



# Ochrana dat ve zdravotnických IS

## *Etická, právní a provozní specifika*

MUDr. Miroslav Seiner

## Prolog

- 13.2.2007
  - Ø Alabama Veteran´s Hospital
    - » Ztráta hard disku s lékařskými záznamy o 535 000 pacientech a lékařskými účty od 1,3 mil. lékařů
- 13.2.2007
  - Ø St. Mary´s Hospital, Leonardtown, Maryland
    - » Ztráta dat o 130 000 pacientech – krádež počítače, na kterém byli pacienti registrováni
- 7.2.2007
  - Ø John Hopkins Hospital, Maryland
    - » Ztráta záložních pásků o 53 000 zaměstnancích a 83 000 pacientech, včetně lékařských záznamů
- 28.11.2006
  - Ø Kaiser Permanente
    - » Ztráta notebooku s osobními daty o 38 tisíci pacientech (krádež v autě) – data osobní, administrativní lékařská.... Důvod: příprava projektu kvality

n Zdroje: <http://www.consumeraffairs.com>

## Obsah přednášky

- Důvody proč data chránit
- Právní podklady ochrany dat
- Specifika ochrany dat ve zdravotnických IS
- Metody ochrany dat
  - Ø jak chránit data v IS
- Reflexe zahraničních zkušeností

## Proč chránit data pacientů ?

- Důvody etické a mravní
  - Ø Je to správné, morálně nezbytné
- Důvody právní
  - Ø Je to dáno zákonem a hrozí trest při zanedbání
- Dodržení odborných norem, a standardů kvality
  - Ø Vynucují to standardy kvality
- Důvody obchodní (marketingové)
  - Ø Může to být obsahem konkurenčního boje o zákazníka (klienta)

## Argumenty odpůrců důsledné ochrany dat

- Poukazování na aktuální stav v klasické dokumentaci
- Absolutizace a karikování problému
- Poukazování na protikladné právo pacienta na správnou léčbu
- Poukazování na provozní problémy

## Diskuse – srovnávání....

- Srovnávání ochrany dat v informačních systémech s ochranou dat v klasické dokumentaci
  - Ø Zdravotnická data v IS mají jiné typy a rozsah ohrožení - například množství potenciálních útočníků, možnost rychle získat velké objemy dat
  - Ø Celkově nároky na ochranu soukromí se zvyšují vzhledem ke zkušenostem, které má civilizace s jejich zneužitím

## Diskuse - absolutizace

- Absolutizace problému - „nelze dosáhnout nikdy absolutní bezpečnosti a proto nemá ochrana význam“
  - Ø Opravdu nelze dosáhnout absolutní ochrany ale není to argument proti
  - Ø Nesmí se usilovat o **absolutní** ale o **definovanou a kontrolovanou úroveň bezpečnosti**
  - Ø **Významná závislost ceny zabezpečení na požadované míře ochrany**

## Diskuse – právo pacienta na léčbu

- Oháníte se právy pacienta na ochranu soukromí ale berete mu právo na správnou léčbu
- Tato dvě práva nejsou v protikladu
- Pacient má především sám nezcizitelné právo rozhodovat o tom, co se ho osobně dotýká

## Diskuse – provozní problémy

- „Nelze kombinovat provozní požadavky na dostupnost informací a ochranu dat“
  - Ø Vážný argument, který je nutno respektovat, ale který má řešení v kombinaci technologie a organizačních opatření
  - Ø Je třeba zajistit u každého typu tad specificky:
    - » Rutinní přístup tomu, kdo s daty běžně pracuje
    - » Mimořádný přístup tomu, kdo data potřebuje mimořádně, ale vážně
    - » Absolutní zabránění přístupu těm, kdo nemají na data nárok
    - » Kontrolu všech

## Právní rámec ochrany dat pacientů v České republice

- **Nadnárodní normy**
  - Ø *Směrnice Evropského parlamentu a Rady 95/46/ES*
  - Ø *Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie medicíny*
- **Ústavní ochrana práva na ochranu soukromí a osobnosti**
  - Ø Listina základních práv a svobod, čl. 10
- **Zákony**
  - Ø Zákon o ochraně osobních údajů č. 101/2000Sb.
  - Ø Zákon o péči o zdraví lidu č.20/1966 Sb.
    - » *Novela 260/2001 Sb., § 67 a - d*
    - » *Návrh zákona o zdravotní péči řeší prakticky stejně jako zákon dosavadní*
  - Ø Trestní zákon
    - » Zák. č 140/1961 Sb., § 178, neoprávněné nakládání s osobními údaji

## Právní principy ochrany soukromí (citlivých osobních údajů)

- Každý má právo dovídat se (ale také zpracovávat, sbírat, uchovávat) osobní údaje **jen v mezích, které mu povoluje zákon** nebo kterou **mu povolila osoba, jichž se údaje týkají**
- Povinnost ochrany dat **leží na správci i na zpracovateli dat** - (provozovateli IS, nemocnici, ZZ...)
- Zákonné povinnosti i eventuální sankce se týkají **nejen institucí, ale i konkrétních pracovníků**
- Porušení ochrany soukromí je kryto citelnými **sankcemi** finančními i trestními
- Trestá se i **nedbalost a zanedbání** !

## Specifické právní zásady ochrany zdravotnických dat

- Data o zdravotní péči mohou (musí) být **vedena i bez souhlasu osoby**, které se dotýkají
- **Přístup ke zdravotnické dokumentaci** je v zákoně řešen explicitně - výčtem „oprávněných“ subjektů- **profese i instituce**, které mají ke zdravotnické dokumentaci přístup
- Rozsah přístupu je omezen na „**rozsah nezbytně nutný** ke splnění konkrétního úkolu...“

## Poslední významné úpravy v legislativě – rok 2007

Ø Zákon č. 111/2007 Sb.

