Informační a komunikační technologie ve zdravotnictví (D)

Petr Včelák

14. února 2024

Obsah

1 Počítačová a informační bezpečnost **4**
- 1.1 Nejprve ... si uděláme test! . . . 4
- 1.2 Jak se chovat? . . . 4
  - 1.2.1 Znaky . . . 5
- 1.3 Útoky . . . 5
  - 1.3.1 Typy podvodů . . . 6
  - 1.3.2 Typy útoků . . . 6
- 1.4 Jak jsou hrozby reálné? . . . 8
- 1.5 Bezpečnost ICT vs. oblast zdravotnictví . . . 10
  - 1.5.1 Papírová dokumentace . . . 10
  - 1.5.2 Elektronická zdravotnická dokumentace . . . 11
  - 1.5.3 Technické vybavení – přístroje . . . 12
  - 1.5.4 Implantované zdravotnické přístroje . . . 12
  - 1.5.5 Nositelná elektronika, sebekontrola, detekce změny chování . . . 12
- 1.6 Zásady ICT bezpečnosti . . . 13
  - 1.6.1 Aktuální software . . . 13
  - 1.6.2 Netriviální heslo . . . 13
  - 1.6.3 Nikomu nesdělujte své přihlašovací údaje . . . 13
  - 1.6.4 Zamykejte za sebou . . . 13
  - 1.6.5 Pouze své pacienty . . . 13
  - 1.6.6 Pouze služební email . . . 14
  - 1.6.7 Nekopírujte, nefoťte, nesdílejte . . . 14
  - 1.6.8 Vzdálený přístup jen z důvěryhodného počítače . . . 14
- 1.7 Zásady – výtahová kampaň (NÚKIB, 2022) . . . 14

2 Legislativa a ICT ve zdravotnictví **17**

3 Informační systémy ve zdravotnictví **18**
- 3.1 Typy zdravotnických zařízení . . . 18
- 3.2 Workflow ZZ . . . 18
- 3.3 Informační systém . . . 19
- 3.4 Typy informačních systémů ve zdravotnictví . . . 19
  - 3.4.1 Klinický modul . . . 20
  - 3.4.2 Laboratorní modul . . . 20
  - 3.4.3 Radiologický modul – PACS . . . 20
- 3.5 Data a metadata . . . 21
- 3.6 Standardizace dat ve zdravotnictví . . . 22
- 3.7 Klinická data . . . 22
- 3.8 Klasifikační systémy . . . 22

4 Datové formáty **24**
- 4.1 DASTA . . . 24
- 4.2 HL7 . . . 26
- 4.3 FHIR . . . 26
- 4.4 DICOM . . . 26

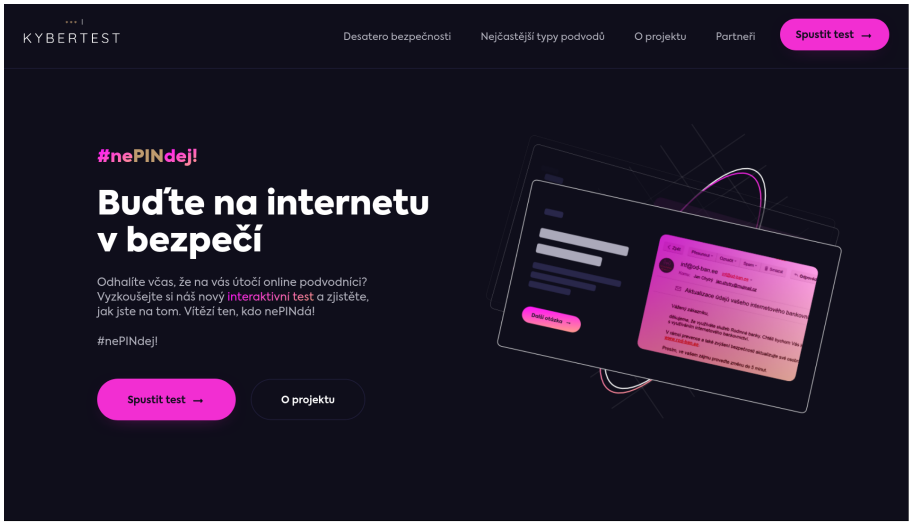
4.4.1 Historie 27
4.4.2 Modality 27
4.4.3 Popis 28
4.4.4 Akvizice dat 29
4.4.5 Informační objektový model 29
4.4.6 Metadata pro snímek 30
4.4.7 Příklady snímků 30
4.4.8 DICOM Viewer 32

1 Počítačová a informační bezpečnost

1.1 Nejprve ... si uděláme test!

Jste spíše důvěřiví nebo rozpoznáte rizika, se kterými se můžete běžně setkat? Otestujte se ...

- Kybertest (https://www.kybertest.cz/) – jak se zachováte v situacích ...



Obrázek 1: Web www.kybertest.cz.

  Jakého výsledku jste v testu dosáhli? Uchránili jste všechny své finance?

  - Jaký máte osobní dojem z otázek?
  - Který z podvodných postupů Vás překvapil?
  - Kde jste o peníze přišli?
  - Uvědomujete si, na co musíte ve skutečném světě dát pozor?

1.2 Jak se chovat?

- Prostředkem k útoku je vždy **nejslabší článek**!
- Máte-li byť minimální podezření, musíte **zpozornět** a **nejednat zbrkle**!
- Útočníkovi se podaří vás **přinutit** „chybu“ udělat.
  - časová tíseň (máte reagovat hned, nebo např. pouze do 30 minut),
  - nepozornost (otevření odkazu).
- Lepší být obezřetný a s někým se nejdříve poradit.
  - Např. kontaktovat technickou podporu uživatelů.
  - Vždy raději jiným komunikačním kanálem.
  - S útočníkem však nekomunikujte – nevolejte mu zpět ani nepište odpověď.
- Desatero bezpečnosti na internetu[1]

[1] https://www.kybertest.cz/desatero-bezpecnosti-na-internetu

1.2.1 Znaky

- Špatná čeština a gramatika může být znakem, ale těchto zjevných chyb ubývá. Útočníci se zlepšují, stejně jako jazykové modely a překladače.
- Zpráva (email, SMS, IM) může přijít i od někoho, koho znáte.
  - Může jít o falešný profil.
  - Zfalšovat je možné emailovou adresu odesílatele i jméno v hlavičce emailu.
  - Jako prevenci dotyčnému raději zatelefonujte. Může mít napadený počítač nebo sociální síť (instalace aplikací, her).
- Adresa odkazu může vypadat bezpečně, ale když na ní najedete myší, uvidíte skutečný odkaz – může vést úplně jinam – na web útočníka.
- Zabezpečené webové stránky mají na začátku adresy „https://“ (písmeno S z anglického „Secure“, zabezpečený), což znamená že komunikace není v čitelné podobě.
  - Jenže i útočník může mít web „zabezpečený“.
  - Je nutné zkontrolovat celý odkaz. Název např. banky může být jen část z podvržené adresy v odkazu.
  - Adresu elektronického bankovnictví zapište přímo do adresní řádky(!) Nikdy takto zásadní adresu nevyhledávejte, protože se můžete dostat na podvodný web, který vypadá shodně.
- Nikdy nikomu nesdělujte osobní ani finanční údaje – žádným způsobem.

1.3 Útoky

Cílem je finanční prospěch útočníka. Existuje mnoho způsobů, jak může být veden útok na vše co lze zpeněžit přímo nebo nepřímo.

- Na vaši osobu, zařízení nebo data – osobní údaje:
  - čísla k bankovním účtům, telefonní nebo jiné číslo (OP), ...
  - některé údaje sami dobrovolně sdělujete – na sociálních sítích.
- Na vaše okolí
  - Např. vytvoření falešné identity s vaší profilovou fotografií.
  - S vaší identitou osloví vaše přátele, aby vám (hned!) poslali peníze, telefonní číslo, kódy ze SMS, ...
- Na firmu/zaměstnavatele a jeho data nebo vybavení/zařízení.
  - Posloužíte jako „trojský kůň“, který mu otevře cestu.
  - Napadení:
    - počítačové sítě – nefunkční síť firmu zcela odstaví,
    - webu – nefunkční e-shop znamená finanční ztrátu před konkurencí,
    - dat – zašifrování dat (jsou nečitelné),
    - osobních údajů – např. únik
      1. osobní údaje,
      2. zvláštní kategorie osobních údajů.

Vidíme potřebu ochrany:

- dat před neoprávněným přístupem, poškozením, či pozměněním,
- elektronické komunikace před odposlechem a podvržením,
- počítačové techniky a software před záměrným poškozením.

1.3.1 Typy podvodů

Nejčastější typy podvodů[2] míří obvykle na vaši osobu nebo vaše okolí:

- podvodné emaily – phishing (rhybaření),
- podvodné SMS – smishing,
- podvodné telefonáty bankéřů, policistů, investičních poradců, ... – vishing,
- podvodné m-platby,
- podvodné platební brány,
- podvodné mobilní aplikace a udílení oprávnění k aplikacím,
- podvodné e-shopy a weby,
- podvodné veřejné WiFi sítě,
- bílí koně – money mules.

1.3.2 Typy útoků

Útočník je vždy o krok napřed před aplikacemi, které mohou útoky automaticky detekovat a varovat vás. Nový typ útoku je vždy největším rizikem, než jsou podvodné adresy, aplikace, servery a další prostředky odhaleny a běžně detekovány.

Hoax šíření klamavých informací, dezinformací.

Spam nevyžádané obchodní sdělení (nejčastěji emailem).

Phishing se do češtiny překládá jako „rhybaření“.

- Útočník nastraží falešný web s přihlašováním, který vypadá jako originál, ale je na jiné adrese.
- Uživatele přiměje zadat své přístupové údaje. Jak?
  - Např. útočník rozešle email o nutnosti změnit heslo a doplní jej o falešný odkaz.
- Jestliže uživatel odkaz použije, vyplní uživatelské jméno a heslo, útočník uživatele chytil jako rybu na návnadu.
- Kombinaci uživatelského jména a hesla získá útočník! Může se za vás vydávat.
- Útočník uživatele obvykle do skutečného webu přihlásí, aby nevzbuzoval podezření.
- Poučení: Všude, kde musíte zadávat své uživatelské jméno a heslo (přihlášení, změna hesla, ...) musíte být obezřetní a zkontrolovat:
  - aktuální adresu v prohlížeči,
  - platnost certifikátu.

