Avoiding breaches and subsequent audits

October 2010

Overview

- Speaker
  - Cliff Baker
  - Chief Strategy Officer, HITRUST Alliance
  - cliff.baker@hitrustalliance.net
- Presentation Overview
  - Understanding your risks and exposures
  - Prioritizing your efforts
  - Supporting your decisions

Understand your risks – risk framework

Meaningful Use

- 42 CFR §495.6 (a) (EPs) , (b) (hospitals): Stage 1 objectives and associated measures
- (d)(15)(EPs), (f)(14)(hospitals):
  - (i) **Objective**. Protect electronic health information created or maintained by the certified EHR technology through the implementation of **appropriate technical capabilities**.
  - (ii) **Measure**. Conduct or review **a security risk analysis** in accordance with the requirements **under 45 CFR 164.308(a)(1)** and implement **security updates** as necessary and **correct identified security deficiencies** as part of its **risk management process.**

HIPAA

- 164.308(a)(1)(ii)(A)
  - Risk Analysis (R): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.
- 164.308(a)(1)(ii)(B)
  - Risk Management (R): Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Section 164.306(a).

Risk Assessment Methodology (NIST, ISO)

- Areas of exposure

- Leverage a Security Framework
- Align with reasonable practice

•NIST SP 800-30, Risk Management Guide on Technology Systems
•OCR Risk Management Guidance
//www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html

High Risks for Healthcare Organizations

- Insecure and/or unauthorized removable/transportable media and laptops (internal and external movements)
- Insecure and/or unauthorized external electronic transmissions of covered information
- Insecure and/or unauthorized remote access by internal and third-party personnel
- Insider snooping and data theft
- Malicious code and inconsistent implementation and update of prevention software
- Inadequate and irregular information security awareness for the entire workforce
- Lack of consistent network isolation between internal and external domains
- Insecure and/or unauthorized implementation of wireless technology
- Lack of consistent service provider, third-party and product support for information security
- Insecure web development and applications
- Ineffective password management and protection
- Ineffective disposal of system assets

Cybercrime

- Healthcare organizations are a newly favored target among cybercriminals because of the wealth of personal data they collect which can be monetized.
- **Fraud** resulting from exposure of health data versus other kinds of sensitive information **increased from 3% in 2008 to 7% in 2009**.
- Criminals were able to exploit information from medical records to commit fraud for **four times longer** as compared to other types of identity theft.
- Information contained in medical records has much broader utility, can be used to commit multiple types of fraud or identity theft, and does not change, even if compromised.
- The value of personal data to a cybercriminal is much higher than a credit card or bank account number.

RSA White Paper: Cybercrime and the Healthcare Industry

Cybercrime—Why Steal Healthcare Data?

- Harder to detect:
  - Medical information fraud takes more than twice as long to identify as compared to regular identity theft
  - Victims cannot delete or change their personal information, medical records or history of prescription use
- It pays:
  - The World Privacy Forum has reported that the street cost for stolen **medical information is $50**, versus $1 for a stolen Social Security number
  - The average payout for a medical identity theft is $20,000, compared to $2,000 for a regular identity theft.