Ø Vyhláška Ministerstva zdravotnictví  
č. 64/2007

- » Pacient má právo nahlížet do zdravotnické dokumentace o své osobě
- » Pacient má právo na opis
- » Musí být evidovány osoby, které mají oprávnění nahlížet dle rozhodnutí pacienta
- » Musí být evidována nahlédnutí do dokumentace jinými osobami

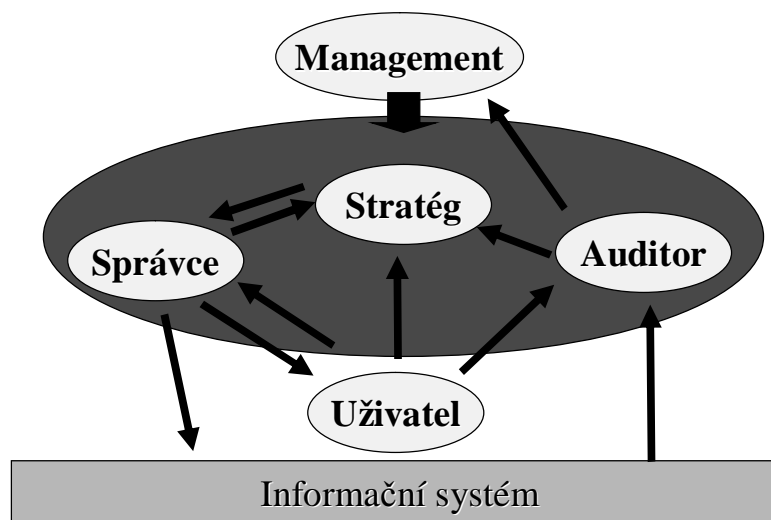
## Vztah ochrany dat (soukromí) a mlčenlivosti

- (Lékařská) mlčenlivost není pouze etickou kategorií ale výslovně ji požaduje zákon a stanovuje její podmínky.
- Mlčenlivost, které podléhají zdravotničtí pracovníci ale neruší obecnější požadavky zákona na ochranu soukromí a nedávají zdravotníkům právo na nekontrolovaný přístup k citlivým údajům
- Lékař musí **pomlčet o skutečnostech, které se dozvěděl**, ale to se týká skutečností, které se dozvěděl oprávněně

## Organizační zajištění bezpečnosti informačních systémů

- Musí vycházet z rozhodnutí managementu
- Musí být systematické, dlouhodobé
- Musí existovat konkrétní osobní odpovědnost
- Musí existovat pevná struktura bezpečnostního managementu
  - Ø Bezpečnostní strategie
  - Ø Bezpečnostní správa
  - Ø Bezpečnostní audit

## Bezpečnostní management IS





## Role pacientů v ochraně citlivých dat

- Rola pacientů v ochraně jejich vlastních dat poroste s rostoucím povědomím osob o této problematice
- Pacient musí být plně a srozumitelně informován o bezpečnostní politice konkrétního IS a to především o tom:
  - Ø Kdo a za jakých podmínek má k jeho datům přístup
  - Ø Jak dlouho jsou jeho data uchovávána
  - Ø K jakým účelům a kým mohou být jeho data využita a komu jsou dále poskytována

## Zahraniční inspirace: Privacy Rule HIPAA

- Standards for Privacy of Individually Identifiable Health Information (tzv. Privacy Rule“)
  - Ø U.S. Department of Health and Human Services (HHS) v březnu 2002 po dvou letech přípravy
  - Ø Vyplývá ze zákona HIPAA (Health Insurance Portability and Accountability Act), 1996
  - Ø <http://www.hhs.gov/ocr/hipaa>

## Principy Privacy Rule HIPAA

- Kdo je povinen pravidla dodržovat
- Jakých typů informací se dotýkají
- Základní principy nakládání s daty a popis jednotlivých typů nakládání s daty
- Požadavky na subjekty
- Sankce

## Výběr z požadavků Privacy Rule HIPAA

- Organizace musí
  - Ø zveřejnit svou bezpečnostní politiku
  - Ø určit osobní odpovědnost za provádění
  - Ø trénovat a poučovat zaměstnance
  - Ø napravit či zmírnit v přiměřené míře škody
  - Ø Chránit data všemi přiměřenými prostředky
  - Ø Zabránit tomu, aby byl kdokoli odmítnut pro péči jen z důvodu dožadování se těchto práv
  - Ø 6 let uchovávat veškerá data, nutná k prokázání správné bezpečnostní politiky

## Závěr

- Ochrana osobních citlivých údajů ve zdravotnických IS **je nezbytná** z důvodů etických, právních i dalších.
- Současný **stav není příznivý** - problematika je podceňována a je snaha ji obcházet
- Dobré **řešení není snadné** vzhledem k nutnosti spojit oprávněné nároky na vysokou a specifickou dostupnost zdravotních dat při léčebné péči s požadavky na ochranu dat
- Řešení je v
  - Ø **postupném budování definované** úrovně bezpečnosti,
  - Ø v **kombinaci technických a organizačních opatření**
  - Ø v **realizaci bezpečnostní politiky** a bezpečnostního managementu podle standardních pravidel

## Kontakt

Miroslav Seiner

seiner@infomed.cz

www.infomed.cz