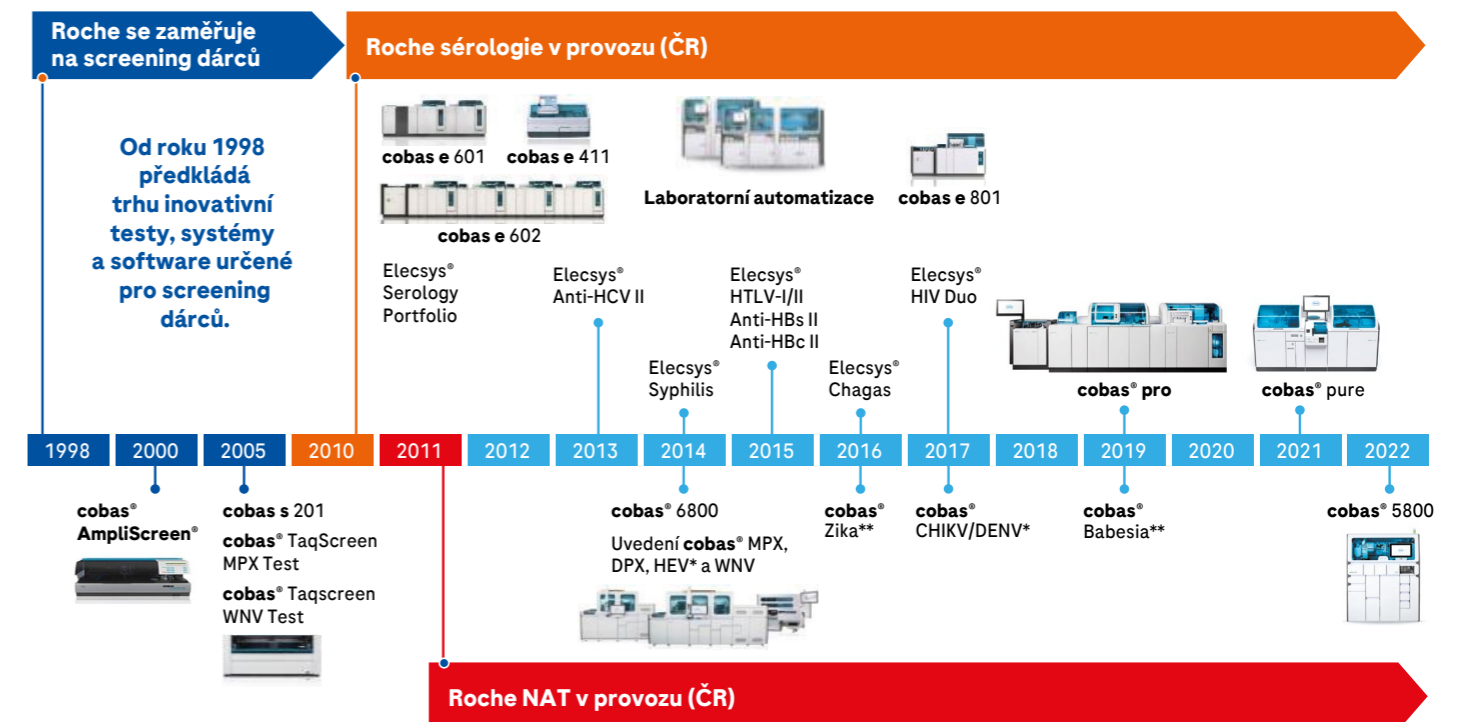
Mimořádně závažné riziko, které s sebou může nést krevní transfuze, představuje přenos infekce prostřednictvím krevního přípravku či krevního derivátu. Zásadním úkolem transfuzních zařízení a zpracovatelů plazmy při zajištění bezpečnosti krevních přípravků a derivátů je tudíž minimalizace rizika přenosu infekce.

Zajištění bezpečnosti krevních přípravků a derivátů a jejich dostupnost pro pacienty se tedy stává klíčovým prvkem a velkou výzvou jak pro zařízení transfuzní služby a zpracovatele krevní plazmy, tak i pro diagnostické firmy, které laboratorím mohou nabídnout technologie určené pro screening dárců.

Firma Roche si klade za cíl zajistit co nejkomplexnější řešení v oblasti bezpečnosti krve a krevních produktů. Strategie **Roche Blood Safety Solution (RBSS)** se snaží přispět ke zvýšení bezpečnosti krevních produktů jedinečným a komplexním řešením, které přináší laboratorním zařízením transfuzní služby spolehlivé systémy a vyšetřovací testy společně s personalizovanou laboratorní automatizací a managementem dat. Tato řešení splňují požadavky, které jsou kladeny na screening dárců jak na globální, tak na regionální úrovni.

V současné době jsou v České republice povinně všechny odebrané krevní vzorky testovány na přítomnost HIV1/2, HCV, HBV a Syphilis pomocí sérologických testů. Tento typ testů s sebou nese poměrně velké riziko nepřesného výsledku v důsledku tzv. diagnostického okna (HIV 2–3 týdny, HBV 4–6 týdnů, HCV 2–6 měsíců). Možností, jak toto riziko snížit, je rozšířit screening o molekulárně biologické metody, kterými se zjišťuje přítomnost nukleové kyseliny daného viru (Nucleic acid testing – NAT). Citlivost těchto metod je vyšší ve srovnání se sérologickými metodami, což umožňuje zkrácení diagnostického okna (u HIV o 7–9 dnů, u HCV o 59–65 dnů a u HBV o 25–30 dnů). Tento typ vyšetření není zatím v České republice legislativně předepsán, nicméně jeho značné rozšíření v řadě vyspělých i rozvíjejících se zemí celého

Neustálé zavádění inovací



> Historie uvádění na trh inovativních produktů Roche klíčových pro transfuzní lékařství