  Web banky, emailové schránky, nemocničního systému, sociálních sítí, ... navštívit vlastním zadáním adresy do prohlížeče, příp. mít odkaz uložen v záložkách.

  Obecně odkazy v emailech nepoužívat nebo považovat za nebezpečné. Některé prohlížeče mají detekci a mohou vás varovat. Nikoliv však vždy nebo včas.

Malware je software s cílem infiltrovat nebo poškodit počítačový systém.

- Činnost:
  1. ovládnutí infikovaného systému – váš počítač se stane součástí *botnetu*, tj. sítě infikovaných strojů, které útočník vzdáleně ovládá:

[2] https://www.kybertest.cz/nejcastejsi-typy-podvodu

- rozesílání spamu,
- sledování aktivity uživatele (komunikace, kontakty, přihlašovací údaje),
- distribuované útoky (DDos)
- ukládání a distribuce nelegálního obsahu (např. dětská pornografie),

2. destruktivní – smaže/přepíše/zašifruje data,

- Jsou to
  - *Počítačový vir* napadá ostatní aplikace jejichž součástí se po napadení stanou. Vir je aktivní obvykle při každém spuštění infikovaného programu.
    Poučení: nestahovat a neinstalovat z internetu úplně vše, mít aktuální antivir.
    - *Spyware* je virus, odesílá data z napadeného počítače bez vědomí uživatele.
  - *Počítačový červ* se dokáže šířit aktivně sám (vir nikoliv), protože využívají chyby operačních systémů a zabezpečení.
    Poučení: pravidelně aktualizovat operační systém i všechny aplikace a používat firewall.
  - *Trojský kůň* předstírá užitečnou funkcionalitu (často jednoduché zábavné hry, ale může se jednat i o aplikace získané z nedůvěryhodného zdroje) a přitom (nebo už při instalaci) vykonává škodlivou činnost – instalace dalších aplikací, zapojení počítače do botnetu, manipulace s daty, prohledávání sítě a síťových disků, ...
    Poučení: Aktualizovaný antivirový program, operační systém a instalace software z důvěryhodných zdrojů.
  - *Adware* je software zobrazující uživateli reklamy změnou obsahu zobrazovaných webových stránek, kam přidává vlastní reklamní bloky.
  - *Keylogger* slouží k zachytávání, záznamu a odeslání znaků psaných na klávesnici. Cílem je získat hesla, osobní/obchodní korespondenci nebo důvěrné dokumenty bez vědomí uživatele.
  - *Ransomware* provede zašifrování dat nejen na napadením počítači, ale často primárně na připojeních (sdílených) síťových discích, kde mohou být zálohy, apod. Pro dešifrování je nutné útočníkovi zaplatit výkupné (např. Bitcoin).

DDoS je zkratka z anglického *Distributed Denial of Service* a jedná se o útok způsobující **přetížení** služby. Útoky vedou útočníci prostřednictvím botnetů, kdy obrovským množstvím požadavků zahltí webový server a web se pro běžné uživatele zdá být nedostupným. Obvykle je výsledkem pouze nedostupnost, nikoliv narušení dat.

Koláčky zejména tzv. „sledovací koláčky“ (tracking cookies) zajišťují sledování aktivity uživatele napříč weby. Obecně jsou koláčky (cookies) neškodným textem a běžnou součástí webů (zapamatování si přihlášeného uživatele). Ke sledování byly zneužity pro přesnější cílení reklamy na internetu prostřednictvím množství reklamních systémů (Google, Facebook/Meta, ...). Pro zájemce viz Druhy reklamních systémů[3].

Řešení:

- Weby by měly uživateli dávat na výběr jaké koláčky akceptuje.
- Současně prohlížeče umožňují nastavení, zda na daném webu koláčky třetích stran akceptovat.
- Existují rozšíření do prohlížeče, které dávají větší možnosti při zajištění blokace.

Reálně je pro sledování používáno více metod i současně:

- tzv. otisk prohlížeče,

[3] https://www.jakpsatweb.cz/reklama/systemy.html

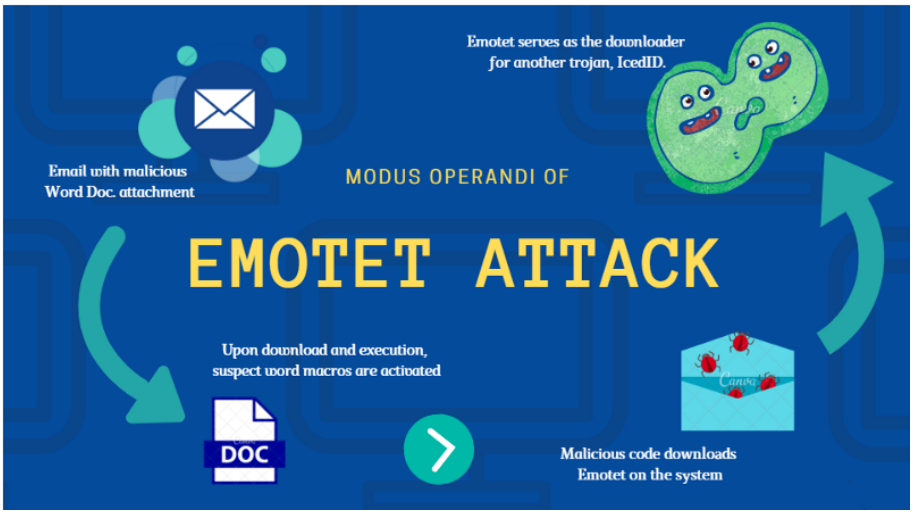
- identifikátory reklamních systémů doplněné jako parametr (v odkazu „kdekoliv“ za otazníkem) v odkazech vedoucích na jiné weby, např. parametr *fbclid* (Facebook Click Identifier): má spárovat pohyb a činnost uživatele na Facebooku před proklikem s tím, co člověk pak na cílovém webu dělá (je-li na webu použit reklamní systém). Odkaz je navíc zbytečně dlouhý. Porovnejte:

```
https://https://example.cz/?fbclid=IqAB-1iRBiUNKQmM1Hpk5hjLWWglUGcnu8d4NgYjdQD22epPggd
https://https://example.cz/
```

Zákaz koláčků třetích stran nebo právě těch sledovacích nemusí cílení reklamy zabránit. Podobně je to s technologií JavaScriptu, když je na webech používána. Může se stát, že blokací některých částí webu (koláčků, JavaScriptu) bude vypadat web jinak, nebo chybně fungovat. Ostražitost by měla být v případě míst, kde zadáváte osobní údaje (své i cizí).

1.4 Jak jsou hrozby reálné?

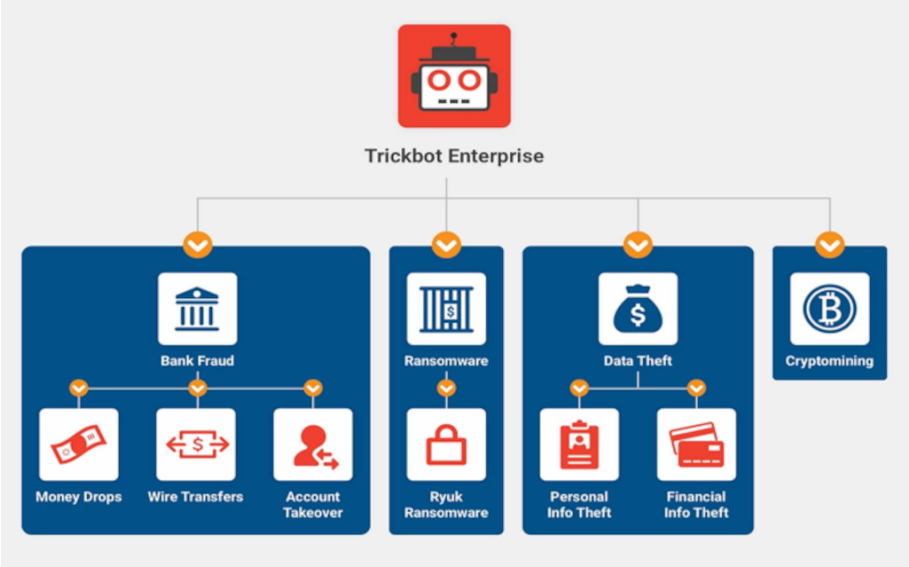
- Web České televize – DDoS útok, 21. 5. 2019.
  - Výsledek?
    - Pouze nedostupnost.
    - DDoS útok nemívá za cíl poškodit data, ale znepřístupnit služby po dobu útoku nebo následného zotavení se po obrovské zátěži.
- **Nemocnice Rudolfa a Stefanie Benešov** – ransomware Ryuk, 2019.
  - Výsledek?
    - Cca tři týdny omezení provozu – omezení lékařských výkonů, zrušení plánovaných vyšetření a operací.
    - Škoda cca 59 milion korun.
  - Jak? Ransomware *Ryuk* je instalován pomocí dalších kmenů malwaru jako *Emotet* a *Trickbot*.
    - Na začátku je phishingový email s infikovanou přílohou a **neopatrný příjemce přílohu otevře**/spustí.
    - *Emotet*[4] – nakažená příloha ve formě Word dokumentu s makry.



Obrázek 2: Modus operandi malwaru Emotet.

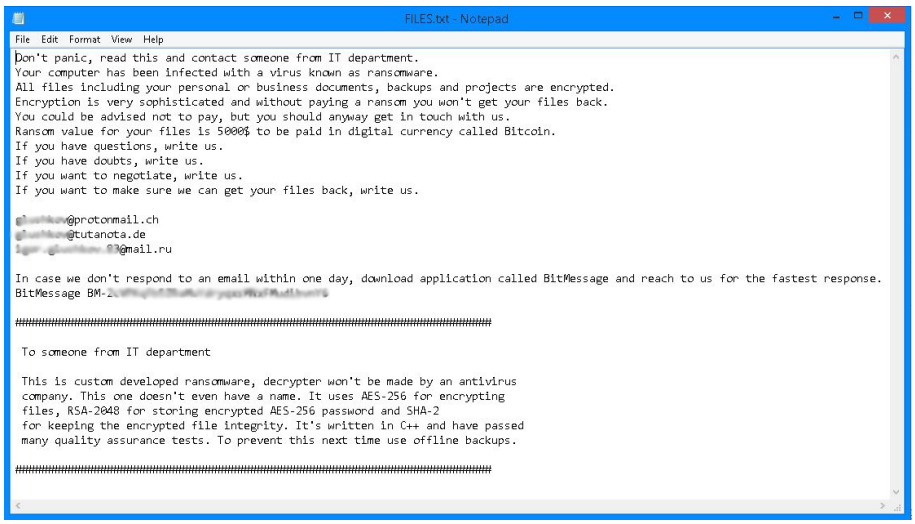
[4]https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

* a Trickbot[5] byl původně trojský kůň, ale nyní modulární a sofistikovaný. Na počátku je nakažená příloha s makry.