RSA White Paper: Cybercrime and the Healthcare Industry

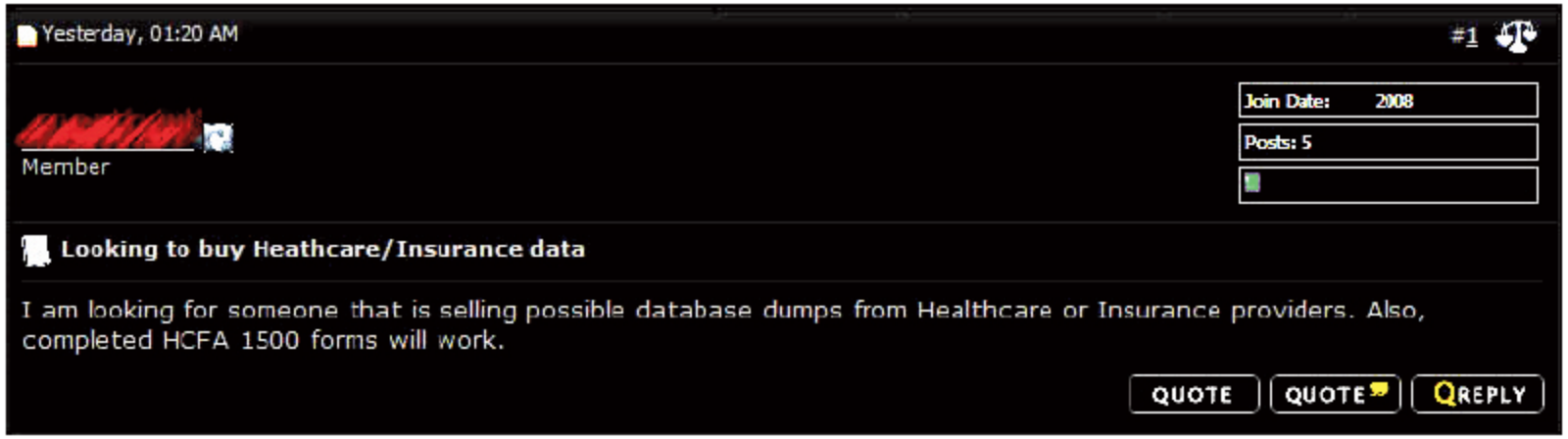
Cybercrime—How to Use Healthcare Data

- Cybercriminals target not just consumer data but also information from healthcare providers, insurers, and pharmaceutical manufacturers and distributors.
- One of the ways in which cybercriminals are committing healthcare fraud is by filing false patient claims to insurers and government agencies that provide health services.
- Another example is simply selling data on individual medical records in the black market.
- There is also a demand for pharmaceutical data, which cybercriminals can use to order prescriptions at multiple pharmacies and then attempt to resell the medicine online.
- Physicians' information is also valuable to cybercriminals because they can use it to write fake prescriptions to facilitate schemes involving the purchase and resale of prescription drugs.

RSA White Paper: Cybercrime and the Healthcare Industry

Cybercrime—Example (i)

- Cybercriminal seeking data that will enable him/her to file false medical claims:



RSA White Paper: Cybercrime and the Healthcare Industry

Cybercrime—Example (ii)

- A post in the underground seeking buyers for the medical records of over 6,500 patients:

6561 individuals claims notification report medical records

6561 individuals claims notification report medical records

I have a large file that contains 6561 individuals claims notification report medical records.

File comes with these fields for each person.
---
certno
group
deductible
tpa
lcm
treaty
insured
patient name
ssn
status1
status2
status3
icd9
diagnosis - This field contains their diagnosis such as AIDS, HIV, Left Heart Failure, Diabetes, etc
tpa_paid
med_expense
transplant

Here are some examples of Diagnosis from the file
- HIV W/SPECIF INFECTIONS
- Malignant Neoplasm Of Lateral Wall Of Urinary Bladder
- Morbid Obesity; chronic nonalcoholic liver disease
- Alcoholic Cirrhosis Of Liver, other spec intestinal malabsorption
- HIV, cachexia, HTLV-1, neoplasm of uns. nature of digestive system
- Liver Replaced By Transplant
- Excessive Or Frequent Menstruation

- Price: make offers

RSA White Paper: Cybercrime and the Healthcare Industry

Cybercrime—Affect on Patients

- Consumers of healthcare services are also affected in many ways by having their medical records exposed or breached, including:
  - Personal data being used by criminals to open new credit accounts in their name
  - Being wrongly accused of abusing medical services due to criminals filing false medical claims using their information
  - Threatened with blackmail or extortion from criminals threatening to expose sensitive medical or health details (while no cases of blackmail have yet been reported with consumers of healthcare services, cybercriminals who had stolen 8.3 million patient records from the Virginia Prescription Monitoring Program demanded a $10 million ransom – this could certainly happen with the medical information of high-earning individuals)

