Ochrana dat ve zdravotnických IS

Etická, právní a provozní specifika

MUDr. Miroslav Seiner
říjen 2007

Obsah přednášky

- Právní podklady ochrany dat
- Specifika ochrany dat ve zdravotnických IS
- Metody ochrany dat
  - jak chránit data v IS

Prolog

- 13.2.2007
  - 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
  - St. Mary´s Hospital, Leonardtown, Maryland
    - Ztráta dat o 130 000 pacientech – krádež počítače, na kterém byli pacienti registrováni
- 7.2.2007
  - John Hopkins Hospital, maryland
    - Ztráta záložních pásků o 53 000 zaměstnancích a 83 000 pacientech, včetně lékařských záznamů
- 28.11.2006
  - Kaiser Permanente
    - Ztráta notebooku s osobními daty o 38 tisíci pacientech (krádež v autě) – data osobní, administrativní lékařská.... Důvod: příprava projektu kvality

Zdroje: http://www.consumeraffairs.com

Proč chránit data pacientů ?

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

Právní rámec ochrany dat pacientů v České republice

- Nadnárodní normy
  - *Směrnice Evropského parlamentu a Rady 95/46/ES*
  - *Úmluva na ochranu lidských práv a důstojnosti lidské bytosti v souvislosti s aplikací biologie medicíny*
- Ústavní ochrana práva na ochranu soukromí a osobnosti
  - Listina základních práv a svobod, čl. 10
- Zákony
  - Zákon o ochraně osobních údajů *č. 101/2000Sb.*
  - 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*
  - Trestní zákon
    - » Zák. č 140/1961 Sb., § 178, neoprávněné nakládání s osobními údaji

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…“

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** !

Nové prvky v legislativě 2007

- Zákon č.111/2007Sb.
- 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

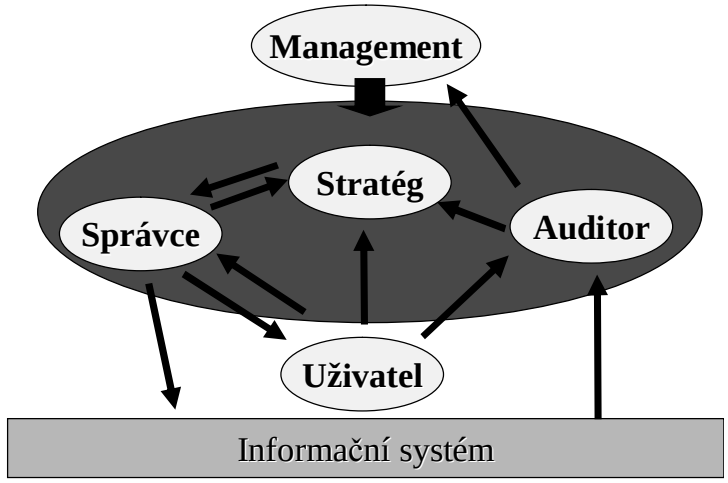
Organizační zajištění bezpečnosti informačních systémů

- 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

Chybné argumenty odpůrců důsledné ochrany dat

- 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
- Absolutizace problému - „nelze dosáhnout nikdy absolutní bezpečnosti a proto nemá ochrana význam“
  - Ø Nesmí se usilovat o **absolutní** ale o **definovanou úroveň bezpečnosti**
- „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

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:
  - Kdo a za jakých podmínek má k jeho datům přístup
  - Jak dlouho jsou jeho data uchovávána
  - K jakým účelům a kým mohou být jeho data využita a komu jsou dále poskytována

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

Zahraniční inspirace: Privacy Rule HIPAA

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

Výběr z požadavků Privacy Rule HIPAA

- Organizace musí
  - zveřejnit svou bezpečnostní politiku
  - určit osobní odpovědnost za provádění
  - trénovat a poučovat zaměstnance
  - napravit či zmírnit v přiměřené míře škody
  - Chránit data všemi přiměřenými prostředky
  - Zabránit tomu, aby byl kdokoli odmítnut pro péči jen z důvodu dožadování se těchto práv
  - 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 **kombinací technických a organizačních opatření**
  - Ø v **realizaci bezpečnostní politiky** a bezpečnostního managementu podle standardních pravidel

Kontakt

Miroslav Seiner

seiner@infomed.cz

www.infomed.cz

(i aktualizované informace o legislativě)