Obrázek 3: Cíle malwaru/trojana TrickBot. Zdroj Bleeping computer.

- **Fakultní nemocnice Brno** – ransomware Defray (Defray777), 13. 3. 2020.
  - Po napadení snaha získat výkupné.
  - Provoz byl obnoven po čtyřech týdnech.



Obrázek 4: Ransomware Defray zanechá uživateli zprávu i pro IT oddělení, že mají pro příště používat tzv. offline zálohy.

- **Psychiatrická nemocnice v Kosmonosech** – ransomware, 27. 3. 2020.
  - Pravděpodobně zneužití nedostatečně zabezpečených serverů.
  - Útok odstaví bezpečnostní řešení, aktivuje škodlivý kód, který zašifruje vše dostupné(!) – lokální i síťové disky.

[5] https://learn.cisecurity.org/TrickBot-Not-Your-Average-Hat-Trick-A-Malware-with-Multiple-Hats

  - Provoz obnoven po deseti dnech.

- a další. Zdroj Avast Threat Labs. Nemocnice pod náporem hackerů: Jak proběhly nejznámější kyberútoky na české nemocnice[6]. 29. duben 2021. Citováno 10. 9. 2022.

Cílem nejsou pouze zdravotnická zařízení. Útoky probíhají nepřetržitě na všechna zařízení v síti.

- Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB; https://www.nukib.cz/).
- Kybernetické incidenty pohledem NÚKIB (září 2022)[7]

1.5 Bezpečnost ICT vs. oblast zdravotnictví

Bezpečnost v oblasti zdravotnictví může ovlivnit nejen provoz zdravotnického zařízení, ale současně technického vybavení a moderních technologií používaných od diagnostiky, přes léčbu (nebo její podporu), až po dispenzarizaci pacientů. Počítačová síť propojuje pracovní stanice, odborná pracoviště a jejich technické vybavení, které zahrnuje také všechny používané přístroje.

Nejcennější jsou původní **data**.

- Počítač a aplikace můžeme přeinstalovat.
- Hardware opravíme nebo vyměníme.
- Co data?
  - Některá data nahradit nelze – např. CT vyšetření, fotografie.
  - Některá lze obnovit za vysokou cenu (časovou, finanční, úsilí). Bakalářskou/diplomovou práci, výroční zprávu lze vypracovat znovu. V případě ransomware zaplatit vysoké výkupné.

Potřebujeme:

důvěryhodnost dat – zaručit důvěru v data a soukromí pacienta (nikdo neoprávněný nemá přístup),

integritu dat – nikdo s daty nemanipuloval (neměnil);

dostupnost dat – k datům je potřeba se dostat; výpadek způsobí problémy při poskytování zdravotní péče.

1.5.1 Papírová dokumentace

- Existuje fyzicky na konkrétním místě.
- Získat lze pouze v daném místě.
- Ochrana
  - Pouze fyzicky – přístup do archívu, zámek do ordinace/kartotéky.
  - Záloha – neexistuje (kopie).
- Rizika?
  - Přírodní živly – voda/vlhkost, oheň, ...
  - Zcizení – útočník musí být v daném místě fyzicky.

[6] https://blog.avast.com/cs/nemocnice-pod-naporem-hackeru-jak-probihaji-kyberutoky-na-ceske-nemocnice
[7] https://www.nukib.cz/download/publikace/vyzkum/2022-09_Kyberneticke_incidenty.pdf.

1.5.2 Elektronická zdravotnická dokumentace

- Existuje pouze v datovém úložišti.
  - Lokálním – získat lze pouze v daném místě.
  - Vzdáleném – získat lze z více míst i současně.
- Ochrana – elektronická
  - Autentizace – ověření identity subjektu – přihlášení/odhlášení.
    - Odpověď na otázku: „Kdo to je?“
      Konkrétní osoba, např. „Tomáš Marný“ – zjistíme identitu.
    - Následuje autorizace.
  - Autorizace – souhlas, schválení, umožnění provedení konkrétní operace (přístupu) k datům.
    - Odpověď na otázku: „Co může dělat?“
      Zobrazit pacienta, klinickou událost, vystavit žádanku, ...
    - Reálně to určují konkrétní přidělené role subjektu (uživatele). Nejčastěji na základě pracovní smlouvy a úvazků.
      - Lékař, střední zdravotnický personál, manažer, ...
  - Audit dat
    - Odpověď na otázku: „Co, kdy, kde a kdo dělal?“
      - Kdy a odkud se přihlásil/odhlásil.
      - Kdy a jaká data (např. klinické události) prohlížel/editoval/vytvářel/smazal.
  - Záloha dat
    - Data musí být současně na **minimálně dvou** fyzicky oddělených místech.
    - Různé typy a aspekty dat potřebují různé typy zálohování.
      - Objem dat – denní, měsíční, roční přírůstky dat.
      - Typ dat – textové, tabulky, fotografie, databázové systémy, serverové služby (email, web, kalendář, adresář/uživatelé).
      - Četnost a časová náročnost – kompletní vs. přírůstkové.
      - Zabezpečení záloh – šifrování, lokální vs. vzdálené.
      - Zálohovací technologie – diskové úložiště, páskové jednotky, ...
  - Plán obnovy (recovery plan) – měl by existovat a být **ověřen**(!) pro případ havárie.
    - Úspěšnost a rychlost obnovy ovlivní funkčnost/použitelnost a aktuálnost existujících záloh.
- Rizika – eliminují/minimalizují bezpečnostní politika, zálohy, plán obnovy.
  - **Lidský faktor**
    - IT oddělení – přetíženo nebo nedostatečně zajištěno (pouze externista, poloviční úvazek, ...)
    - **Personál** (ne)vědomě **umožní průnik** do sítě – lékaři, střední zdravotnický personál, ostatní personál.
  - Data přístupná lokálně/vzdáleně
    - **únik dat** po útoku – phishing, malware/ransomware
    - zašifrování a požadavek na výkupné.
  - Selhání HW (vadný disk, paměť) – závažná ztráta dat, především pokud byla data pouze lokálně a bez existence zálohy.

1.5.3 Technické vybavení – přístroje

Současné přístroje jsou často označovány jako „chytré“. Je to generace technicky (nikoliv nutně z pohledu obsluhy) složitějších přístrojů[8] – mají vlastní operační systém a softwarové vybavení běžící nad vlastní výpočetní jednotkou (procesor, paměť, úložiště dat), a komunikující po počítačové síti zdravotnického zařízení.

Historicky měly přístroje pro administraci jednoduchá rozhraní, často nezabezpečená, anebo zcela nedostatečně. Přístroje měly ve firmware[9] např. definované přístupové údaje bez možnosti změny (přímý útok) nebo nepodporují šifrovanou komunikaci (lze odposlechnout).

Správa vybavení jako jsou anesteziologické přístroje, dávkovače/infuzní pumpy, diagnostické přístroje, monitory životních funkcí, zobrazovací metody (např. CT nebo RTG), a mnoho dalšího bylo pro administrátory a servisní techniky snazší, ale tím bylo současně rostoucí riziko nebezpečí v případě útoku prostřednictvím sítě.

Prostřednictvím internetu lze vyhledat velké množství přístrojů s veřejně přístupným rozhraním. Bezpečnostní výzkumníci Scott Erven a Mark Collao v roce 2015[10] (video na Youtube.com[11]) objevili nejmenovanou zdravotnickou organizaci se 12 000 zaměstnanci a 3 000 lékaři, která má do sítě internet vystavila na 68 000 medicínských systémů. Alarmující je, že se jednalo:

- o 21 anesteziologických systémů,
- 488 kardiologických systémů,
- 67 nukleárně medicínských systémů,
- 133 infuzních systémů,
- 31 kardiostimulátorů,
- 97 MRI,
- a 323 zařízení pro archivaci a komunikaci snímků obrazových diagnostických metod.

Vést útok na tento typ přístrojového vybavení by mohl mít fatální důsledky.

1.5.4 Implantované zdravotnické přístroje

Dalším typem elektroniky jsou implantované zdravotnické přístroje jako jsou např. kardiostimulátory, inzulínové pumpy nebo neurostimulátory. Implantovaný přístroj má pacient nepřetržitě i několik roků, než je vyměněn za nový. Způsob pro čtení a konfiguraci může být prostřednictvím kabelu nebo bezdrátově, kdy se přiloží čtečka elektromagnetického záření nebo rádiového signálu. Nové přístroje přinášejí další a snazší cesty komunikace jako jsou *bluetooth* nebo *webová rozhraní*. To může mít i negativní důsledky, protože se komunikační cesta otevírá širšímu okruhu osob ...

1.5.5 Nositelná elektronika, sebekontrola, detekce změny chování

Významně se projevuje fenomén nositelné elektroniky a mHealth představující lékařskou praxi a veřejné zdraví podporované prostřednictvím *mobilních zařízení*.

Jednou částí je obecně nositelná elektronika, kde se prakticky nejedná o přístroj určený ke zdravotnickým účelům. Jsou to chytré hodinky, náramky nebo sporttestery používané pro sport, volný čas nebo jako „módní“ doplněk.

[8] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4516335/

[9] Firmware zajišťuje řízení hardware na nejnižší úrovni. Jedná se o software, který poskytuje základní fungování konkrétního hardware přístroje, komunikaci v jeho bezprostředním okolím, např. s ostatním softwarem v zařízení. Firmware obvykle vytváří a dodává výrobce přístroje/zařízení.