RSA White Paper: Cybercrime and the Healthcare Industry

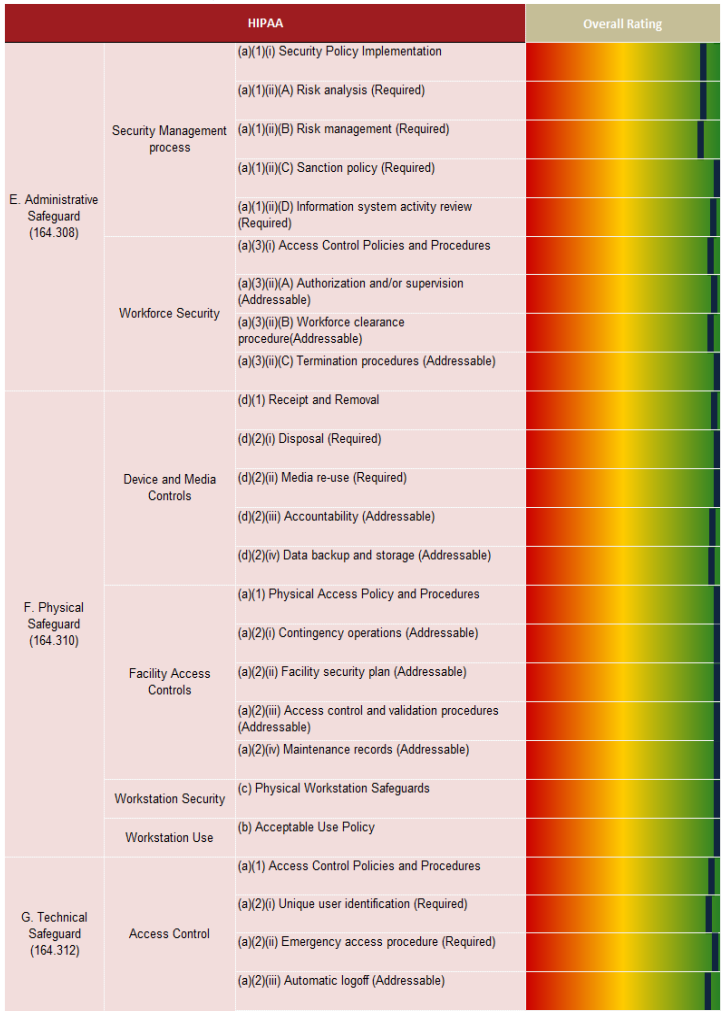
Cybercrime – Harm to Patients

- The stakes are high as the Institute of Medicine (IOM) highlights in its recent publication related to privacy:
  - *"breaches of an individual's privacy and confidentiality may affect a person's dignity and cause irreparable harm" and "[unauthorized disclosures] can result in stigma, embarrassment, and discrimination."*
    IOM: Beyond the HIPAA Privacy Rule—Enhancing Privacy, Improving Health Through Research, February 4, 2009

Approach to Security Risk Assessment

HIPAA Compliance Scorecard

- Understand your state of compliance with HIPAA



Executing the assessment

- Interview roles:
  - Web application manager
  - Internal audit
  - Security assurance manager (risk management, business continuity management, vulnerability management, training and awareness, security policies)
  - Monitoring and response manager
  - Server engineering
  - Desktop engineering
  - Human resources
  - Access and identity management
  - Application developer

Executing the assessment (cont'd)

- Documents review:
  - Asset inventory with risk classification
  - Network diagram
  - Organization chart
  - Business Associate Agreement template
  - Risk assessment program
    - Application assessment questionnaires
    - Sample web application assessments
    - Sample network vulnerability assessments
    - Sample attack and penetration report
  - Project/engagement hierarchy

Executing the assessment (cont'd)

- Documents review (continued):
  - Business continuity management program
    - Business Impact Analysis templates
    - Business continuity plan template
    - Disaster recovery plan template
    - Sample business continuity and disaster recovery plans
  - Sample security awareness and training materials
  - Policies and standards framework
    - Policy and standards third party review report
  - Incident monitoring and response program and associated procedures
  - Security council charter

Lessons Learned

- Healthcare providers have challenges – you will have gaps
- Assessment methodology
  - Sound approach – NIST, HITRUST
- Supporting attestation
  - Make sure attesting officer is properly informed about risks, updates, corrections, etc.
    - Create and retain supporting documentation file
    - In any field where officer does not have appropriate expertise, ensure s/he is briefed and provided with supporting documentation from appropriate experts
    - Good “business judgment” is the attesting officer’s best friend
  - **Show your work!**
    - Document risk analysis process and findings
    - Document implementation of updates and corrections
    - Providers must retain “documentation supporting their demonstration of meaningful use for 6 years” after attestation
      - HIPAA has same document retention period
- Address meaningful use but also address longer term goals and maintain HIPAA compliance