[10] https://www.theregister.com/2015/09/29/thousands_of_directly_hackable_hospital_devices_found_exposed/

[11] https://www.youtube.com/watch?v=ZusL2BY6_XU

Druhou část představuje **sebekontrola** (self-monitoring) nebo také domácí/laické měření např. kontroly hladiny krevního cukru glukometrem viz např. Selfmonitoring a jeho význam v moderní léčbě diabetu[12] (Kateřina Štechová, 2017).

Zmínit je možné tzv. **SOS tlačítka**, která slouží pro přivolání pomoci, odesílá SMS, vytáčí telefonní hovor, zavolá lékařskou pomoc, apod. Součástí může být detektor pádu nebo GPS lokátor. Setkat se můžeme s podobou přívěšku nebo hodinek.

1.6 Zásady ICT bezpečnosti

1.6.1 Aktuální software

Instalace bezpečnostních záplat by měla být samozřejmostí pro operační systém i používané aplikace. Automatická a pravidelná by měla být také aktualizace antivirové databáze. Tuto úlohu by mělo zajistit primárně vaše IT oddělení. Vlastní zařízení musíte udržovat sami.

1.6.2 Netriviální heslo

Do informačního systému, kde jsou osobní údaje, je potřeba se vyvarovat se triviálních hesel jako jsou „12345“, „borec“, „plice“, rok narození nebo jméno psa.

- Vyberte pro vás snadno zapamatovatelnou sekvenci znaků/slov, kde jsou malá písmena, velká písmena, číslice, a nějaký další znak (např. interpunkce).
- Vyhněte se raději znakům s diakritikou, protože na jiném oddělení nemusí být k dispozici české rozložení klávesnice, tj. nepřihlásíte se.
- Nepoužívejte ani heslo, které už máte kdekoliv jinde (např. v soukromé emailové schránce, na sociální síti nebo e-shopu), protože by mohlo uniknout a ohrozit zdravotnické zařízení.
- Nevystavujte jej na lístečku na stole nebo monitoru. Tím bylo prolomeno!

1.6.3 Nikomu nesdělujte své přihlašovací údaje

Zásadně **nikdy s nikým nesdílíte** své heslo, které máte do informačního systému. Nebo snad PIN k platební kartě také půjčujete kolegům? Každý zaměstnanec má své uživatelské jméno a heslo, pod kterým pracuje. Svou identitu používáte vždy výhradně Vy sami! Heslo nesmíte sdělit nikomu jinému – ani kdyby jej chtěl někdo z IT oddělení nebo samotný ředitel.

Jestliže nemá přidělen přístup, musí oslovit svého nadřízeného pracovníka, aby mu bylo potřebné oprávnění řádně přiděleno. Zneužití je velmi jednoduché. Chybný záznam, neoprávněný přístup k osobním údajům pacienta, klinickým událostem, apod. Zodpovědnost máte jednoznačně vy – ostatně logy při auditu poskytnou jasné důkazy s vaším jménem.

1.6.4 Zamykejte za sebou

Musíte-li opustit svoji pracovní stanici, vždy se **odhlaste** z informačního systému, anebo **uzamkněte** pracovní stanici, pokud je chráněna heslem – měla by být! Volně přístupný informační systém by mohl kdokoliv zneužít – kolega nebo třeba pacient. I prohlížení dokumentace bude evidováno s vaší identitou.

1.6.5 Pouze své pacienty

Pracujte pouze se svými pacienty. Informační systém ze zákona zaznamenává veškerou aktivitu a jakékoliv činnosti (prohlížení, změna) jsou evidovány. Pacient může žádat přehled přístupů do jeho dokumentace. Z provedeného auditu bude vše poznat a může vás to stát nejen pracovní místo, ale také soudní řízení.

[12] https://www.solen.cz/pdfs/lek/2017/03/03.pdf

1.6.6 Pouze služební email

Vždy důsledně oddělujte pracovní a soukromé záležitosti. Veškerou pracovní komunikaci realizujte prostřednictvím své emailové schránky u zaměstnavatele (důvěryhodnost). Zcela se vyvarujte použití osobní emailové schránky jako jsou například služby na Seznam.cz nebo Gmail.com. Přihlašovací údaje (emailová adresa a heslo) mohou uniknout a obsah schránky by se stal přístupným, což by znamenalo ohrožení zdravotnického zařízení nebo únik dat.

1.6.7 Nekopírujte, nefoťte, nesdílejte

V klinickém systému je přímo funkce, která zajistí kopii předchozího vyšetření nebo výsledků do nové klinické události.

Kopírování prostřednictvím schránky operačního systému se vyhněte. Schránku mají přístupnou všechny aplikace a její obsah může být dostupný i po odhlášení se. Pokud schránku přece jen použijete, označte a zkopírujte do ní následně nějaký neškodný text.

Podobná situace je focení na své mobilní zařízení. V případě zobrazených osobních údajů tím dochází k úniku, jestliže mobilní zařízení nepatří zaměstnavateli. Fotografie se mohou automaticky synchronizovat s cloudovým úložištěm, čímž opustí zdravotnické zařízení, Českou republiku nebo dokonce Evropskou unii.

Pro předání dat na jiné oddělení nebo do jiného zdravotnické zařízení použijte vhodný komunikační kanál. Zdravotnické zařízení bude mít pravděpodobně zabezpečené (šifrované) interní úložiště nebo existují systémy jako je PACS, ePACS, apod.

V krajním případě by mohl být řešením CD, externí disk nebo flash disk, ale pouze pokud data zašifrujete nebo alespoň použijete heslem chráněný ZIP soubor, do kterého všechna data umístíte. Nebude tak na médiu přímo v čitelné podobě.

Smazání souboru nic neznamená ani na flash disku. Dokud není místo, kde byl soubor uložen přepsán, obvykle jej bude možné poměrně snadno obnovit. Proto na disku nenechávejte nešifrované soubory, ani je přímo na disku nedešifrujte (nejprve zkopírujte do služebního počítače).

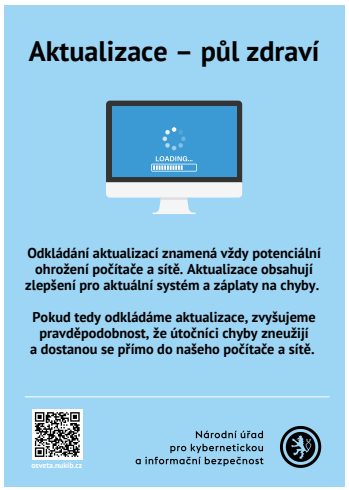
1.6.8 Vzdálený přístup jen z důvěryhodného počítače

V případě zabezpečeného vzdáleného přístupu (VPN) k informačnímu systému použijte pouze svůj soukromý počítač (aktuální), ze zabezpečeného domácího připojení. Nikoliv na veřejnosti (někdo bude za vámi) nebo prostřednictvím nezabezpečené bezdrátové sítě (např. kavárna, knihovna, obchody, ve vlaku).

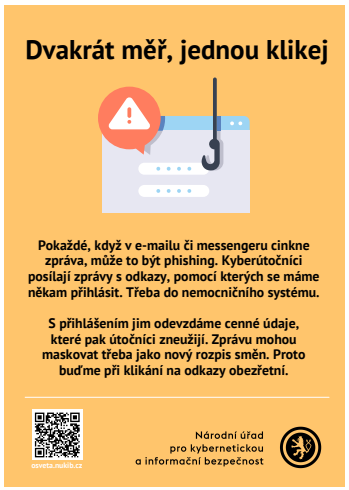
1.7 Zásady – výtahová kampaň (NÚKIB, 2022)

Článek V českých nemocnicích probíhá „Výtahová kampaň“[13] (NÚKIB, říjen 2022) zdůrazňuje problematiku formou plakátů se základními pravidly bezpečného pohybu v kyberprostoru. Akce FBI: Kampaň pro zdravotníky (nukib.cz)[14] je v rámci „Festivalu bezpečného internetu (FBI)[15]“ (říjen 2022).

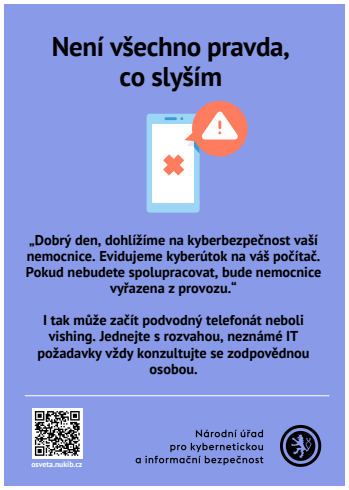
[13] https://www.nukib.cz/cs/infoservis/aktuality/1893-v-ceskych-nemocnicich-probiha-vytahova-kampan-2/
[14] https://osveta.nukib.cz/mod/page/view.php?id=2385
[15] https://osveta.nukib.cz/course/view.php?id=111



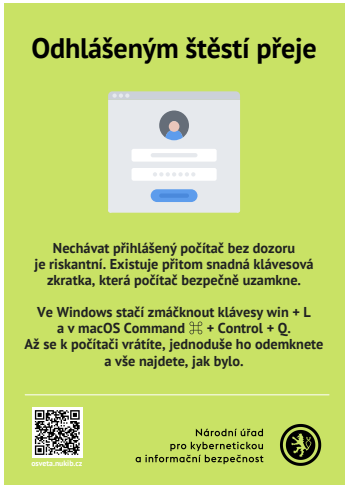
Obrázek 5: Plakát „*Aktualizace – půl zdraví*“. Zdroj NÚKIB.



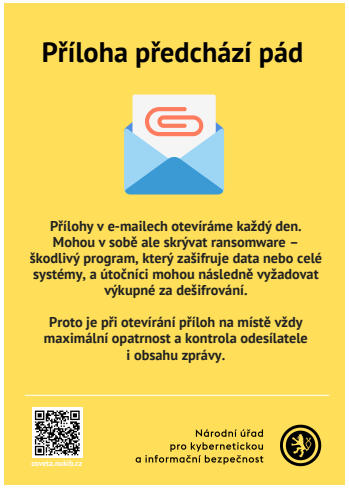
Obrázek 6: Plakát „*Dvakrát měř, jednou klikej*“. Zdroj NÚKIB.



Obrázek 7: Plakát „*Není všechno pravda, co slyším*“. Zdroj NÚKIB.



Obrázek 8: Plakát „*Odhlášeným štěstí přeje*“. Zdroj NÚKIB.



Obrázek 9: Plakát „*Příloha předchází pád*“. Zdroj NÚKIB.

2 Legislativa a ICT ve zdravotnictví

ICT oblasti se týká tzv. Obecné nařízení o ochraně osobních údajů (GDPR). Zejména tzv. **zvláštní kategorie osobních údajů**, které „vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení, členství v odborech, **zdravotním stavu** či o sexuálním životě nebo sexuální orientaci fyzické osoby.“ Zvláštní kategorie osobních údajů byla známa původně pod označením „citlivé osobní údaje“.

Zákonná ochrana osobních údajů se nevztahuje jen na pacienty, ale i např. personál (zaměstnance). V případě zaviněného úniku dat se může jednat např. o poškození dobrého jména (zaměstnavatele) nebo trestný čin. Důsledky mohou být různé – náhrada škody pro nesplnění povinnosti k odvrácení škody, ukončení pracovního poměru a další.

3 Informační systémy ve zdravotnictví

3.1 Typy zdravotnických zařízení

Zdravotnická zařízení (ZZ) rozlišujeme dle typu:

- první styk
  - PLD, PLDD, ZL, GA, LS PP;
- ambulance
  - oční, ortopedie, psychiatrie, neurologie, dermatologie, rehabilitace,
  - urologie, ORL, alergologie, . . .
- laboratoř
  - cytologie, klinická biochemie, hematologická laboratoř, mikrobiologie;
- lékárna/výdejna
  - lékárna, oční optika, optometrie;
- hospitalizace
  - nemocnice – různé typy/velikosti,
  - LDN, odborný léčebný ústav (psychiatrická léčebna);
- zdravotní doprava
  - převozová sanitka, ZZS, LZS;
- ostatní
  - domácí péče, hygienická služba, lázeňské ZZ, porodní asistentka.

3.2 Workflow ZZ

Workflow je závislé na kontextu:

- ambulantní dokumentace,
- radiologie, PACS,
- bioptické a patologické laboratoře,
- hospitalizace, evidence podávání léčiv, ošetřovatelská dokumentace,
- nemocniční infekce,
- specializovaná oddělení – gynekologie/porodnice, kardiologie, operace,
- rehabilitace,
- logistika (léky, materiál), vykazování zdravotní péče,
- vyvolávací systém pro čekárnu, informované souhlasy,
- nežádoucí události, lékové interakce.

Příklad workflow v ambulanci:

1. příchod do čekárny,

2. zadání údajů sestrou,
3. vyšetření pacienta lékařem,
4. vytvoření lékařské zprávy,
5. objednání pacienta k další návštěvě,
6. tisk potřebné dokumentace,
7. vykázání výkonů plátci zdravotní péče.

3.3 Informační systém

Jaký je účel IS?

- Tvorba, shromažďování/ukládání, zobrazování, zpřístupnění, zpracování a řízení.

Jaké čtyři komponenty má IS?

- Lidé, procesy, technologie a data.

Co je hlavní/primární cíl a účel IS ve ZZ?

- Podpora zdravotní péče o pacienta + administrace.

Znáte jaké existují typy zdravotnického IS?

- Klinický, laboratorní, nemocniční, radiologický, ...

3.4 Typy informačních systémů ve zdravotnictví

Mezi typy informačních systémů ve zdravotnictví patří:

- ambulantní
- a nemocniční.

Tyto systémy komunikují s množstvím dalších informačních systémů jako jsou:

- Česká správa sociálního zabezpečení (neschopenky),
- pojišťovny (vykazování),
- Státní ústav pro kontrolu léčiv (eRecept),
- záchranné služby (urgentní příjem).

Ze zákona existuje řada zdravotních registrů, které jsou používány.

3.4.1 Klinický modul

Klinický modul je podstatou informačního systému, protože je orientován na pacienta a klinické události, kterou si lze představit jako jakoukoliv jednotlivou činnost, kterou s pacientem provádíme (a vykazujeme). Informační systém poskytuje těsnou integraci kódování péče pro vykazování zdravotním pojišťovnám.

Vše začíná vyhledáním (příp. založením nového) pacienta, následuje vytvoření klinické události, kde může být součástí anamnéza, popis/výsledek vyšetření, předepsání léků, vystavení neschopenky, žádanky pro další odborné vyšetření specialistou, až po objednání na další termín. Práci může zjednodušit např. funkce pro zobrazení objednaných pacientů, nebo frontu již čekajících pacientů (správa čekárny).

V případě nemocnic je řešen celý proces hospitalizace pacienta dokumentující vše od příjmové zprávy (anamnéza, status praesens, vstupní diagnóza a plán péče), chorobopisu s dekurzy, žádanky na vyšetření, kumulativní nálezy, až po propouštěcí zprávu.

Jednotlivé části klinického modulu na sebe navazují. Zejména v nemocnicích nebo větších zdravotnických zařízeních pak žádanku vystavenou ambulantním specialistou příslušné oddělení rovnou vidí (žádanka, příp. objednávka) a po příchodu pacienta na ni přímo reaguje. Funguje to také opačně, tj. výsledek vyšetření je okamžitě k dispozici u žádajícího oddělení a žádanka je označena za dokončenou.

3.4.2 Laboratorní modul

Realizuje kompletní provoz laboratoře. Vstupem jsou žádanky a vzorky k laboratornímu zpracování. Vzorky/zkumavky jsou značeny jménem, ale také unikátním čárovým kódem, který celý proces automatizuje a zabraňuje záměně pacientů. Na specializovaných přístrojích proběhne vyšetření vzorků a z přístrojů jsou přijímána data. Pracovník zajistí kontrolu výsledků, vyhodnocení a na závěr následuje předání laboratorních výsledků žádajícímu pracovišti.

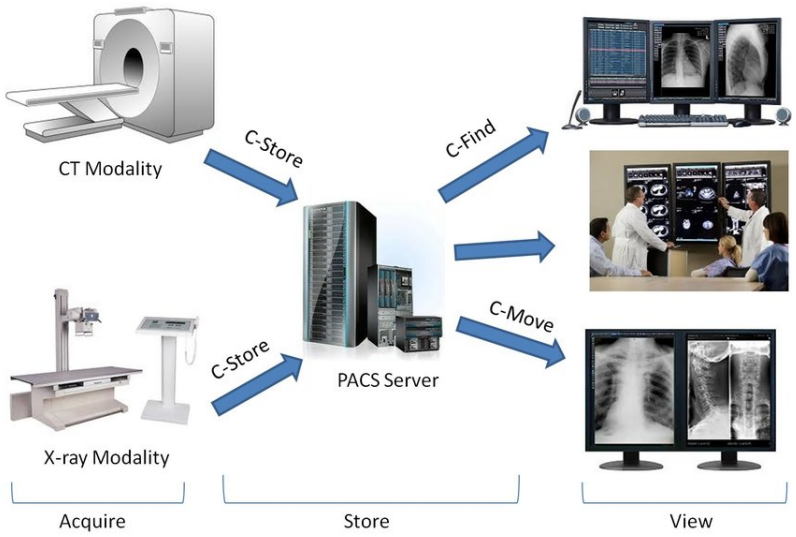
Pro laboratorní data se v ČR používá formát DASTA s množstvím číselníků. V tomto případě *Národní číselník laboratorních položek*.

3.4.3 Radiologický modul – PACS

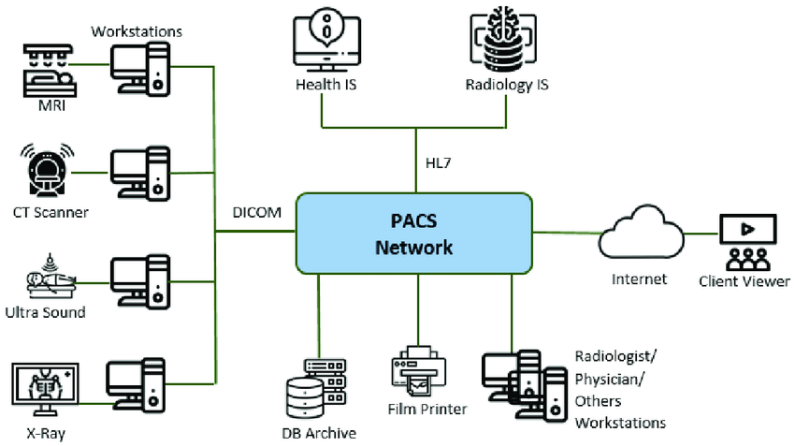
Radiologický modul je určen pro zobrazovací metody jako jsou např. RTG, CT, MR, SONO. Je propojený s použitým informačním systémem, kde doplňuje klinický modul o možnost výsledků zobrazovacích metod. Často je to prostřednictvím *Picture Archiving and Communication System* (PACS), který má čtyři komponenty:

1. Lékařská zobrazovací zařízení, jako jsou MRI, CT, rentgenové systémy, ultrazvukové přístroje a další.
2. Zabezpečená síť pro výměnu a distribuci dat z vyšetření pacienta.
3. Pracovní stanice nebo mobilní zařízení DICOM pro prohlížení, opětovné zpracování a interpretaci snímků.
4. Dále archivy a tiskárny pro ukládání a vyhledávání snímků a související dokumentace a zpráv.

PACS zajišťuje integraci komponent ve zdravotnickém zařízení – zachycení, uložení, prohlížení a sdílení snímků interně nebo externě, a umožňuje realizovat vzdálenou diagnostiku spočívající v interpretaci snímků.



Obrázek 10: Komponenty PACSu a ukázka DICOM zpráv. [Kamran Sartipi]



Obrázek 11: Referenční návrh infrastruktury sítě PACS. [Steffen Wendzel]

3.5 Data a metadata

- Data
  - strukturovaná, nestrukturovaná, semi-strukturovaná.
- Metadata – strukturovaná data s informaci o popisovaných datech:
  - popisná – o obsahu dat, lokalizace, porozumění,
  - strukturální – relace a vztahy mezi popisovanými daty/zdroji,
  - administrativní – vznik a přístup:
    - technická – nutná pro dekódování nebo zobrazení záznamů (formát, velikost souboru, komprese),
    - archivační – dlouhodobé zachování zdroje i správu (kontrolní součty),
    - právní – ochrana práv (licence, práva držitele, důvěrnost),
  - značkovací jazyk – přímo v původním obsahu.
- Data != Metadata? vs. Strukturovaná data == Metadata?

3.6 Standardizace dat ve zdravotnictví

- Cíl
  - vzájemné porozumění mezi lékaři,
  - eliminovat různé značení,
  - sjednotit formáty dat.
- Možnosti
  - nutnost shodného jazyka → latina,
  - klasifikace – třídění, zařazování objektů do tříd,
  - nomenklatura – systém pojmenování, názvosloví, terminologie,
  - tezaurus – slovník, lexikon, velký slovník.

3.7 Klinická data

- Anamnéza, vyšetření fyzikální/specialistou, pomocné metody:
  - numerická – laboratorní výsledky, věk,
  - textová – lékařská zpráva, poznámky, jména,
  - kódovaná – MKN/ICD, číselníky, laboratorní výsledky, škály/skóre,
  - obrazová:
    - digitalizované dokumenty, fotografie,
    - CT (computed tomography),
    - MRI (magnetic resonance imaging),
    - PET (positron emmision tomography),
    - RTG (radiografie),
    - SPECT (single proton emission computed tomography),
    - ultrazvuková tomografie, nukleární medicína,
    - video sekvence (video EGG), ...
  - signálová:
    - ECG (elektrokardiografie), EEG (elektroencefalografie),
    - EMG (elektromyografie), EOG (elektrookulografie),
    - EGG (elektroglotografie), ...
  - zvuková
    - hlasivky, srdeční ozvy, ...

3.8 Klasifikační systémy

Klasifikačních systémů, číselníků, nomenklatur nebo škál je ve zdravotnictví a vykazování používáno velmi mnoho. Příkladem jsou:

- *International Classification of Diseases* (ICD) je v českém prostředí pod označením *Mezinárodní klasifikace nemocí*[16] (MKN),

  Například: I63, I63.x, J10.8, U07.1, ...
- *Národní číselník laboratorních položek* (NČLP) obsahuje >18 000 definic, vychází z uznávané mezinárodní nomenklatury IFCC.

  Příklad NČLP klíč 12352:
  „Glukóza (P; látková konc. [mmol/l] abs. spektrofotometrie) Glukóza měřená v plazmě stanovovaná jako látková koncentrace v jednotkách mmol/l metodou absorpční spektrofotometrie.“

[16] *https://mkn10.uzis.cz/*

- *Logical Observation Identifiers Names and Codes*[17] (LOINC),
- *Systematized Nomenclature of Medicine – Clinical Terms*[18] (SNOMED-CT),

Každý obor/oblast má své vlastní číselníky, škály a způsoby klasifikace. Například pro neurologické vyšetření jsou využívány mimo jiné také škály:

- *National Institute of Health Stroke Scale*[19] (NIHSS) je standardizované neurologické vyšetření pro popis deficitu u pacientů s iktem.
  - Cílem je získat srovnatelné výsledky od různých vyšetřujících, které hodnotí pacienty: vědomí, slovní odpovědi, vyhovění výzvám, okulomotorika, zorné pole, faciální paresa, motorika HK a DK, ataxie, senzitivita, řeč, dysartrie, neglect.
- *Modified Rankin Scale*[20] (mRS) je škála s hodnotami 0–6, která je určená pro hodnocení následků po CMP.
- *Hodnocení rekanalizace*[21] (TIBI).

[17] *https://loinc.org/*
[18] *http://www.ihtsdo.org/snomed-ct/*
[19] https://www.manual-cmp.cz/nihss/
[20] https://www.manual-cmp.cz/modified-rankin-scale-mrs/
[21] https://www.manual-cmp.cz/?rc_blocks=tibi

4 Datové formáty

Datové formáty a standardy – podobnost s jinými oblastmi

- zájmové skupiny, výrobci – proprietární formáty,
- legislativa – forma nařízení, Sbírka zákonů.

Datový formát a dilema:

- zachovat *obecnost* nebo kontext?
- prosté zprostředkování výměny vs. strojová interpretace a zpracování?
- flexibilní výměnný formát?
- komplexita?
- zájmové skupiny?

Diagnostická a terapeutická data, laboratorní výsledky:

- DASTA,
- HL7.

Obrazová data

- DICOM

Specifické formáty – dle domény/modality/výrobce/IS:

- proprietární formáty výrobce zařízení,
- zájmové skupiny,
- signálová data – více kanálů, metadata:
  - European Data Format – EDF, EDF+,
  - Hierarchical Data Format 5 – HDF5,
  - Ovation, NeXus Format, NEO, NeuroHDF, NIX, WG1/WG2 (Walter Graphtek), ...
    Pro formáty existují různá omezení, možnosti konverzí nebo rozšíření.
- registry.

4.1 DASTA

DAtový STAndard (DASTA) [dastacr.cz]

- národní standard výměny informací ve zdravotnictví – ČR, SR,
- státních organizace, veřejné/privátní subjekty,
  - Česká společnost zdravotnické informatiky a vědeckých informací,
    Česká lékařská společnost J. E. Purkyně (ČLS JEP) [http://cszivi.cls.cz/ (2003)][cls.cz]
- zaštítěn, podporován a vydává **MZ ČR**,
  - 1992: prvotní impuls – individuální přístupy – sjednotit
  - 1997: DS 01.10, textový formát

  - 2001: DS 01.20, [DS1.20.rtf[22]]
  - 2002: DS 02.01, DTD (plánována harmonizace DS2.00 s HL7)
  - 2003: DS 03.01,
  - 2007: **DS 04.01**, XML Schema
  - 2018: DS 04.16.01 rozšíření *eHealth Digital Service Infrastructure* (eHDSI or eHealth DSI) ⇒ transformace podmnožiny DASTA do HL7 CDA [epSOS – Patient Summary[23]].
- Kde je formát DASTA používán?
  - ČR, SR,
  - nemocniční IS:
    - firmy DATAPLAN, HICOMP, ICZ, LOGIS, MEDICALC, MEDICON, PCS, SMS, SOPHIS, STAPRO, STEINER, VIP, ...
  - laboratorní IS:
    - firmy CNS, CSC, DS SOFT, DYNATECH, HICOMP, ICZ, LIRS, MEDICON, MP PROGRAM, PCS, SMS, STAPRO, STEINER, TIS,
  - IS pro praktické lékaře, specialisty, RDG, MIS,
  - též ÚZIS (data NZIS),
  - Státní zdravotní ústav (SZÚ),
  - hygiena a epidemiologie (kvalita vody, ...),
  - vykazování výkonů – zdravotní pojišťovny,
  - dočasná pracovní neschopnost – ČSSZ, ...
- Co je obsahem?
  - identifikační data pacienta,
  - informace o pacientovi – nacionále, RČ, adresy, výška, hmotnost, . . .
  - urgentní informace – alergie, krevní skupina, rizikové faktory, náhrady/implantáty/zařízení, trvalá medikace, očkování proti tetanu
  - anamnéza,
  - léky,
  - očkování,
  - diagnózy – trvalé a aktuální,
  - klinické události – objednávky, výsledky, zprávy,
    - viz číselník klinických událostí – laboratoře, RDG, dokumentace mnoha typů, speciální vyšetření,
  - platební vztahy, pojišťovny, pracovní neschopnosti,
  - podklady pro vyúčtování a MIS
  - speciální datové bloky, nástroje pro vkládání speciálních firemních datových bloků
- Podoba formátu [Datový standard MZ ČR]
  1. datová struktura (XML Schema),
  2. dokumentace – popis způsobu vyplnění datových bloků, omezení, kontext,
  3. číselníky – interní a externí:
     - DASTA (interní),
     - Národní číselníky laboratorních položek (NČLP),
     - Národní zdravotnický informační systém (NZIS)/ÚZIS.

[22] http://cszivi.cls.cz/clp/0012/SDR2.rtf
[23] https://dastacr.cz/PS.html

4.2 HL7

Health Level 7 (HL7), [hl7.org]

- HL7v2 od 1989, všechny verze 2.x jsou zpětně kompatibilní;
- HL7v3 od 2005;
- HL7 International spravuje:
  - HL7 v2.x – interoperabilní zdravotní a lékařské transakce;
  - HL7 v3 – interoperabilní zdravotní a lékařské transakce;
    - Clinical Document Architecture (CDA) – model výměny klinických dokumentů dle HL7 v3;
  - Fast Healthcare Interoperability Resources (FHIR).

4.3 FHIR

Fast Healthcare Interoperability Resources (FHIR) – vytvořen HL7 [web]

- Rámec standardů nové generace – kombinuje nejlepší:
  - HL7v2, HL7v3, CDA, webové a další existující standardy.
- Nabízí:
  - silné zaměření na implementaci – rychlá a snadná implementace;
  - více implementačních knihoven, mnoho příkladů pro zahájení vývoje;
  - specifikace – volně k použití, bez omezení;
  - interoperabilita základem – zdroje lze použít přímo nebo dle potřeby upravit;
    - často – místní požadavky pomocí profilů, rozšíření, terminologií, ...;
  - evoluce od HL7v2 a CDA – standardy vedle sebe a využívají se;
  - Webové standardy: XML, JSON, HTTP, OAuth, ...;
  - Podpora architektur založených na službách – RESTful;
  - stručné a snadno srozumitelné specifikace;
  - člověkem čitelný serializační formát pro použití vývojáři;
  - analýza založená na ontologii s formálním mapováním správnosti (ve vývoji)

4.4 DICOM

Digital Imaging and COmmunications in Medicine (DICOM), [dicomstandard.org] představuje datový standard, datový formát, ale také komunikační protokol pro biomedicínská data. Hlavní část jsou multimediální data jako jsou snímky, ale formát DICOM slouží spíše jako obálka, která umožňuje vložení i videa nebo biomedicínských signálů. Nejčastěji to jsou právě obrazová data. Možná je také komprese multimediálního obsahu.

Každý DICOM soubor je doplněn o metadata, která popisují kontext – pacienta, studii, sérii, snímek, ale také samotnou modalitu nebo konfiguraci, apod. Jsou to informace o pořízeném snímku.

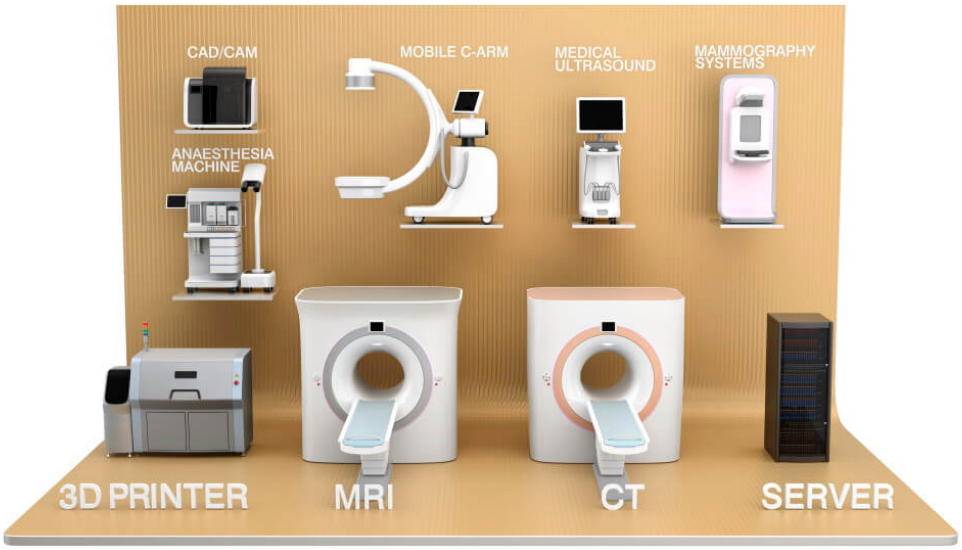
Pro zobrazení DICOM snímků nebo celých vyšetření se používá specializovaný software.

4.4.1 Historie

- 1983 – American College of Radiology (ACR) a National Electrical Manufacturers Association (NEMA) tvoří společnou komisi/výbor:
  - digitální komunikace obrazové informace,
  - nezávislost na výrobci modality,
  - archivační a komunikační systém,
  - podpora spolupráce s okolními systémy nemocnice,
  - tvorba sdíleného archívu diagnostických informací.
- ACR-NEMA 300-1985: 1. verze; 1986 – 1. revize; 1988 – 2. revize
  - hardwarové rozhraní pro komunikaci point-to-point, není síťová podpora přenosu snímků,
  - datový slovník a pravidla kódování informací, základní příkazy.
- ACR-NEMA 300-1988: 2. verze:
  - podpora příkazů pro zobrazovací zařízení,
  - nové schéma identifikace a prvky popisu snímku.
- 1993 – 3. verze, standard revidován, označení DICOM.
- 1995 – existuje široká spolupráce napříč zobrazovacími specializacemi.

4.4.2 Modality

AR Autorefraction; **ASMT** Content Assessment Results; **AU** Audio; **BDUS** Bone Densitometry (ultrasound); **BI** Biomagnetic imaging; **BMD** Bone Densitometry (X-Ray); **CR** Computed Radiography; **CT** Computed Tomography; **DG** Diaphanography; **DOC** Document; **DX** Digital Radiography; **ECG** Electrocardiography; **EPS** Cardiac Electrophysiology; **ES** Endoscopy; **FID** Fiducials; **GM** General Microscopy; **HC** Hard Copy; **HD** Hemodynamic Waveform; **IO** Intra-Oral Radiography; **IOL** Intraocular Lens Data; **IVOCT** Intravascular Optical Coherence Tomography; **IVUS** Intravascular Ultrasound; **KER** Keratometry; **KO** Key Object Selection; **LEN** Lensometry; **LS** Laser surface scan; **MG** Mammography; **MR** Magnetic Resonance; **NM** Nuclear Medicine; **OAM** Ophthalmic Axial Measurements; **OCT** Optical Coherence Tomography (non-Ophthalmic); **OP** Ophthalmic Photography; **OPM** Ophthalmic Mapping; **OPT** Ophthalmic Tomography; **OPV** Ophthalmic Visual Field; **OSS** Optical Surface Scan; **OT** Other; **PLAN** Plan; **PR** Presentation State; **PT** Positron Emission Tomography (PET); **PX** Panoramic X-Ray; **REG** Registration; **RESP** Respiratory Waveform; **RF** Radio Fluoroscopy; **RG** Radiographic imaging; **RTDOSE** Radiotherapy Dose; **RTIMAGE** Radiotherapy Image; **RTPLAN** Radiotherapy Plan; **RTRECORD** RT Treatment Record; **RTSTRUCT** Radiotherapy Structure Set; **RWV** Real World Value Map; **SEG** Segmentation; **SM** Slide Microscopy; **SMR** Stereometric Relationship; **SR** SR Document; **SRF** Subjective Refraction; **STAIN** Automated Slide Stainer; **TG** Thermography; **US** Ultrasound; **VA** Visual Acuity; **XA** X-Ray Angiography; **XC** External-camera Photography;



Obrázek 12: Ukázky podporovaných modalit v DICOM. [postdicom.com]

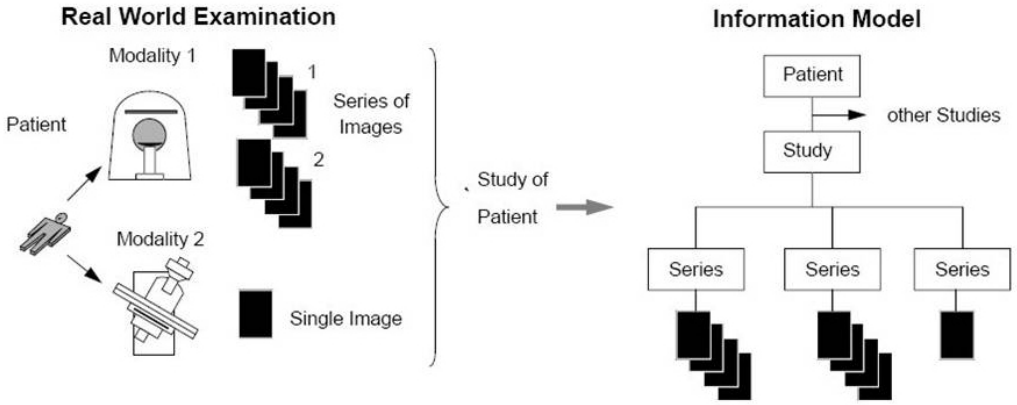
4.4.3 Popis

„Health Informatics – Digital Imaging and Communication in Medicine (DICOM) Including Workflow and Data Management“ [NEMA PS3[24], ISO 12052:2017[25]]

- Souborový formát:
  - obrazová informace – specifický atribut,
  - metadata:
    - o pacientovi (identifikace, výška, hmotnost),
    - údaje o akvizici (typ zařízení, nastavení),
    - o snímku (rozlišení, tloušťka řezu),
    - a další.
- Síťový protokol:
  - výměna dat, snímky DICOM, informace o pacientech a postupech,
  - vyhledávání studií/snímků v archivu a získání na pracovní stanici pro zobrazení,
  - pokročilé příkazy – řízení/sledování léčby, plánování procedur, hlášení stavů.
- Integrace modalit různých výrobců.

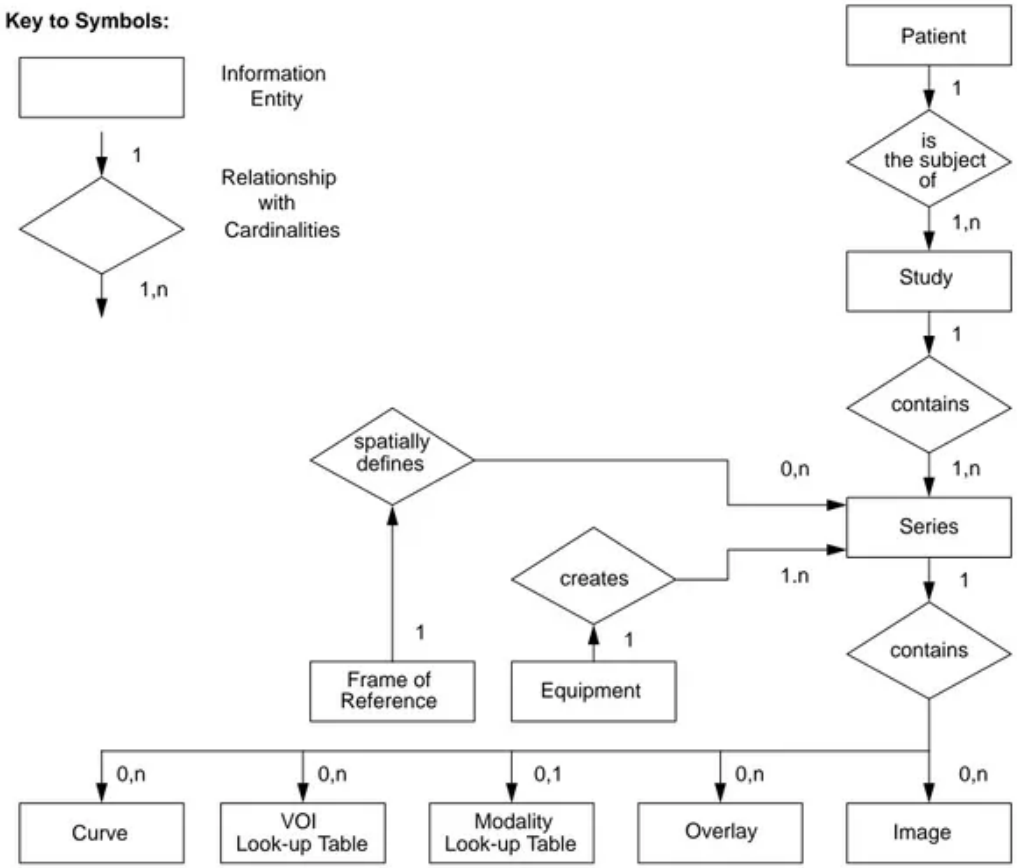
[24] https://dicom.nema.org/medical/dicom/current/output/html/part01.html
[25] https://www.iso.org/standard/72941.html

4.4.4 Akvizice dat



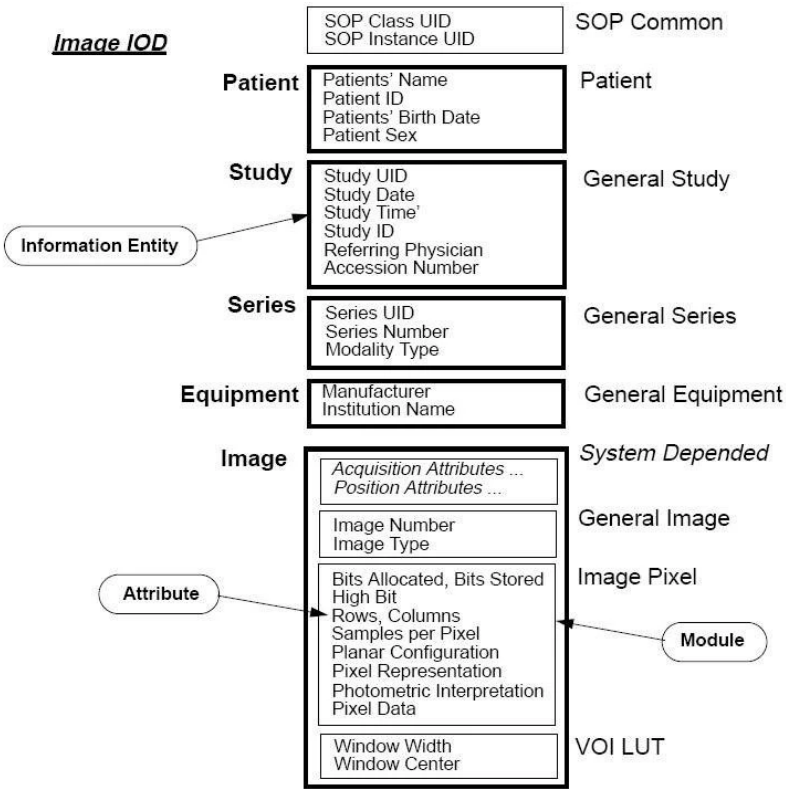
Obrázek 13: Ilustrace akvizice dat a informačního modelu DICOM. [dcm4che.atlassian.net]

4.4.5 Informační objektový model



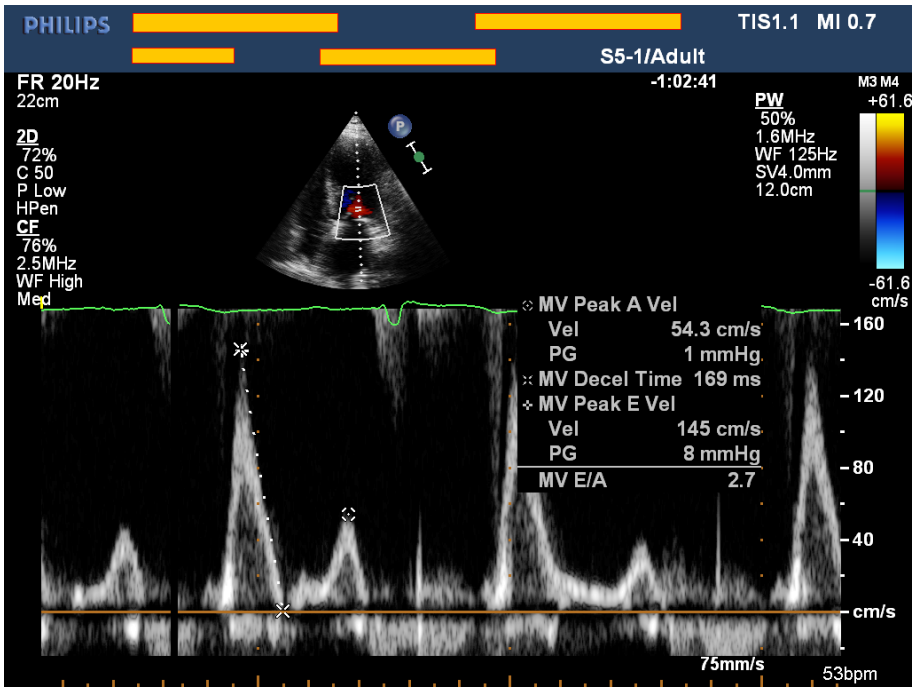
Obrázek 14: Informační objektový model DICOM.

4.4.6 Metadata pro snímek



Obrázek 15: Metadata snímku pro jednotlivé informační objekty. [dcm4che.atlassian.net]

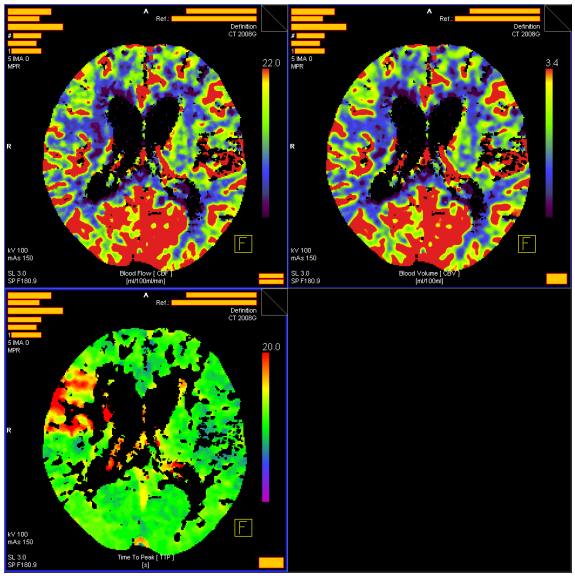
4.4.7 Příklady snímků



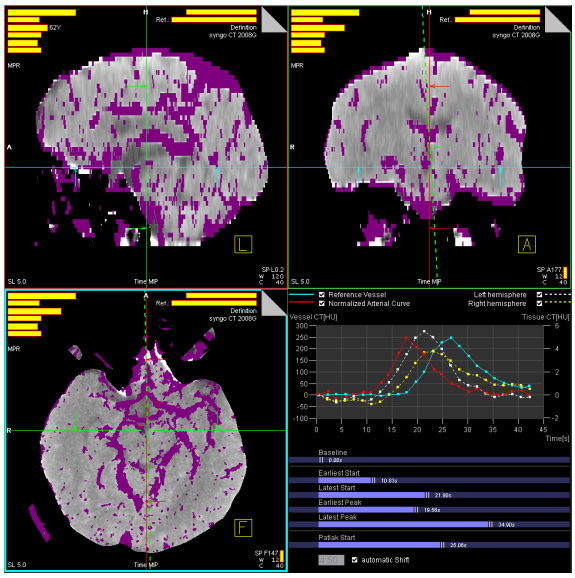
Obrázek 16: ECHO/SONO vyšetření.

Obrázek 17: RTG snímek.

Obrázek 18: RTG snímek.



Obrázek 19: Perfuzní CT. Cerebral Blood Flow (CBF), Cerebral Blood Volume (CBV), Maximum Intensity Projection(MIP), Time to Peak (TTP).



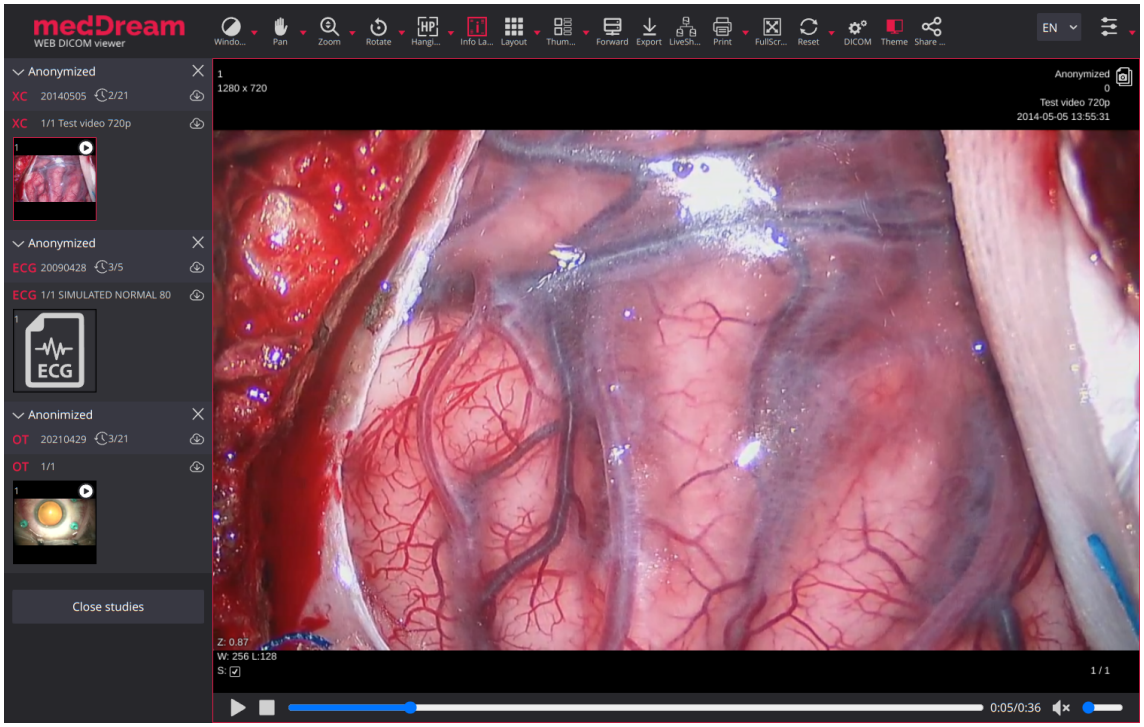
Obrázek 20: Perfuzní CT. Cerebral Blood Flow (CBF), Cerebral Blood Volume (CBV), Maximum Intensity Projection(MIP), Time to Peak (TTP).

4.4.8 DICOM Viewer

DICOM Viewer od společnosti Softneta.com je k dispozici online. DICOM prohlížeč lze používat prostřednictvím webového prohlížeče (https://www.softneta.com/online-dicom-viewer/).

Demoverze (demo.softneta.com) prohlížeče poskytuje příklady různých modalit, se kterými můžete různě manipulovat. Pro citlivější jedince mohou být některé příklady[26] nevhodné – byli jste varováni – vyzkoušejte pouze na vlastní nebezpečí.

[26] Třeba video z operace oka.



Obrázek 21: DICOM Viewer. [demo.softneta.com]